Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

February 17, 2026

California Attorney General Secures Record CCPA Settlement: Cross-Device Opt-Outs Now a System-Level Obligation

Can your identity architecture honor consumer choice across platforms, devices, and advertising ecosystems?

By Amy S. Mushahwar and Tricia Y. Wagner CIPP/US, CISSP, CISA

The California Attorney General recently announced a $2.75 million settlement with The Walt Disney Co.—the largest enforcement action to date under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act. Beyond the monetary penalty, the order imposes structured remediation obligations, including 60-day compliance reporting checkpoints. Disney's remediation timetable is now under active regulatory examination.
The Attorney General's position signals a structural shift: If a business builds the capability to recognize consumers across devices, services, and advertising environments for monetization or analytics purposes, it must honor opt-out rights at that same operational scope. Recognition architecture and rights architecture must align.

For multichannel platforms, this reinforces what we have been counseling for years: Opt-out compliance is no longer an interface issue. It is an enterprise architecture issue embedded across the customer identity graph[1] and digital journey.
For legal and privacy teams, this enforcement shift means compliance assessments can no longer stop at policy language or user interface (UI) review. Legal risk now depends on how identity resolution, consent orchestration, and data activation systems are implemented in production, requiring a legal-technology fused review.

The Enforcement Theory: Identity Resolution Symmetry

The core issue was not the absence of opt-out mechanisms. It was architectural asymmetry.

According to the enforcement theory reflected in the settlement with The Walt Disney Co., consumers were recognized across devices and services for cross-context behavioral advertising, yet opt-out requests were implemented at a narrower scope, often limited to a specific device, browser, or interface. Meanwhile, opt-in recognition operated systemwide.

The result: A consumer could be linked across environments for monetization purposes, but their opt-out request did not propagate across those same linked systems. In regulatory terms, recognition and rights were not symmetrical.

Section 7004 of the amended CCPA regulations requires that user-enabled privacy controls be implemented in a manner that is symmetric between opt-in and opt-out mechanisms. The settlement clarifies that this obligation applies at the same operational level at which identity is resolved. If a company's architecture enables systemwide identity recognition, its rights implementation must operate at that same level.

For companies uncertain whether their systems can technically harmonize opt-outs across linked environments, the risk is no longer theoretical. Privacy implementation is now an engineering question subject to regulatory examination.

Alleged Operational Gaps Identified in the Settlesment

The settlement highlights several system-level issues that regulators view as high risk.

1. Fragmented Opt-Out Implementation

Opt-out requests submitted through one interface (e.g., a website or mobile application) were reportedly applied only to that specific service or device. For example, a consumer who opted out on an iPad could still have personal information sold or shared from the same account accessed through a laptop, mobile phone, or smart television. Where an account spanned multiple devices or services, data sharing could continue from linked environments unless a separate opt-out was initiated from each device.

The regulatory concern is not merely interface inconsistency. It is identity-layer inconsistency.

Modern platforms often resolve identity at multiple levels—deterministically (e.g., known authenticated login credentials, hashed email addresses, subscriber IDs) and probabilistically (e.g., inferred device fingerprints, IP address clustering, household modeling, inferred cross-device linkages). These identity techniques enable cross-context behavioral advertising and unified customer profiling across environments.

> Legal-Tech Translation Note:
>
> **Deterministic identity** = confirmed identity (login, account ID, hashed email)
>
> **Probabilistic identity** = inferred identity (device fingerprinting, IP clustering, behavioral modeling)
>
> Both create cross-device recognition.
> Recognition scope defines suppression scope.

Where identity is resolved at an account, household, or probabilistic cluster level for monetization purposes, regulators are signaling that opt-out suppression must operate at that same level of resolution, increasing the scope of the opt-out. This raises an unresolved but increasingly urgent compliance question: Where identity linkage is probabilistic rather than deterministic—for example, where a platform infers device association through IP address clustering, behavioral fingerprinting, or household-level modeling without explicit account authentication—does the symmetrical obligation extend to those inferred linkages? The settlement does not address this directly, but the enforcement logic points in one direction. If probabilistic identity resolution is sufficient to justify cross-device monetization, it may be difficult to argue that it is insufficient to trigger cross-device suppression. Organizations relying on probabilistic identity graphs should treat this as an area of material regulatory risk and consider whether their suppression architecture can operate at the same inferential scope as their targeting architecture.

