

CPPA's Precision Strike: Tackling the Fine Print of CCPA Regulations

May 30, 2025

A pair of recent enforcement actions by the California Privacy Protection Agency (CPPA) unveiled the agency's latest enforcement priorities for business-to-consumer companies. In March 2025, the CPPA announced a settlement with [Honda](#) for alleged violations of the California Consumer Privacy Act (CCPA). This was the CPPA's first enforcement action under the CCPA, which had previously only been enforced by the California attorney general, and originated with the CPPA's review of the privacy practices of connected vehicle manufacturers and related technologies initially [announced in July 2023](#). Earlier this month, the CPPA announced another settlement under the CCPA, this time with clothing retailer [Todd Snyder](#). These enforcement actions underscore several of the agency's key enforcement priorities, including compliance with the CCPA's:

1. Requirements related to authenticating consumers who have made privacy requests.
2. Requirements related to requests to opt out of the "sale" and "sharing" of personal information (opt-out requests) and requests to limit a business's use and disclosure of sensitive personal information (SPI requests).
3. Prohibition on "dark patterns."
4. Requirement to apply opt-out preference signals to known consumers.
5. Requirements for contracts with third parties.
6. General requirements related to consumer requests.

They also serve to implement the CPPA's enforcement advisories on [Avoiding Dark Patterns](#) and [Applying Data Minimization Principles to Consumer Requests](#).

Specifically, the CPPA alleged that Honda:

- Unlawfully required consumers to verify their identity when submitting opt-out requests and SPI requests.
- Unlawfully required consumers to confirm that they had given permission to an authorized agent to submit an opt-out request or SPI request on their behalf.
- Failed to provide a "symmetrical choice" when offering consumers the option to opt out of certain cookies and other tracking technologies through the company's cookie management tool.
- Failed to show that they have contracts in place with their adtech vendors and partners, which the CCPA requires include specific provisions.

In the case of Todd Snyder, like in the action against Honda, the CPPA also alleged that the company unlawfully required consumers to verify their identity when submitting opt-out requests. In addition, according to the CPPA, Todd Snyder:

- Unlawfully required consumers to submit more information than necessary to process their other privacy requests.
- Failed to ensure that the technical infrastructure of its privacy portal was properly configured, which resulted in the company's failure to process opt-out requests for 40 days.

As stipulated in the final order, [Honda agreed to pay an administrative fine of \\$632,500](#) – the second-highest fine imposed under the CCPA to date – which was based in part on multiplying the number of consumers affected by Honda’s noncompliance by \$2,500 per consumer (i.e., 119 consumers who provided more personal information than necessary to submit opt-out requests and SPI requests, 20 consumers whose requests were denied due to lack of verification and 14 consumers who were required to confirm with Honda directly that they had given their authorized agents permission to submit requests on their behalf). [Todd Snyder agreed to a \\$345,178 fine](#). The orders also require the companies to modify their privacy practices in a number of ways within either 90 or 180 days of their effective date, which we summarize below.

Verification of consumer privacy requests

1. Consumers cannot be required to verify their identity for opt-out requests and SPI requests.

Unlike consumer requests to know, correct and delete, which must be verified “because [of] the potential harm to [c]onsumers resulting from an imposter accessing, deleting, or changing personal information maintained by the business,” the CCPA prohibits businesses from requiring consumers to verify themselves before processing opt-out requests and SPI requests, for which the potential harm is “minimal or nonexistent.”¹ Instead, covered businesses may only require consumers to provide information necessary to process an opt-out request or SPI request – in other words, the information necessary to identify the consumer within their systems, rather than to verify that the person making the request is the person about whom the business collected information. This requirement accords with the “foundational principle” of applying data minimization to consumer requests, about which the CCPA issued its [first-ever enforcement advisory](#) in early 2024.²

The CPPA noted that Honda’s web form for submitting consumer privacy requests was the same for all types of requests and required consumers to provide at least their first and last name, full address, email and phone number, though according to the order, “Honda generally needs only two data points ... to identify the [c]onsumer within its database.” Todd Snyder similarly maintained a privacy portal that linked to a common web form for submitting all consumer privacy requests and, in each case, required the consumer to submit their first and last name, email, country of residence and a photo of them holding an “identity document” (e.g., a driver’s license).

