Articles + Publications | October 23, 2025

7 Lessons From The Tractor Supply CCPA Enforcement Action

WRITTEN BY

Sadia Mirza | David J. Navetta | Ronald Raether, Jr. | Bianca Nalaschi

This article was originally published on Law360 and is republished here with permission as it originally appeared on October 23, 2025.

On Sept. 30, the California Privacy Protection Agency **announced** its latest enforcement for alleged violations of the California Consumer Privacy Act — In the Matter of Tractor Supply Company.

This action targeted the nationwide retailer, Tractor Supply, resulting in a $1.35 million fine and a mandate to further cultivate certain parts of its privacy compliance program.

Regulatory decisions like this can offer valuable lessons, especially in the field of privacy. This case provides businesses with critical insights into what they can anticipate from an enforcement perspective in the coming months, including factors that might render a company a prime target.

It also emphasizes the compliance areas that remain a priority for the California regulator, offering businesses key issues to monitor when evaluating their own programs and suggesting avenues for improvement.

Such decisions, often an underutilized source of guidance, help navigate a legal landscape that frequently appears to be in flux. So, what does the Tractor Supplier action imply?

1. Retailers and businesses with significant consumer interactions remain in the spotlight.

Since the CCPA took effect in 2018, the California attorney general and the CPPA have initiated nearly a dozen enforcement actions.

They have predominantly targeted retailers, data brokers, and other businesses characterized by high consumer interaction and data processing, such as hospitality, travel, food delivery platforms and vehicle manufacturers.

As businesses develop their compliance programs, they should assess how they interact with consumers, including the volume and sensitivity of the consumer data they process. Companies with significant consumer engagement, like retailers, are likely to remain under scrutiny. If the business operates in other high-touch consumer sectors, such as hospitality or travel, the risk profile is similarly elevated.

With this in mind, remember that when crafting disclosures and implementing your compliance program, your

audience isn't just consumers — it is likely inquisitive regulators as well.

Businesses should consider how their privacy practices will look to regulators from the outside, what they want regulators to understand about their compliance efforts, and whether these issues can be effectively addressed through their disclosures. For instance, does the business primarily handle publicly available data? Do its opt-out mechanisms cover all types of selling or sharing, or do consumers need to take additional steps?

Recognizing that regulators are likely to scrutinize these disclosures and related workflows, businesses should anticipate the questions regulators might have and take proactive steps to address them.

2. The role of the 30-day cure period continues to diminish.

The financial penalty in this case underscores the fact that the 30-day cure period, initially available when the law was first enacted, is no longer a guaranteed right for businesses.

The CPPA acknowledged and credited Tractor Supply for its remediation efforts, noting that since becoming aware of the investigation in 2024, the company had significantly revised its practices, addressed numerous issues, and allocated substantial financial resources to rectify the shortcomings identified in the final order.

Despite these efforts, Tractor Supply was fined $1.35 million.

Previously, when the cure provision was in effect, Tractor Supply might have avoided a fine altogether. Five years later, however, businesses should not expect the cure period to be their saving grace. Instead, they should proactively consider their compliance strategies and be ready to present a convincing narrative that demonstrates their good faith efforts to comply with the law.

3. Consumer complaints help regulators identify potential targets.

Businesses should be aware that both the California attorney general and the CPPA have mechanisms in place for consumers to file complaints if they believe their privacy rights have been violated.

These complaints can be submitted through dedicated portals provided by the CPPA and the attorney general, which request detailed information about the complaint, the rights allegedly violated, supporting materials (such as screenshots of emails or interactions), and whether the consumer has already contacted the business.

Often, consumers will first reach out directly to businesses to resolve their concerns. This initial contact is a critical opportunity for businesses to de-escalate the situation before it potentially escalates. Tractor Supply, for example, became the focus of regulatory attention due to a consumer complaint submitted through these channels.

When responding to consumer complaints, it is important to implement strategies that attempt to effectively calm and resolve issues internally. This involves clear communication, understanding the consumer's perspective, and offering sometimes creative solutions.

Remember that when interacting with consumers, your audience includes regulators, as your communications

may be forwarded to them. Consider what language you would want included if a regulator were to review it later and draft it to clearly convey a narrative of robust compliance and a commitment to prioritizing consumer interests.