For businesses leveraging centralized identity graphs or unified customer data platforms, or systems that connect email addresses, login credentials, device IDs, IP signals, advertising identifiers, cookie IDs, and subscriber IDs into a unified profile—the enforcement message is clear:

Account-level recognition implies account-level suppression.

2. Incomplete Suppression of Third-Party Advertising and Ad-Tech Partners

The Attorney General alleged that opt-out submissions halted certain internal advertising activities but did not fully propagate suppression to all third-party advertising and analytics technologies embedded across digital properties.

An opt-out mechanism that stops internal processing but fails to suppress downstream data flows to software development kits (SDKs), tracking pixels, ad exchanges, or analytics partners may still constitute continued “sale” or “sharing” under the CCPA. This risk is compounded by the industry’s ongoing migration from client-side to server-side data collection architectures. Many organizations have adopted server-side tag management, through platforms such as server-side Google Tag Manager, Segment Connections, or mParticle, to move data collection and transmission off the user’s device and onto the server infrastructure. In these architectures, a suppression signal that fires only at the client side, disabling a JavaScript tag or blocking a browser-based pixel, may have no effect on data flows that are already routed server-to-server before the opt-out signal reaches the collection layer. The result is an opt-out mechanism that appears functional in the user interface but is not effective. Personal information would continue to flow through server-side pipelines. For organizations operating hybrid or fully server-side architectures, suppression logic must be implemented at the server layer where data transmission occurs, not merely at the client-side tag layer that the consumer interacts with. This is a concrete example of why compliance cannot be evaluated solely by reviewing the front-end experience.

For organizations that have navigated consent revocation in other regulatory contexts, such as telemarketing, this issue is familiar, but the scale is not. Modern ad-tech ecosystems involve dozens of embedded technologies operating across web, mobile, connected television, and retail properties.

Complex ecosystems and layered privacy tools do not reduce compliance obligations. They increase architectural accountability. In environments where consumer segments, services, or business lines operate in technical silos, suppression failures can occur even when policies appear compliant.

The enforcement message is straightforward: Organizations must be able to demonstrate that their opt-out mechanisms propagate across internal systems and downstream partners or be prepared to document and assess the technical limitations as material compliance risk.

3. Functional Opt-Outs in Connected TV (CTV) and Space-Constrained Environments

In certain CTV applications, users were directed to external webforms rather than provided with a fully functional in-app opt-out mechanism. The Attorney General concluded that this approach did not effectively halt data sharing originating from the CTV application itself.

CTV and similar environments differ materially from web and mobile ecosystems. They typically do not support cookies, browser extensions, or Global Privacy Control signals. Remote navigation makes multistep form entry cumbersome. Screen constraints limit disclosures. Operating systems impose technical rendering limitations.

These are real engineering constraints. They are not compliance exceptions.

However, the regulatory message is clear: Form factor does not diminish obligation. If data flows out of a device, the opt-out must function on that device.

4. Global Privacy Control (GPC)[2] and Account-Level Propagation

GPC signals were reportedly honored only on the device transmitting the signal, even where the consumer was authenticated into a cross-device account spanning multiple environments.

The Attorney General emphasized that statutory opt-out rights apply “wherever and however” personal information is sold or shared. That framing carries significant architectural implications.

In environments such as CTV, which lack a browser layer and do not natively support GPC detection, the compliance analysis becomes more complex. If a consumer transmits a GPC signal from a browser while logged in to the same account used across mobile, web, and CTV applications, the enforcement theory reflected in the settlement suggests that the opt-out must propagate across the linked account, even where legacy infrastructure was not designed for cross-environment signal propagation.

In other words, GPC cannot be treated as a device-scoped preference where identity resolution operates at the account or household level.

