Lessons Learned 3 Years After First CCPA Enforcement Action

By **Tatum Andres** (August 20, 2025)

Tatum Andres

Aug. 24 marks the three-year anniversary of California Attorney General Rob Bonta's first public enforcement action under the California Consumer Privacy Act: a $1.2 million settlement with beauty retailer Sephora.

Since that landmark case, Bonta has pursued a steady stream of enforcement actions across industries, targeting companies that fail to comply with the CCPA's requirements for collecting, sharing and disclosing consumer personal information. Three years in, a clearer picture has emerged of how the law is being interpreted and enforced, and what that means for businesses moving forward.

Most recently, on July 24, the California Privacy Protection Agency Board held a public meeting to finalize proposed amendments to existing CCPA regulations and discuss new rules implementing the Delete Request and Opt-Out Platform, or DROP. These actions build on the enforcement trends of the past three years and significantly raise the bar for businesses still working to meet their compliance obligations.

Understanding these developments and how we got here is essential for any company seeking to stay ahead of regulatory expectations.

The Sephora Case: Setting the Tone

The Sephora enforcement action remains one of the most instructive examples of how the California attorney general is interpreting and applying the CCPA. In connection with the Aug. 24, 2022, settlement, Bonta alleged that Sephora:

- Did not disclose that it was selling personal information;
- Did not honor global privacy control signals; and
- Did not have valid service provider agreements in place with each party that collected personal information through Sephora's website or mobile app.

In addition to monetary penalties, Sephora was required to:

- Update its privacy disclosures to affirmatively state that it sells personal information;
- Implement and honor opt-out signals sent via global privacy control;

- Ensure its service provider contracts included the provisions required under the CCPA; and

- Submit ongoing compliance reports to the attorney general.

Although the facts were specific to Sephora, the settlement provided a broader warning to businesses about the importance of transparency, opt-out functionality and contractual compliance.

Broader Enforcement Trends Since Sephora

Since the Sephora case, Bonta has continued to pursue enforcement actions across a range of industries. While the specific facts vary from case to case, several recurring themes have emerged as common grounds for enforcement, including:

- Collecting or sharing personal information for targeted advertising or analytics without proper notice or opt-out rights;

- Failing to honor opt-out signals sent via global privacy control;

- Using cookie banners or interfaces that mislead consumers about their ability to opt out;

- Lacking service provider contracts that meet the CCPA's legal requirements;

- Sharing children's personal data without proper parental or affirmative consent; and

- Using personal information for purposes inconsistent with the original disclosures

In many of these cases, Bonta has secured injunctive relief in addition to financial penalties, requiring businesses to clarify its online disclosures, conduct internal audits and enhance contract oversight.

These enforcement actions offer valuable insight into how the CCPA is being interpreted in

practice. They also reflect the areas where the attorney general is focusing his attention, including opt-out rights, service provider relationships, children's privacy and financial incentive disclosures.

The following sections outline several key themes that have emerged and highlight practical steps businesses can take to align with regulatory expectations.

The right to opt out remains central.

One of the most consistently cited issues in enforcement actions is failure to comply with the CCPA's opt-out framework.

Under the CCPA, consumers have the right to opt out of:

- Sales of personal information, defined broadly to include disclosures for monetary or other valuable consideration; and

- Sharing of personal information for purposes of cross-context behavioral advertising, regardless of monetary value.

To comply, businesses must:

- Provide an opt-out mechanism such as a "Do Not Sell or Share My Personal Information" link;

- Honor opt-out requests sent via global privacy control; and

- Ensure that service provider contracts include the required restrictions to avoid classification as a sale or sharing.

Privacy disclosures must match reality.

The CCPA requires businesses to provide consumers with clear and detailed privacy policies. These policies must identify the categories of personal information collected, the purposes for which the information is used — also known as the purpose limitation principle — and whether any of that information is sold or shared.

In a July CCPA enforcement action, The People of the State of California v. Healthline Media LLC, in the Superior Court of the State of California, County of San Francisco, Bonta targeted Healthline for failing to clearly disclose its data-sharing practices. According to the complaint, Healthline shared personal information that could potentially reveal health-related information — e.g., article titles that may suggest an individual reader's medical condition — with third-party advertisers.