The orders require that the companies collect from consumers making an opt-out request (or SPI request) only the information necessary to process the request, which also means the methods for submitting these requests must be separated from the methods for submitting other, verifiable privacy requests. The CPPA noted that Todd Snyder’s requirement to provide identity documents, which are common examples of “sensitive personal information” under the CCPA, made the company’s unnecessary data collection even worse.

2. Consumers cannot be required to directly confirm to a business that they gave their authorized agent permission to submit an opt-out request or SPI request.

The CCPA similarly sets forth distinct standards for opt-out requests and SPI requests when submitted by an authorized agent on behalf of a consumer. Apart from opt-out requests made through an opt-out preference signal, such as the Global Privacy Control (GPC), covered businesses may generally require authorized agents to provide the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on their behalf when submitting a privacy request. For requests to know, correct and delete, businesses **also** may require that the consumer either verify their own identity directly with the business, or directly confirm with the business that they provided the authorized agent with permission to submit the request (unless a consumer has provided the authorized agent with power of attorney pursuant to the California probate code). However, this is not permissible for opt-out requests and SPI requests.

Honda required consumers to directly confirm that they had given their authorized agent permission to submit an opt-out request or SPI request on their behalf. In addition to only requiring information necessary to identify the consumer (see above), the order required Honda to stop reaching out to consumers directly for confirmation (which also means that Honda's web form must request the contact information of the authorized agent and not just the consumer).

3. Even for consumer requests to access, correct or delete personal information, businesses cannot require more information than necessary to verify a consumer's identity.

When verifying a consumer's identity, the CCPA requires covered businesses to consider a number of factors enumerated in the law and, if feasible, match the identifying information provided by the consumer to personal information already maintained by the business.³ Businesses must avoid collecting more information than necessary,⁴ and collecting specific types or combinations of more sensitive information (including name and government identification number, such as driver's license or passport number) unless it is necessary to verify the consumer.⁵

The CPPA concluded that Todd Snyder was able to identify consumers without government identification. Therefore, requesting this information violated the CCPA's prohibition on collecting sensitive information where it is not necessary to verify the consumer and also "unlawfully ... discouraged [c]onsumers from submitting CCPA [r]equests."

Processing opt-out requests via cookie management tools

4. When relying on a cookie management tool as a method through which consumers can submit opt-out requests, a link to "Manage Cookie Preferences" must be included in the privacy center, privacy policy and in the footer of privacy policy web pages.

The CCPA allows covered businesses to provide a single "Alternative Opt-Out Link" (which may be called "Your Privacy Choices" or "Your California Privacy Choices"), instead of posting separate "Do not sell or share my personal information" and "Limit the Use of My Sensitive Personal Information" links. This single link must direct consumers to a web page that informs them of their rights to opt out of sales/sharing and to limit use of personal information, and allows them to exercise both rights.

Honda included a "Your Privacy Choices" link in the footer of its websites, which took consumers to the company's online privacy center for submitting all types of privacy requests, including opt-out requests and SPI requests. Honda separately had a cookie management tool that allowed website visitors to opt out of certain categories of cookies (specifically, performance, functional and advertising cookies) in a "Manage Cookie Preferences" pop-up. The CPPA recognized Honda's cookie management tool (and specifically the ability of consumers to turn off "advertising cookies") as "a method through which [c]onsumers can submit their [opt-out request]," despite the fact that the pop-up did not explicitly address the sale or sharing of personal information. For background, the CCPA regulations state:

A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.⁶

Moreover, if opt-out requests submitted through the cookie management tool only allowed consumers to opt out of sales and sharing related to targeted advertising on the websites, while those submitted through Honda's privacy center allowed consumers to opt out of other sales and sharing of their personal information, then consumers would need to submit two separate opt-out requests to fully opt out of sales and sharing. This may explain why the CPPA in its order required Honda to include the link to

"Manage Cookie Preferences" within its privacy center, privacy policy and in the footer of its privacy policy web pages.

5. Companies must validate that their cookie management tools are properly configured and functioning as intended.

Todd Snyder also sold and/or shared personal information related to targeted advertising on its website and advised consumers to submit opt-out requests related to such sales and sharing by visiting the cookie preferences center in their website footer. However, according to the CPPA, the company's opt-out mechanism wasn't properly configured for 40 days in late 2023, so when consumers clicked the cookie preferences center link, a cookie banner appeared on the side of their screen but instantaneously disappeared, preventing them from submitting an opt-out request. This also meant that opt-out requests submitted through GPC weren't honored during this period.

In addition to requiring Todd Snyder to ensure its cookie management tools are properly configured to comply with opt-out requests, the order requires the company to develop, implement and maintain procedures to identify all sales and sharing of personal information, along with policies, procedures and technical measures to assess the effectiveness and functionality of its methods for submitting opt-out requests.

'Dark patterns' in cookie management tools

6. Cookie management tools must provide symmetrical choices for opting into and opting out of cookies and similar tracking technologies.

The CCPA regulations require covered businesses to:

[D]esign and implement methods for submitting CCPA requests that are easy to understand, provide symmetry in choice, avoid language or interactive elements that are confusing to the [c]onsumer, avoid choice architecture that impairs or interferes with the [c]onsumer's ability to make a choice, and are easy to execute.

As explained in the regulations, a choice is not symmetrical if "the path for a [c]onsumer to exercise a more privacy-protective option [is] longer or more difficult or time-consuming than the path to exercise a less privacy-protective option."⁸ The regulations contrast examples of unsymmetrical or unequal choice (e.g., when the business's process for opt-out requests takes more steps than the process to opt back in) and compliant examples (e.g., a website banner that offers choices to "Accept All" or "Decline All" and a process to opt in to the sale of personal information that gives the choices of "yes" and "no").⁹ These requirements were specifically highlighted in the CPPA's [enforcement advisory on avoiding dark patterns](#), published in September 2024.

The CPPA took issue with Honda's "fail[ure] to provide symmetrical choice" in its cookie management tool, since consumers could accept all cookies with one click (by clicking "Confirm My Choices," as all categories of cookies were toggled on by default). But, if consumers wanted to opt out of cookies, they would need to toggle off each category (performance, functional and advertising) and then click "Confirm My Choices." In addition, a consumer could opt back in to cookies after previously opting out by either toggling each category back on and clicking "Confirm My Choices," or clicking "Allow All," which would then close the "Manage Cookie Preferences" pop-up.¹⁰ To address this lack of symmetry, the order requires Honda to include a "Reject All" button along with the "Allow All" button.

The CPPA recognized Honda's cookie management tool as a method through which consumers could submit opt-out requests, and therefore found that the CCPA's prohibition on dark patterns applies. However, the CCPA does not require covered businesses to provide the ability to opt out of cookies and similar third-party tracking technologies that do not involve the sale or

sharing of personal information (which would include many such technologies classified as performance and functional cookies, for example). Therefore, the Honda order suggests that companies subject to the CCPA must take care to avoid dark patterns **even where** providing opt-in and opt-out preference options is not required by the law.

Applying opt-out preference signals to known consumers

7. Global Privacy Control must be applied to known consumers.

The CCPA requires covered businesses to treat opt-out preference signals such as GPC as valid opt-out requests not only for the particular browser or device, but also for any consumer profile associated with the browser or device, as well as for the consumer, if known.¹¹ For example, if consumers create an account on a company's website, the company may be able to identify logged-in consumers who submit opt-out requests via GPC. Where consumers can be identified, covered businesses must opt out the consumer from all sales and sharing, and not just sales and sharing in the targeted advertising context tied to the consumer's device and/or browser. This is typically much more challenging than just opting the consumer out of targeted advertising-related sales/sharing.

Though the CPPA did not allege noncompliance with the CCPA's requirement to treat GPC as a valid opt-out request for known consumers in either case, both orders require the companies to apply GPC to known consumers as a remediation measure.

Contracts with adtech partners

8. Companies must ensure they have compliant contracts in place with adtech partners to whom they sell or share personal information.

The CCPA requires covered businesses to ensure they have contracts in place with "service providers," "contractors" and "third parties" to whom they disclose, sell or share personal information, which must contain certain specific terms.

While according to the order, Honda sold and/or shared with adtech companies personal information collected from visitors to its websites, the company was unable to provide contracts with these adtech companies. As a result, the order requires the company to put in place compliant contracts and more generally to modify its contract management and tracking process to ensure that all required contractual terms are in place with all external recipients of personal information. Even though the CPPA made no allegations related to deficient contracts in the case of Todd Snyder, that order also requires Todd Snyder to maintain a contract management and tracking process to ensure required contractual terms are in place with all external recipients of personal information.

Given the nature of digital advertising and the complex data flows involved, it is often difficult for advertisers to negotiate or execute contracts with all recipients of personal information (or even to track all of these data flows and recipients). The [Multi-State Privacy Agreement](#) of the Interactive Advertising Bureau automatically establishes contractual relationships among advertisers, agencies, adtech vendors and publishers who sign onto the agreement, which provides a potential solution to this problem.

General requirements related to consumer requests

In addition, the orders require the companies to make the following changes generally related to consumer privacy request processes:

- **CCPA consumer request training** – Both companies must ensure that all personnel handling consumer privacy requests are informed of the CCPA's requirements. (This training is a CCPA requirement.)
- **UX designer** – While not required by the CCPA, the Honda order requires the company to consult with a user experience (UX) designer to help ensure that methods for submitting consumer privacy requests are “easy to use” and avoid “confusing” language and interactive elements.
- **Consumer privacy request metrics** – The Honda order also requires the company to annually post CCPA consumer privacy request metrics to its website for at least the next five years. It is unclear whether Honda would otherwise be required to comply with the CCPA regulations mandating these disclosures, which only apply to businesses that “alone or in combination, buy[], receive[] for the business’s commercial purposes, sell[], share[], or otherwise make[] available for commercial purposes the personal information of [10 million] or more consumers in a calendar year.”¹²

Conclusion

The CPPA has hit its stride as a CCPA enforcement authority alongside the California attorney general. Recent enforcement actions likely reflect a “new normal” in the regulatory environment, with similar enforcement actions to follow going forward. The CPPA’s recent enforcement advisories broadcast that its areas of focus include the prohibition on the use of dark patterns and data minimization requirements, and the orders discussed above show the CPPA is looking for companies to be totally CCPA-compliant, including with the law’s more difficult or technical requirements. Now is the time for companies to assess their CCPA compliance or risk facing six-figure fines and above-and-beyond requirements. The scrutiny that the CPPA is placing on areas of widespread noncompliance sends a clear signal: comply or beware.

Cooley associate Emma Plankey also contributed to this alert.

Notes

1. Honda Stipulated Final Order at p. 5.
2. California Privacy Protection Agency, Enforcement Advisory No. 2024-01 at p. 1.
3. Cal. Code Regs. tit. 11, § 7060(c)(1), (3).
4. Id. at § 7002(d)(1).
5. Id. at § 7060(c)(2).
6. Id. at § 7026(a)(4).
7. Id. at § 7004.
8. Id. at § 7004(a)(2).
9. Id.
10. Note, however, that the regulations specifically require “a two-step opt-in process” for opting in to sales/sharing of personal information after having previously opted out, “whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in” 7028(a).
11. Cal. Code Regs. tit. 11, § 7025(c)(1).
12. Id. at § 7102.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as “Cooley”). By accessing this content, you agree that the information provided does not constitute

legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our [AI Principles](#), may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Kristen Mathews New York	kmathews@cooley.com
Claire M. Gibbs Washington, DC	cmgibbs@cooley.com +1 202 776 2125

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.