At the same time, account- or household-level suppression may extend beyond the precise context in which the signal was transmitted, raising operational questions about scope, user intent, and over-suppression. These complexities do not eliminate the obligation; they underscore the need for deliberate architectural design and documented suppression logic.

For organizations operating unified account systems or centralized identity graphs, GPC requires account-level signal propagation infrastructure, not merely device-level detection. In practice, this requires a centralized preference management service, whether through a commercial consent orchestration platform or custom-built infrastructure, that operates as the authoritative source for opt-out state across all environments tied to a given identity. The preference service must be query able by CTV applications, mobile SDKs, and server-side systems at the point of data transmission, not merely at the point of user interaction. For most organizations, this infrastructure does not exist today. Building it requires integration between identity resolution systems, consent management platforms, and downstream advertising and analytics pipelines, a cross-functional engineering effort that cannot be led by legal or compliance teams alone.

Putting It All Together: What the Settlement Means for Multi-Platform Businesses

The Disney settlement reflects a broader regulatory evolution under the CCPA. To evaluate your organization, ask some key questions, including:

- Does identity resolution operate across devices?
- Does advertising activation operate across devices?
- Are suppression signals implemented at the same layer as monetization logic?
- Do third-party partners receive and honor opt-out signals consistently?
- Is testing performed to validate that suppression functions as designed?
- For CTV and constrained-environment platforms: Does the in-app opt-out technically suppress SDK-level and ad-tech data transmission, or does it merely update a UI preference?

If the answer to the first two questions is “yes,” but suppression is device-specific, risk exposure could increase at your organization.

Operational Takeaways for CCPA-Covered Organizations

Companies should consider the following structural steps:

- Adopt account-level opt-out governance. Where consumers interact through logged-in accounts, opt-out requests should apply across all associated devices, services, and affiliated environments.
- Inventory and map third-party data flows. SDKs, pixels, and embedded advertising technologies should be identified, documented, and incorporated into suppression workflows.
- Propagate suppression signals downstream, including at the server layer. Where data collection has migrated

to server-side architectures, opt-out logic must be integrated at the server-side pipeline level, not merely at the client-side tag or UI layer. A suppression mechanism that disables a browser pixel but leaves server-to-server data flows intact does not satisfy the CCPA's functional standard.

- Honor GPC signals consistently. GPC should be treated as a valid opt-out of sale/sharing and implemented in alignment with how identity and advertising systems function in practice.
- Validate functionality through testing. Organizations should test opt-out flows to confirm that suppression stops data sharing across environments.
- Build CTV and constrained-environment compliance into the product development life cycle. For platforms operating in space-constrained environments, opt-out functionality cannot be retrofitted as an afterthought. It must be designed into application architecture from the outset, with suppression logic integrated at the SDK and ad-tech layers rather than the UI layer. Product, engineering, privacy, and legal teams must collaborate to ensure that opt-out mechanisms are technically effective within each deployment environment, not merely available on a companion website.

A Shift From Interface Compliance to Architectural Accountability

The Disney settlement underscores a critical shift in CCPA enforcement.

Regulators are evaluating whether consumer rights operate at the same level of integration as the business's monetization infrastructure.

For organizations leveraging unified identity systems and cross-context behavioral advertising, opt-out compliance must be engineered at the same architectural layer.

If monetization is cross-device, compliance must be cross-device.

For multichannel platforms, streaming services, retail ecosystems, and advertising-supported models, this is not a minor compliance adjustment. It is a data governance design requirement.

---

[1] An "identity graph" is the data infrastructure that links disparate identifiers (such as cookies, device IDs, account logins, and hashed emails) to recognize a single consumer across platforms, services, and devices. The same architecture that enables cross-device monetization must, under emerging enforcement theories, also be capable of propagating consumer opt-out signals at equivalent scope.

[2] GPC is a standardized, browser-level opt-out signal that communicates a user's preference to opt out of the "sale" or "sharing" of personal information. The signal is transmitted automatically via HTTP header or JavaScript and is designed to operate as a persistent, frictionless alternative to individual opt-out webforms. California's CCPA regulations require businesses to process valid GPC signals as a recognized opt-out mechanism.
More information: https://globalprivacycontrol.org/

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data Privacy, Security, Safety & Risk Management
T: 202.753.3825
amushahwar@lowenstein.com

TRICIA Y. WAGNER CIPP/US, CISSP, CISA
Counsel
T: 202.753.3658
twagner@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.

APPENDIX

CCPA Enforcement Actions: Evolution in Enforcement Theory

From Privacy Choice Presence to Effectiveness

All seven enforcement settlements brought by Attorney General Rob Bonta under the California Consumer Privacy Act (CCPA) reflect an evolution in enforcement theory. Earlier actions focused primarily on whether opt-out mechanisms and disclosures existed at all, while later settlements evaluated whether consumer privacy choices were implemented effectively across systems, signaling the California Attorney General's shift from interface-level compliance to operational accountability.

#	ENTITY	DATE	PENALTY	HOLDING / KEY VIOLATIONS
1	**Sephora** *Retail/Beauty* Sephora Settlement	Aug. 2022	**$1.2M**	Failed to disclose sale of consumer personal information; failed to process opt-out requests via Global Privacy Control (GPC); did not cure violations within 30-day period. Sharing data with third parties for analytics/advertising constituted a “sale” under the CCPA.
2	**DoorDash** *Food Delivery* DoorDash Settlement	Feb. 2024	**$375K**	Sold consumer personal information to marketing cooperatives without notice or opt-out opportunity. Sharing data with a marketing co-op for “other valuable consideration” constituted a sale under the CCPA. Also violated California Online Privacy Protection Act disclosure requirements.
3	**Tilting Point Media** *Entertainment/ Gaming* Tilting Point Media Settlement	June 2024	**$500K**	Collected and shared children’s data without parental consent in “SpongeBob: Krusty Cook-Off.” Used non-neutral age screen (defaulting to birth year 1953); misconfigured third-party SDKs. First CCPA children’s data action. Also violated federal Children’s Online Privacy Protection Act.
4	**Healthline.com** *Website Publisher/ Health* Healthline.com Settlement	July 2025	**$1.55M**	Failed to honor consumer opt-outs for targeted advertising; a misconfigured opt-out mechanism continued transmitting data. Shared article titles revealing potential medical diagnoses with ad-tech vendors, violating CCPA’s purpose limitation principle. Advertising contracts lacked required terms.
5	**Sling TV** *Streaming Service* Sling TV Settlement	Oct. 2025	**$530K**	First action from the CA Department of Justice’s streaming services sweep. Used deceptive, hard-to-find opt-out methods; combined CCPA opt-out with cookie preferences; required resubmission of known information. Failed to provide in-app opt-out on connected TV devices. Lacked children’s privacy protections.

#	ENTITY	DATE	PENALTY	HOLDING / KEY VIOLATIONS
6	**Jam City** *Mobile App Gaming* Jam City Settlement	Nov. 2025	**$1.4M**	Sold/shared consumer data across 21 mobile gaming apps without providing any CCPA-compliant opt-out mechanism. 20 of 21 apps had zero opt-out controls. Misconfigured age gates resulted in selling/sharing data of consumers ages 13–15 without required affirmative consent.
7	**The Walt Disney Co.** *Entertainment/ Streaming* Disney Settlement	Feb. 2026	**$2.75M**	Largest CCPA settlement to date. Second action from streaming sweep. Failed to fully effectuate opt-out requests across all devices and streaming services linked to a consumer's account. In-app toggles limited to single service/device; GPC signals honored only on originating device rather than account-wide.

INVESTIGATIVE SWEEPS

To monitor business compliance with the CCPA, Attorney General Bonta has conducted investigative sweeps related to the following topics: location data, streaming apps and devices, employee information, and surveillance pricing.

Source:* California Office of the Attorney General Press Release (Feb. 11, 2026) *and individual settlement announcements.