While Healthline's privacy policy stated it "may provide [consumers'] information to advertising providers for purposes of targeted advertising," it did not mention article titles. As a result, Healthline could not establish that consumers reasonably expected that Healthline would share potentially health-related data, as the purpose limitation principle requires.

Children's data demands extra care.

Businesses that knowingly collect personal information from children under the age of 16 are subject to heightened consent requirements under the CCPA. Businesses can only sell the personal information of a child that they know to be under the age of 16 if they get affirmative authorization for the sale of the child's personal information.

For children under the age of 13, that opt-in must come from the child's parent or guardian. For children who are at least 13 years old but under the age of 16, the opt-in can come from the child.

In an enforcement action from June 2024, The People of the State of California v. Tilting Point Media LLC in the U.S. District Court for the Central District of California, Tilting Point was found to have collected personal information from children without obtaining the required opt-in consent. The issue stemmed in part from the design of its age gate, which was not neutral and did not encourage users to accurately report their age.

Additionally, the company had misconfigured software development kits that resulted in data sharing with third parties. The June 2024 resolution required the company to reconfigure its software development kits, implement neutral age-screening mechanisms, and provide just-in-time notices that clearly explain when and why the child's data is collected and shared.

Financial incentives trigger disclosure duties.

The CCPA allows businesses to offer discounts, loyalty rewards or other incentive programs in exchange for the collection or retention of personal information. However, companies must first provide consumers with a notice of financial incentive that describes the material terms of the incentive program's offer.

If a consumer asks a business to delete or stop selling their personal information, and that information is essential to participating in the incentive program, the business may no longer be able to provide such incentives to the consumer. However, companies must ensure that consumers are not penalized simply for exercising their CCPA rights.

By way of example, if a customer joins a company's incentive program and agrees to share her purchase history in exchange for a 10% discount, the company must provide a notice of financial incentive explaining the incentive program's offer and the value of her data. If the customer later opts out of data sharing, the company can inform her that she will lose the discount but cannot otherwise penalize her for exercising her rights.

The attorney general has not brought as many public enforcement actions in this category, but it remains an area of risk, especially for companies that offer digital rewards or targeted incentives tied to data collection.

The CPPA Signals Its Next Enforcement Priority: Data Brokers

On July 24, the CPPA Board held a public meeting to advance proposed amendments to the CCPA regulations and to consider the implementation of the DROP requirements for data brokers.

While the proposed CCPA regulations regarding automated decision-making technology, risk assessments, cybersecurity audits and insurance were finalized, the CPPA Board opted to revisit and refine the proposed DROP regulations.

The Rising Focus on Data Brokers

This meeting confirmed the CPPA's increasing focus on data brokers. A data broker is a business that buys and sells information about consumers from other businesses, but consumers do not directly interact.

For example, a consumer might sign up for a meal delivery app. A data broker could purchase a list of recent sign-ups of that meal delivery app and sell it to a kitchen appliance company looking to target potential customers. The consumer never interacts with the data broker, but their information is bought and sold regardless.

This type of data exchange has become a major concern for regulators. The DROP platform and related rules, described below, reflect a broader trend toward improving consumer control and holding data brokers more accountable.

Background: The California Delete Act

The California Delete Act, signed into law on Oct. 10, 2023, introduced a new set of compliance requirements for data brokers operating in the state. Among other changes, the law:

- Requires all data brokers to register annually with the CPPA;
- Expands transparency obligations, including detailed public reporting on privacy request handling; and
- Creates a centralized deletion mechanism, or DROP.

The DROP platform is intended to simplify the consumer experience by allowing a single, verifiable deletion request to apply to all registered data brokers. The CPPA expects to launch DROP by Jan. 1, 2026, and data brokers will be required to begin checking the system regularly starting Aug. 1, 2026.

At a minimum, they must review the platform once every 45 days.

CPPA Board Meeting Highlights

During the July meeting, the CPPA Board chose not to adopt the DROP regulations in their current form. Instead, it opened a new 15-day public comment period to consider several proposed modifications. Key updates include:

Clarifying Suppression List Requirements

The Delete Act requires data brokers to delete all personal information associated with a DROP request. This includes inferences drawn from data collected from third parties or through indirect means.

However, brokers must retain the minimal information necessary to comply with DROP requests. This record, referred to as a suppression list during the meeting, helps ensure the broker does not reintroduce deleted individuals into its data systems.

The proposed revisions would also allow brokers to share this suppression list with their service providers and contractors. This measure is intended to prevent repopulation of personal data that was already subject to deletion.

Verification of California Residency

As currently written, consumers may need to have their California residency verified by the CPPA before submitting a DROP request. The revised approach would shift the full responsibility for verification to the CPPA. Once a request is verified, data brokers would be obligated to honor and process it accordingly.

Future Compliance Requirements and Milestones

The Delete Act includes several other long-term compliance obligations.

Annual Reporting

Data brokers must publish metrics on the number of consumer privacy requests they receive, fulfill (in full or in part) or deny. They must also disclose the average and median number of days it takes to respond to these requests.

Third-Party Audits

Starting Jan. 1, 2028, all data brokers must undergo an independent audit every three years to evaluate compliance with applicable privacy laws. And beginning Jan. 1, 2029, data brokers will be required to disclose whether they have completed an audit, specify the year of the most recent audit, and confirm whether the audit materials were submitted to the CPPA.

Additional Technical Considerations Under Review

The CPPA is also evaluating technical issues and implementation details related to DROP, including:

Data Matching Standards

The CPPA is working on clarifying how data brokers should compare consumer-submitted

data to their internal records. If a request matches multiple profiles, the broker may be required to opt out of selling or sharing the data rather than deleting it outright.

Audit Mechanisms

The board is developing methods to confirm whether data brokers have properly deleted personal information.

Preimplementation Testing

Data brokers are being allowed to test hashing and other technical methods before enforcement on Aug. 1, 2026.

Final Thoughts

Three years after the Sephora enforcement action, it is clear that CCPA enforcement is active and evolving. Bonta continues to prioritize transparency, consumer choice and accountability. Meanwhile, the CPPA is expanding the regulatory framework, further shaping how businesses must operationalize compliance.

Now is the time for companies to reassess data practices, review contracts, verify opt-out mechanisms and update privacy policies. With DROP launching in 2026 and audits beginning in 2028, data brokers especially should prepare for increased scrutiny. Taking these steps today can help avoid costly enforcement tomorrow.

Practical Compliance Steps

Opt-Out Mechanisms

Display a prominent "Do Not Sell or Share My Personal Information" link wherever personal data is collected, ideally in a clear pop-up or banner that also links to your business's privacy policy. Ensure your systems are configured to honor global privacy control signals and routinely test opt-out functionality across devices and browsers.

Privacy Policy

Limit data collection and use to the purposes disclosed at the time of collection and within the consumer's reasonable expectations. Reassess disclosures when launching new products or engaging new vendors. The Federal Trade Commission has recently scrutinized whether sharing customer browsing history with third parties aligns with consumer expectations, underscoring the importance of transparency.

Provide clear notice of material changes to the privacy policy through pop-ups or direct email communications.

Cookie Practices and Tracking Technologies

Do not activate session replay tools or some nonessential cookies before obtaining user consent. Clearly categorize cookies (e.g., strictly necessary, functional, analytics, advertising) and implement a cookie banner that includes "Accept" and "Reject" options, along with granular controls that allow users to manage preferences by category.

Vendor Contracts and Data Subject Rights

Set clear service-level agreement terms requiring your vendor to help you meet legal deadlines for responding to data subject access requests.

Children's Data Collection

Use neutral age gates that do not encourage misreporting. Implement just-in-time notices in child-directed services. Do not sell or share the personal information of users under 13 without parental consent, and do not sell or share the personal information of users at least 13 and less than 16 years old without the consumer's affirmative opt-in consent.

Data Brokers

If your business meets the definition of data broker, you should prepare for the launch of the DROP platform by Jan. 1, 2026. You will be required to review and honor deletion requests submitted through the system beginning Aug. 1, 2026. In the meantime, continue monitoring for upcoming rules on suppression lists and verification of California residency expected later this year.

Tatum Andres is an associate at Kilpatrick Townsend & Stockton LLP.