CCPA ENFORCEMENT HEATS UP: WHAT THE LATEST FINES AGAINST HONDA, TODD SNYDER AND DATA BROKERS SIGNAL FOR THE FUTURE OF CONSUMER PRIVACY COMPLIANCE

by Trina L. Glass, Esq. and Shade Oladetimi, Esq.

Enforcement on the Rise: What the CPPA is Prioritizing

On May 6, 2025, the California Privacy Protection Agency Board ("CPPA") issued a $345,178 penalty against national retailer Todd Snyder, Inc. ("Todd Snyder") for violations of the California Consumer Privacy Act and its implementing regulations ("CCPA"). This marks the second major enforcement action this year by the CPPA and follows a significant $632,500 fine imposed on American Honda Motor Co. ("Honda") in March. Taken together, these cases offer more than just monetary figures—they reflect a new era of privacy accountability and serve as a wake-up call for companies that collect and process consumer data in California.

The Honda Case: Connected Cars, Disconnected Compliance

In March 2025, **the CPPA Board found that Honda** had created unnecessary obstacles for consumers trying to exercise fundamental privacy rights. The agency cited several violations:

- Requiring excessive personal data—ironically, including sensitive information—to verify identity for simple opt-out of the sale and or sharing of their personal data or data limitation requests.
- Using an online privacy tool that failed to offer consumers their choices in a clear, equitable manner. Obstructing authorized agents or other third parties from acting on behalf of consumers.
- Obstructing authorized agents or other third parties from acting on behalf of consumers.
- Sharing consumer personal data with ad tech companies without the contractual safeguards required by the CCPA.

In response, Honda agreed to overhaul its privacy processes, train employees, and engage user experience specialists to ensure compliance. The message - data privacy design must be consumer-centric and functionally transparent.

The Todd Snyder Case: Misconfigured Tools and Misguided Demands

On May 6, 2025, the **CPPA Board reached a settlement with a national clothing retailer, Todd Snyder,** over allegations that the company's opt-out and other privacy request processes did not comply with the CCPA. Specifically, the CPPA Board found that Todd Snyder violated the CCPA by:

- Failing to oversee and configure properly the technical infrastructure of its privacy portal, resulting in a failure to process consumer requests to opt out of the sale or sharing of personal information for forty days;
- Requiring consumers to submit more information than necessary to process their privacy requests; and
- Requiring consumers to verify their identity before they could opt–out of the sale or sharing of their personal information.

Todd Snyder's enforcement story is a cautionary tale about the dangers of outsourcing privacy obligations without verification. According to the CPPA, the company's opt-out portal was misconfigured for forty days, effectively disabling consumers' ability to reject data sharing. Worse, even when privacy requests were submitted, users were forced to upload government IDs—including driver's licenses and passports—just to exercise their rights. This was not only intrusive but unnecessary. Consumers could shop on the retailer's website with minimal personal information, but asserting their privacy rights required handing over sensitive identity documents. The CPPA characterized this as both disproportionate and potentially discouraging, noting that such practices could deter consumers from exercising their rights due to fear of identity theft.[1]

Data Brokers Beware: CPPA Targets Jerico Pictures, Inc. in Data Broker Enforcement Action

In February 2025, the CPPA announced **an enforcement action against Jerico Pictures, Inc.**, dba National Public Data, a Florida-based data broker ("Jericho Pictures"). The CPPA alleged that the company failed to register in a timely manner under **California's Delete Act** ("Delete Act"), which requires data brokers to register annually and pay a fee[2]. According to the CPPA, Jerico Pictures registered 230 days late, only after being contacted by the agency's Enforcement Division during an investigation. The CPPA is seeking a $46,000 fine in connection with the violation.

1 In 2024, the CCPA issued a warning, about improper verification, **CPPA Enforcement Advisory**, warning businesses against collecting excessive information from consumers asserting their privacy rights.

2 Effective January 1, 2026, the Delete Act will also require data brokers to undergo an independent audit once every three years to verify compliance.

This enforcement action follows a prior claim brought by the CPPA in October 2024 in the U.S. Bankruptcy Court for the Southern District of Florida, in which the agency alleged that Jerico Pictures failed to pay a previous registration-related administrative fine. The February action is part of a broader crackdown—since October 2024, the CPPA has initiated enforcement against five other data brokers, resulting in settlements and public scrutiny.

While Jerico Pictures has not publicly contested the allegations, the company has reportedly taken steps to improve its internal compliance procedures in light of the action. The case serves as a stark reminder to other organizations of the growing pressure to align with California's aggressive privacy enforcement regime.

Key Takeaways for Businesses:

Opt-Out Mechanisms Must Be Reliable
Whether built internally or outsourced to vendors, opt-out tools must function seamlessly. Regular testing, monitoring, and timely fixes are critical. Businesses cannot shield themselves behind third-party failures.

Keep Privacy Requests Proportionate
Companies should only collect the information strictly necessary to fulfill a consumer's request. Verification for opt-out requests is rarely justified and must be used with caution.

Privacy Compliance Is a Design Imperative
The CPPA's directive for Honda to consult UX designers signals a shift: privacy isn't just a legal checkbox—it's a product and design issue. Interfaces must be intuitive, user-friendly, and fair.

Do Not Wait for a Regulator to Come Knocking
Compliance must be proactive. Late action—even if eventually corrected—can still carry steep penalties and reputational risk.

Deadlines Matter
The Delete Act requires data brokers to register annually—on time. Missed deadlines, even if unintentional, can trigger daily fines and enforcement action.

Vendor Tools Aren't a Compliance Strategy

Third-party tools must be actively managed. Regulators expect businesses to understand, monitor, and validate the performance of any tool used for privacy compliance.

Avoid Dark Patterns

Confusing or misleading interface designs that frustrate user choice—commonly known as dark patterns—are now fair game for enforcement. Simplicity, clarity, and accessibility should drive all consumer privacy interactions.

Data Minimization Is the Default

Collect only what's necessary—nothing more. Excessive or invasive data collection, particularly during privacy rights requests, can violate legal obligations and erode consumer trust.

Looking Ahead: Privacy Enforcement Has Arrived—and it's Escalating

The CPPA's enforcement actions in 2025 reveal a powerful shift: California is not just shaping privacy laws anymore—it is rigorously enforcing them. Six-figure fines, public scrutiny, and mandatory operational changes are now very real consequences for non-compliance. Businesses that fail to align with the spirit and intent of the law now face six-figure fines, public scrutiny, and significant reputational damage. As regulators across the country and the world look to California's model, these cases are quickly becoming a benchmark for global compliance expectations.

For organizations operating in California and beyond, the message is undeniable: embed privacy into the core of your business. Compliance is no longer just a legal requirement; it is a trust signal, a brand differentiator, and increasingly, a market expectation. Proactive, user-centered privacy compliance is not optional, it is the new baseline.

*For additional information on the CCPA, evolving privacy requirements, or recent enforcement actions, please contact **Trina L. Glass, Esq.** and **Shade Oladetimi, Esq.**, or visit **www.burghergray.com**.*

BURGHERGRAY LLP
ATTORNEYS AT LAW

www.burghergray.com

1350 Broadway | Suite 1510
New York, NY 10018
T: 646.513.3231 | F: 646.561.9866
info@burghergray.com