4. Tracking technologies remain a priority item for enforcement.

Many enforcement actions under the CCPA have centered around online tracking technologies, and the Tractor Supply case is no exception.

In the stipulated final order, the CPPA identified five violations, two of which involved the use of tracking technologies. The first of these related to effectuating opt-out requests. More specifically, the stipulated order indicated that the retailer's website employed cookies and tracking technologies that were deemed sales and shares of personal information under the CCPA.

Although the website featured a "Do Not Sell My Personal Information" link directing users to a webform to opt out, the process was allegedly flawed. Consumers who completed the webform were not successfully opted out. The webform also allegedly failed to inform consumers where or how they could opt out of Tractor Supply's selling or sharing of personal information through tracking technologies.

The second issue identified related to opt-out preference signals. The order noted that the retailer did not configure its website to honor consumers' requests to opt out of sharing or sale using an opt-out preference signal until July 2024. The retailer's privacy policy also allegedly lacked clarity on how such opt-out signals would be handled.

Businesses should view the Tractor Supply decision as an opportunity to assess their compliance with the CCPA's right-to-opt-out provision.

Businesses that sell or share personal information and are regulated by the CCPA generally must implement at least two opt-out mechanisms. These mechanisms should effectively address the specific type of selling the business engages in. For example, if personal information is shared through cookies, businesses should evaluate whether a webform allowing consumers to opt out of sharing will genuinely affect the disclosure made through their tracking technologies.

Businesses collecting personal information online that sell or share such information are also generally required to configure their websites to honor consumers' requests to opt out of sharing or selling using an opt-out preference signal. While this requirement does not apply to all businesses — depending on specific selling or sharing practices — it is prudent to reassess whether this should be part of a business's compliance program.

5. Regulators are expanding focus beyond service provider contracts.

Initially, when the CCPA was enacted, businesses concentrated on updating vendor contracts to implement service provider terms.

However, the Tractor Supply settlement underscores the importance of extending this focus to include third parties, such as advertising technology partners, with whom personal information may be sold or shared.

The CPPA made a point to highlight that contracts with both service providers and third parties must:

- Specify the limited and defined purposes for processing or disclosing consumers' personal information;
- Ensure that consumers' personal information is used solely for those specified purposes; and
- Require the contracting party to comply with the CCPA, thereby providing the same level of privacy protection required of regulated businesses under the CCPA.

In practice, many terms governing advertising technology partners may seem nonnegotiable, as businesses often lack negotiating power. Nevertheless, it is important to inventory the applicable terms and assess their alignment with CCPA requirements.

Some advertising partners may offer specific terms only upon request. Consider conducting an inventory of your tracking technologies, identifying the governing terms, and reviewing them to pinpoint potential gaps.

6. California continues to plow forward with regulating employee data.

California distinguishes itself as the sole state to incorporate employee-related data within the scope of its privacy law. Despite this unique position, the settlement with Tractor Supply highlights California's commitment to uphold this aspect of the CCPA, even as other states have yet to follow suit.

For businesses with a substantial presence in California and a large workforce in the state, this could result in heightened scrutiny.

It is worth noting that California also regulates certain personal information collected in the business-to-business context, a domain other states have not ventured into. While B2B data typically consists of less sensitive information, such as basic contact details, the recent focus on employee data suggests that B2B data may soon receive similar attention.

7. Businesses need to recognize and remediate the low-hanging fruit.

The CCPA has been in effect for five years. Businesses that are perceived as meeting the CCPA's applicability thresholds but have not taken steps to comply should anticipate attracting regulatory attention.

While compliance can be complex and sometimes seem like a moving target, demonstrating a good faith effort to adhere to the law is essential. If a business has not updated its privacy compliance program since before the CCPA's implementation, it will face difficulties justifying its compliance strategy when regulators inquire.

As California continues to lead in enforcing its state privacy law, other states like Oregon are ramping up their efforts, conducting sweeps and inquiries to assess compliance and identify areas where businesses may fall short. In this collaborative regulatory environment, it is important to remember that state privacy regulators communicate regularly.

Thus, even if you are dealing with one state regulator, it is quite possible that others may be quietly observing. Leveraging any inquiry you receive to demonstrate your commitment to adhering to all applicable privacy laws can

not only address the specific state's concerns but also enhance the business's reputation among regulators in other jurisdictions.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber