Paul, Weiss

Client Memorandum

May 22, 2026

California Privacy Updates: Q1 2026

California remains at the forefront of data privacy regulation in the United States, maintaining a privacy regulatory framework that serves as the benchmark for U.S. state privacy law.

The regime continues to intensify in 2026, with the California Privacy Protection Agency ("CalPrivacy") and the California Attorney General collectively issuing enforcement actions totaling more than $4.22 million in penalties during the first quarter alone. California regulators are focusing on the effectiveness of privacy controls, particularly opt-out mechanisms and the recognition of browser-based preference signals like Global Privacy Control, as well as the accuracy of consumer-facing privacy disclosures. Recent enforcement activity has targeted companies across diverse industries, demonstrating that no sector engaging in the collection of personal information or targeted advertising specifically is beyond regulatory scrutiny.

At the same time, significant new regulatory obligations took effect on January 1, 2026, including risk assessment and cybersecurity audit requirements, expanded data broker obligations and the introduction of a 30-day data breach notification timeline, thereby further raising the compliance bar for businesses subject to the California Consumer Privacy Act ("CCPA").

Key Takeaways

Q1 developments reflect several key themes:

- **Opt-Out Compliance**: Q1 enforcement actions targeted failures in the technical implementation of opt-out mechanisms. Regulators have focused on organizations that fail to honor opt-out requests across all devices and services linked to a consumer's account and barriers to submitting these requests, including verification steps that add unnecessary friction (such as requiring email confirmation before processing an opt-out). Regulators have also called out failures where a business redirected consumers to exercise opt-out rights directly with third-party tracking companies, through centralized industry opt-out programs, instead of employing a functional in-house mechanism.

- **Minors' Data Protection**: CalPrivacy announced its first enforcement decision addressing privacy violations involving students and schools in Q1 2026. The agency described students as a "uniquely vulnerable population" and emphasized that businesses serving school-age audiences should ensure privacy notices are accessible and understandable to those users.

- **Enforcement Spans Diverse Industries**: Enforcement actions this quarter targeted an entertainment and streaming service provider, a youth sports and school services provider, and a connected vehicle manufacturer, suggesting that regulators are increasingly looking across industries and business models when evaluating privacy compliance. Any company that collects and processes personal information, and engages in data sharing or targeted advertising, should be aware of the regulatory scrutiny and see these enforcement actions as a warning to examine and review their own privacy controls.

- **Expanded Data Broker Obligations**: CalPrivacy has made data broker enforcement a priority. The agency's Delete Request and Opt-Out Platform ("DROP") is now live. This platform enables consumers to submit a single request to all registered data brokers to delete their personal information and opt out of its sale, reinforcing greater consumer control over data held by data brokers. Revised regulations also broaden the definition of "data broker" to capture businesses that may not have previously viewed themselves as falling within that category.

- **Risk Assessments and Cybersecurity Audits**: Finalized CCPA regulations imposing risk assessment and cybersecurity audit obligations took effect on January 1, 2026. Risk assessments are required for processing activities that create "significant risk" to consumers, including selling or sharing personal information. Businesses meeting certain revenue and volume thresholds must also complete independent cybersecurity audits. Documentation of these risk assessments and audits must be submitted beginning in April 2028 (with deadlines staggered based on revenue). Recent enforcement actions have also required organizations to undertake risk assessments as part of their remediation obligations.

Q1 Enforcement Activity

California regulators have issued three enforcement actions under the CCPA in the first quarter of 2026.

1. The Walt Disney Company (February 11, 2026)

One of the largest CCPA settlements in California history, the California Attorney General's action against the Walt Disney Company established that businesses must honor opt-out requests across all linked services and devices, not just where the request was submitted.[1] The California Attorney General's investigation into Disney stemmed from a January 2024 investigative sweep of streaming services for potential CCPA violations. Disney operates streaming services that collect personal information for sale, sharing and advertising. The Attorney General alleged key gaps in Disney's opt-out methods, as follows:

- ***Opt-Out Toggles***: Disney failed to fully honor consumers' opt-out requests across all devices and streaming services associated with their accounts. Specifically, when consumers used opt-out toggles within a service on a device, Disney only applied the request to that specific service and device, enabling the sale and sharing of data elsewhere.
- ***Webform***: When consumers opted out of using Disney's webform, Disney stopped sharing personal information through its own advertising platform but continued to sell and share data with third-party ad-tech companies. Furthermore, Disney's connected TV apps lacked in-app opt-out mechanisms, instead directing consumers to the webform, which did not stop data sharing from those apps.
- ***Global Privacy Control ("GPC")***: Disney also limited GPC signals (browser-based signals that facilitate the opt-out process) to the specific device sending the signal, even when the consumer was logged into their account, violating CCPA regulations requiring businesses to apply GPC across all of their interactions with a known consumer.

In addition to paying $2.75 million, Disney must provide compliance updates to the Attorney General every 60 days until fully compliant, honor opt-out requests across all services linked to a consumer's account when logged in (for logged-out users, Disney must either prompt them to log in or apply the opt-out at the device or browser level), and maintain a compliance monitoring program for three years.[2]

2. PlayOn Sports (March 3, 2026)

CalPrivacy resolved an enforcement action against PlayOn Sports ("PlayOn"), a youth sports media company that provides digital ticketing, streaming and sports-related services to schools, to resolve privacy violations related to the use of tracking technologies, deficient privacy disclosures and ineffective opt-out procedures. The enforcement action was the agency's first action targeting privacy violations affecting students and California schools, a population the agency has described as "uniquely vulnerable."[3] CalPrivacy launched a 2024 investigation into PlayOn's privacy practices, during which it received a complaint from a consumer alleging that the company did not allow consumers to opt out of the selling and sharing of personal information through tracking technologies.

CalPrivacy alleged gaps in PlayOn's tracking, opt-out and notice practices:

[1] California Attorney General, *California Won't Let It Go: Attorney General Bonta Announces $2.75 Million Settlement with Disney, Largest CCPA Settlement in California History* (Feb. 11, 2026), available here.

[2] *People of the State of California* v. *The Walt Disney Company*, No. 26STCV04425, Final Judgment and Permanent Injunction (Cal. Super. Ct. Feb. 11, 2026), available here.

[3] California Privacy Protection Agency, *Youth Sports Media Company to Pay $1.10 Million Fine, Change Practices Over Privacy Violations* (March 3, 2026), available here.

- ***Tracking Technologies***: PlayOn used tracking technologies to collect personal information and deliver targeted advertisements to ticketholders, forcing consumers to click "agree" to tracking before they could use their tickets or view PlayOn's websites.
- ***Opt-out Options***: Instead of providing an effective and quick method for consumers to opt out, PlayOn directed consumers to opt out directly with third-party tracking companies via the Network Advertising Initiative and Digital Advertising Alliance, which are industry self-regulatory organizations that provide centralized opt-out programs for participating companies. PlayOn also failed to recognize opt-out preference signals.
- ***Privacy Notice***: PlayOn did not regularly update its online privacy policy and provided inaccurate notice of consumers' privacy rights, falsely claiming that it did not sell consumers' personal information. PlayOn also failed to inform consumers how to exercise their right to opt out.

In addition to paying a $1.1 million fine, PlayOn was obligated to conduct privacy risk assessments, and update those assessments before any material change in its processing of personal information. The company must also provide accurate disclosures on its privacy practices that are easy to read and understandable to the audience using its services, with the explicit requirement that notices for high school events be accessible to student attendees. PlayOn Sports is further required to complete quarterly scans of its website to maintain a current inventory of tracking technologies and implement proper, functional opt-out mechanisms.[4]

3. Ford Motor Company (March 5, 2026)

CalPrivacy also resolved an enforcement action with Ford Motor Company, imposing a $375,703 fine related to the manufacturer's opt-out procedures for data collected by connected vehicle features. Arising from CalPrivacy's review of data privacy practices by connected vehicle manufacturers, this action reinforces that businesses cannot impose unnecessary verification steps that create friction in the opt-out process.[5] CalPrivacy alleged key issues in Ford's opt-out processes:

- ***Verification Steps***: Ford required consumers to complete an email verification step before they could opt out of the sale and sharing of personal information, which added "unnecessary friction" that discouraged consumers from exercising their privacy rights.
- ***Opt-out Processing***: Ford did not process opt-out requests unless consumers completed this verification step, deeming requests "expired" when consumers did not complete the verification. This resulted in Ford not processing dozens of opt-out requests within the period required by the CCPA.

In addition to paying a fine, Ford must modify its methods for handling consumer rights requests to ensure opt-outs are easy and require minimal steps, honor all opt-out requests within the time period required by the CCPA, and conduct an audit of the tracking technologies on its website to ensure such tools function properly to facilitate opt-out requests and comply with opt-out preference signals, including the GPC.[6]

Legislative and Regulatory Developments

CalPrivacy continues to expand its footprint beyond enforcement. In the first quarter of 2026, the agency has sponsored two significant legislative proposals:

- **AB 2021, the Whistleblower Protection and Privacy Act**: This bill would create a whistleblower program similar to whistleblower laws in the financial services and anti-fraud contexts, offering financial awards consisting of a portion of penalties collected from enforcement actions that result from insider tips, along with anti-retaliation protections for employees who report privacy violations.[7]

[4] *In re 2080 Media, Inc. d/b/a PlayOn Sports*, Case No. ENF24-S-PL-24, Order of Decision (Cal. Privacy Prot. Agency, February 27, 2026), available here.

[5] California Privacy Protection Agency, *Ford to Change Practices, Pay Fine for Adding Unnecessary Friction to Opt-Out Process* (March 5, 2026), available here.

[6] *In re Ford Motor Company*, Case No. ENF23-V-FO-3, Order of Decision (Cal. Privacy Prot. Agency, February 27, 2026), available here.

[7] California Privacy Protection Agency, *CalPrivacy Sponsors Whistleblower Protection Bill* (February 24, 2026), available here.

- **SB 923, the Expanding Privacy Rights Act**: This bill would expand consumers' deletion rights to include data obtained from third-party sources and require online businesses to provide multiple methods for submitting privacy requests beyond just email.[8]

Several significant regulatory and legislative changes also took effect in California on January 1, 2026, with new requirements spanning data broker obligations, risk assessments and cybersecurity audits and data breach notification timelines:

- **DROP**: CalPrivacy's DROP went live, allowing California consumers to submit a single request directing all registered data brokers to stop selling their personal information.[9] CalPrivacy has made data broker enforcement a priority, issuing decisions in enforcement actions against Rickenbacher Data LLC, d/b/a DataMasters (for selling "lists of people" based on health conditions) and S&P Global, Inc. (for failing to register under the Delete Act) on December 30, 2025.[10] New regulations also sharpen the definition of "data broker" to capture businesses that historically may not have viewed themselves as falling within that category, including providers of third-party website tracking technologies and businesses who augment their first-party data with third-party data.[11]

- **CCPA Regulations on Risk Assessments, Cybersecurity Audits and automated decision-making technology (ADMT)**: CalPrivacy's finalized CCPA regulations governing risk assessments, cybersecurity audits and automated decision-making technology ("ADMT") are now effective. Risk assessments are required for processing activities that create significant risk to consumers, such as selling or sharing personal information and processing sensitive personal information.[12] For any processing activity that the business initiated prior to January 1, 2026 and that continues after that date, the business must conduct a risk assessment no later than December 31, 2027.[13] For any covered processing activity that the company has not yet initiated, the risk assessment must be completed before starting the processing.[14] Risk assessments conducted in 2026 and 2027 must be submitted to CalPrivacy by April 1, 2028. Businesses meeting certain data volume or risk thresholds are also subject to independent cybersecurity audits covering their security infrastructure and controls.[15] Deadlines for submitting documentation are staggered based on revenue, with the first audits (covering periods beginning January 1, 2027) due by April 1, 2028 for businesses with gross revenue over $100 million, and later deadlines applying to smaller businesses through April 1, 2030. Additionally, businesses using ADMT systems that pose significant risk to consumers' privacy must provide detailed disclosures about system functionality and honor opt-out requests.[16]

- **Data Breach Notification**: California amended its data breach notification statute to impose a fixed 30-day deadline for notifying impacted California residents following discovery of a breach. For breaches affecting more than 500 residents, businesses must also submit a sample data subject notice to the Attorney General within 15 days of notifying impacted consumers.[17]

Practical Implications

In light of the heightened scrutiny and escalating enforcement environment, businesses should consider conducting end-to-end reviews of their privacy compliance program, and their opt-in and opt-out mechanisms in particular—including webforms, in-app tools, cookie banners and GPC signal recognition—to confirm that consumer requests are honored consistently across all platforms, devices and services. Companies should also review their service provider and third-party contracts to ensure that data sharing restrictions and appropriate contractual terms are in place, particularly in relationships involving advertising and

[8] California Privacy Protection Agency, *CalPrivacy Sponsors Bill That Expands Deletion Rights and Accessibility Requirements* (January 30, 2026), available here.

[9] Cal. Civ. Code § 1798.99.80–1798.99.86; California Privacy Protection Agency, *CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers* (January 8, 2026), available here.

[10] *Id*.

[11] Cal. Code Regs. tit. 11, § 7601.

[12] Cal. Code Regs. tit. 11, §§ 7150–7157.

[13] *Id*.

[14] *Id*.

[15] Cal. Code Regs. tit. 11, §§ 7120–7124.

[16] Cal. Code Regs. tit. 11, §§ 7220–7222.

[17] Cal. Civ. Code § 1798.82.

analytics services. Businesses that interact with minors or student populations should evaluate their data collection practices and ensure that privacy notices are tailored to those audiences.

Similar to understanding the broad definitions of "selling" and "sharing" under the CCPA, businesses should also assess whether they qualify as data brokers under California's expanded definitions and confirm whether registration under the Delete Act and participation in DROP is required. Finally, with risk assessment and cybersecurity audit obligations now in effect, organizations should begin scoping these requirements and building internal processes to meet applicable deadlines.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Katherine B. Forrest
+1-212-373-3195
kforrest@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

John Patten
+44 20 7367 1684
jpatten@paulweiss.com

Ian C. Richardson
+1-202-223-7405
irichardson@paulweiss.com

Jacobus "Janus" Schutte
+1-212-373-3152
jschutte@paulweiss.com

Jennifer Songer
+1-202-223-7467
jsonger@paulweiss.com

Audrey M. Paquet
+1-212-373-2397
apaquet@paulweiss.com

Associates Cole A. Rabinowitz and Sarah Shin contributed to this Client Memorandum.