Ebook

State of US Privacy Enforcement

2026: The Year US State Privacy Enforcement Stopped Being Theoretical

osano

Contents

Introduction

The End of the 'Wait and See' Era

For years, US data privacy enforcement was a little bit like cold fusion–it was always coming, always right around the corner, but never here. Most businesses adopted a “wait and see” approach to data privacy compliance.

That era is over.

The sixteen months between January 2025 and May 2026 produced more enforcement activity under comprehensive state privacy laws than the preceding five years combined. The California Privacy Protection Agency (CPPA) and Attorney General together imposed penalties counted in the millions of dollars. Outside of regulation-happy California, multiple states filed their first data privacy enforcement actions. Attorneys General coordinated multi-state investigative sweeps. Hundreds–if not thousands–of investigations have been launched.

With this report, we aim to help businesses understand the dynamics at play during this period of high enforcement activity. We’ve striven to provide a digestible overview of the major facts of enforcement cases, the recurring themes seen throughout, and the tangible, practical steps businesses should take to reduce their risk.

Section 1 documents every significant enforcement action in the period, organized by state and regulator. Section 2 identifies eight violation themes that appear consistently across those actions. Section 3 translates those patterns into prioritized, practical guidance for your compliance program. And Section 4 explains how Osano can help.

We built this report because we think privacy professionals, business stakeholders, and non-privacy experts alike deserve clear, factual analysis of what regulators are actually doing. Armed with this knowledge, you’ll be better equipped to navigate the realities of data privacy enforcement in the US.

— The Osano Team

Overview

Between January, 2025 and May, 2026:

- Regulators in California, Texas, Connecticut, Utah, Florida, and Kentucky took enforcement action under comprehensive state privacy laws—many for the first time.
- California's Privacy Protection Agency (CPPA) imposed multi-million dollar fines in a single year and disclosed that it has hundreds of open investigations, most still unknown to their targets.
- Ten state regulators formally coordinated through a newly established enforcement consortium.

The biggest commonality across these actions was a technical gap in violators' systems and tooling. Consistently, the privacy program looked fine on paper, but the technology told a different story.

We've focused the report on comprehensive data privacy law enforcement actions, but actions under data broker laws and wiretap laws are also included. Although state data privacy law enforcement is significant and ramping up, states and law firms are making use of all of the tools available to them–inclusive of data broker and wiretap laws–to penalize data privacy violations.

Sources: CPPA Board Meeting, Sept. 26, 2025 (Perkins Coie, Oct. 1, 2025; Hudson Cook, Sept. 29, 2025; Privacy Daily, Sept. 26, 2025); oag.ca.gov; texasattorneygeneral.gov; cppa.ca.gov

Enforcement at a Glance

$23M+

Data privacy penalties (excluding the $1.3B Google settlement).

Average penalty size (excluding the $1.3B Google settlement).

$2.07M

4 **states brought their first-ever privacy law enforcement actions.**

CCPA complaints fielded by the CPPA per week on average.

~150

Section 1

Enforcement Landscape by State

Until 2025, data privacy enforcement was something that happened in Europe.

Between January, 2025, and May, 2026, numerous state privacy laws became effective and enforceable. Regulators wasted no time in putting their new tools to use. In this section, we document every significant enforcement action brought under a comprehensive state privacy law during the report period.

But state privacy laws aren't the only ways that data privacy is being enforced–they're merely the most visible. In parallel with the rise of US privacy laws, data broker laws have begun to be enforced. We summarize the state of data broker enforcement during this period here as well. You might not consider your organization to be a "data broker," but you'd be surprised at what businesses meet regulatory definitions.

Last but certainly not least, we cover what is arguably the most active sphere of privacy enforcement in the US–wiretap and VPPA lawsuits. Absent a data privacy law with an opt-in standard of consent, enterprising law firms have been successfully suing businesses left and right under these Cold War-era laws.

California—CPPA (CalPrivacy)

The California Privacy Protection Agency has been the most active dedicated privacy enforcement authority in the United States.

The agency imposed fines in five actions during the period, ranging from $345,178 to $1.35 million. Its deputy director of enforcement, Michael Macko, told the CPPA Board in September 2025 that the agency had opened "hundreds" of investigations, most of which had not yet been surfaced to the businesses under scrutiny.

All of these actions shared a common theme: There was a significant gap between what the businesses said they were doing and what their technology was actually doing.

Opt-out mechanisms existed in policy but failed technically. Vendor contracts referenced compliance without specifying it. Consumer request portals sat misconfigured, silently rejecting submissions. In each case, the CPPA demonstrated that it tests mechanisms, not just policies.

> **"We're receiving about 150 complaints every single week. That number has been increasing over time."**
>
> **— Michael Macko, CPPA Deputy Director of Enforcement, CPPA Board Meeting, Sept. 26, 2025**

CalPrivacy Actions Overview

Organization	Penalty	Date	Core Violations
American Honda Motor Co.	$632,500	Mar. 12, 2025	Used a single standardized form for all CCPA request types including opt-out; required excessive personal information to process opt-out requests; prohibited follow-up verification for opt-out; no CCPA-compliant vendor contracts with ad-tech companies.
Todd Snyder, Inc.	$345,178	May 6, 2025	Privacy request portal misconfigured for 40 days, failing to process opt-outs; required unnecessary personal information from consumers; required identity verification before honoring opt-out (prohibited under CCPA)
Tractor Supply Company	$1,350,000	Sep 30, 2025	Non-functional "Do Not Sell" link; failed to honor GPC signals; no CCPA-compliant vendor contracts with ad-tech companies; failed to inform job applicants of privacy rights; privacy policies not updated annually
Ford Motor Company	$375,703	Mar 5, 2026	Used a single standardized form for all CCPA request types including opt-out; required follow-up email verification for opt-out (prohibited); failed to honor opt-out within required timeframe
PlayOn Sports	$1,100,000	Mar 3, 2026	Tracked high school event ticketholders with targeted advertising; required consumers to “agree” to tracking to purchase tickets; directed consumers to NAI/DAA opt-out instead of providing its own mechanism. First CPPA action focused on student and youth privacy.

Sources: cppa.ca.gov/announcements; CPPA Stipulated Final Orders (Todd Snyder, May 6, 2025; Tractor Supply, Sept. 30, 2025; Ford, Mar. 5, 2026; PlayOn Sports, Mar. 3, 2026); McDermott Will & Emery, Oct. 2, 2025; Troutman Pepper, Oct. 1, 2025

Tractor Supply—The CPPA's First Subpoena Enforcement Action

When Tractor Supply declined to provide information on its activities predating January 1, 2023—arguing CPPA's enforcement authority didn't exist before that date—the agency took the matter to Sacramento County Superior Court (Aug. 6, 2025). The case was mooted by settlement, but Tractor Supply acknowledged in the final order that the CPPA has broad authority to investigate CCPA violations going back to January 1, 2020.

Ford Mirrors Honda

The CPPA's Honda and Ford settlements bookend the connected vehicle enforcement arc in this report. Honda (March 12, 2025, $632,500) was the agency's inaugural enforcement action; Ford (March 5, 2026, $375,703) was its most recent. Both actions featured:

- A standardized opt-out form that conflated opt-out subject rights requests with other request types,
- Identity verification for simple opt-out requests (a prohibited practice under the CCPA)
- A failure to execute CCPA-compliant contracts with ad-tech vendors.

Notably, both companies relied on the same legacy data privacy vendor for their compliance. They didn't realize that this vendor did not provide them with an out-of-the-box compliant configuration, resulting in, for example, non-compliant identity verification for opt-out requests.

Both companies were part of CPPA's 2023 connected vehicles investigative sweep. Additional manufacturers from that sweep remain undisclosed.

California—Office of the Attorney General

The California Attorney General's office ran two investigative sweeps during the period—a January 2024 sweep targeting streaming services and a March 2025 sweep of the location data industry. The streaming sweep produced its first results during this period: four settlements totaling $6.23 million, including the largest CCPA settlement ever recorded.

CA OAG Actions Overview

Organization	Penalty	Date	Core Violations
Healthline Media LLC	$1,550,000	Jul 1, 2025	Failed to honor opt-outs; 118 tracking cookies continued firing even after consumers used all three opt-out methods simultaneously; shared health-article URLs revealing medical conditions (e.g., “Newly Diagnosed with HIV?”) to advertisers; ad contracts lacked CCPA-required terms. First CCPA enforcement of the purpose limitation principle.
Sling TV/Dish Media	$530,000	Oct 30, 2025	Conflated CCPA opt-out with cookie preferences in a confusing interface; no opt-out mechanism on connected TV apps (the primary platform for most subscribers); required name, address, email, and phone to submit opt-out; no affirmative consent process for consumers aged 13–16.

Sources: oag.ca.gov press releases—Healthline Media, Jul. 1, 2025; Sling TV, Oct. 30, 2025

CA OAG Actions Overview (cnt'd)

Organization	Penalty	Date	Core Violations
Jam City, Inc.	$1,400,000	Nov 21, 2025	20 of 21 mobile apps contained no opt-out mechanism; website lacked required opt-out link; age gates screened only for under-13 (not under-16 as required); sold and shared data of 13–16-year-olds without affirmative consent.
Walt Disney Company	$2,750,000	Feb 11, 2026	Opt-out applied only to the specific streaming service and device on which it was submitted—not account-wide, even for logged-in users; GPC honored at device level only; connected TV apps contained no in-app opt-out; Disney linked consumer devices for advertising purposes but not for privacy elections. Largest CCPA settlement to date.
General Motors (OnStar)	$12,750,000	May 8, 2026	Sold names, contact information, geolocation data, and driving behavior of hundreds of thousands of California drivers to data brokers without notice or consent; retained driving data beyond its OnStar operational purpose and sold it for insurance rate-setting; privacy policy affirmatively stated GM did not sell driving or location data.

Sources: oag.ca.gov press releases—Jam City, Nov. 21, 2025; Walt Disney, Feb. 11, 2026

Healthline and Purpose Limitation

The Healthline case explored a novel angle in CCPA enforcement—specifically, the CCPA's purpose limitation principle. Investigators found that 118 third-party advertising cookies continued transmitting data after consumers had exercised all three available opt-out methods—including via the GPC.

In addition, many of Healthline's ad-tech contracts allowed recipients to use shared data for “any business purpose,” for “internal use,” or for unspecific “purposes contemplated” in the contract. Under the CCPA’s purpose limitation principle, compliant vendor contracts must describe the limited and specified purposes for which shared data can be used. This moves enforcement from disclosure-based compliance into the substance of how data is actually used.

Disney and Account-Level Opt-Outs

The Disney settlement established a rule that will require broad system redesign for any business with multi-platform infrastructure: if you link consumer devices together for advertising purposes, you must also link them for privacy elections. A logged-in user's opt-out must follow them across all services and devices—not just the one where they clicked.

> **"Consumers shouldn't have to go to infinity and beyond to exercise their privacy rights"**
> **— California AG Rob Bonta, Feb. 11, 2026 (oag.ca.gov)**

2025 Location Data Investigative Sweep

The California AG's March 2025 location data investigative sweep had not produced publicly announced enforcement actions as of this writing. Given the precedent set by the Healthline and Disney settlements, outcomes from that sweep—if and when they are announced—are likely to involve similar themes around opt-out efficacy and data use beyond disclosed purposes.

General Motors and Data Minimization—A New Enforcement Frontier

The General Motors settlement, announced May 8, 2026, is the largest CCPA penalty in California history at $12.75 million—surpassing the Disney settlement announced just three months earlier. It is also the California AG's first enforcement of the CCPA's data minimization principle.

GM collected precise geolocation and driving behavior data through OnStar, a connected vehicle service marketed to consumers as a safety and navigation tool. Between 2020 and 2024, without consumer notice or consent, GM sold that data to two data brokers who intended to use it to develop driver-rating products for auto insurers.

For businesses outside the automotive sector, the GM settlement shows that the CCPA’s purpose limitation has teeth: data collected for one reason cannot simply be repurposed for another.

Texas—AG Ken Paxton & TDPSA

After California, Texas has been the second-most active state for privacy enforcement operations, combining the Texas Data Privacy and Security Act (TDPSA) with DTPA, the biometric data law (CUBI), and the Insurance Code to create a broad enforcement toolkit.

Chinese-Owned Company TDPSA Cure Notices

AG Paxton issued 30-day TDPSA cure notices to TP-Link, Alibaba, CapCut, and other Chinese Communist Party-affiliated companies, alleging failure to disclose data processing practices, failure to provide opt-out mechanisms, and failure to enable data deletion. Legal action was threatened for non-compliance. The notices named specific companies but did not publicly disclose the underlying evidence.

In February, 2026, Attorney General Paxton's office sued TP-Link for deceptive trade practices, though this suit did not reference TDPSA or other Texan laws with a direct data privacy link. Other than this, no subsequent enforcement actions against these companies had been publicly announced as of this writing.

Sources: TX AG press release, May 6, 2025, Dec. 15, 2025 (texasattorneygeneral.gov); Wiley Law, May 8, 2025; KSST Radio, May 7, 2025; Digital Policy Alert, May 6, 2025; MLex, Apr. 10, 2025; Bloomberg Law, Apr. 14, 2025; Cybersecurity Law Report, May 21, 2025;

Allstate/Arity Lawsuit Dismissed

AG Paxton filed the first TDPSA lawsuit ever in January of 2025 against Allstate and its subsidiary Arity for covertly collecting geolocation and driving data–only for a judge to dismiss the suit in April. While the TDPSA has, like other state privacy laws, an extraterritorial reach, the court ruled that it lacked personal jurisdiction over Allstate/Arity–essentially, citing constitutional due process rights that supersede the TDPSA's authority. Unlike California, Texas's data privacy law requires filing a lawsuit against violators, making it vulnerable to a court's interpretation of its jurisdiction.

Future TDPSA lawsuits may run up against similar challenges when violators have minimal presence in Texas. It's also why data privacy enforcement in Texas has been carried out under other laws, like the Deceptive Trade Practices Act (DTPA).

Smart TV ACR Lawsuits

AG Paxton filed five lawsuits against Sony, Samsung, LG, Hisense, and TCL under the Deceptive Trade Practices Act for automated content recognition (ACR) technology in smart TVs—software that records what a viewer is watching, including content from other devices (cable boxes, game consoles, streaming sticks) connected to the TV, without adequate disclosure or consent. Temporary restraining orders were obtained against Hisense and Samsung. These filings also function as 30-day TDPSA cure notices. All five cases were in active litigation as of this writing.

Netflix—Behavioral Surveillance Lawsuit

AG Paxton filed a lawsuit against Netflix, Inc. for allegedly constructing what the complaint describes as a "behavioral-surveillance program of staggering scale." The lawsuit alleges that Netflix tracked and logged users' viewing habits, preferences, devices, household networks, and application usage across both adult and children's profiles, then disclosed this behavioral data to commercial data brokers and advertising technology companies to build detailed consumer profiles.

The suit is brought under the Texas Deceptive Trade Practices Act (DTPA), consistent with the AG's broader pattern of using DTPA for privacy enforcement actions against large technology companies. The case was in active litigation as of the date of this report.

Google—$1.375 Billion Settlement

The largest single-state privacy settlement in US history resolved claims that Google unlawfully tracked users' geolocation data even after they opted out, collected voiceprints and facial geometry without consent, and misled users about Incognito mode's privacy protections. The case was brought under DTPA and the Texas Capture or Use of Biometric Identifier Act (CUBI), not TDPSA—but its scale sent an unmistakable signal about Texas's enforcement ambitions and the AG's willingness to pursue trillion-dollar companies.

Sources: TX AG press release, May 9, 2025, May 11, 2026; Cybersecurity Law Report, May 21, 2025

> **"This $1.375 billion settlement is a major win for Texans' privacy and tells companies that they will pay for abusing our trust."**
>
> **— Texas AG Ken Paxton, May 9, 2025 (texasattorneygeneral.gov)**

Additional Enforcement Activity

Beyond the above, the Texas AG issued more than 100 data broker noncompliance notices during the period, maintained active investigations into over 15 companies on children's privacy grounds (including Character.AI, Reddit, Instagram, and Discord), and continued litigation against General Motors and OnStar (filed August 2024 under DTPA) for collecting and selling driving data from 1.5–1.8 million Texas vehicles without adequate consent.

Other Active State Attorneys General

One of the period's most significant structural developments was not a single case but a pattern: attorneys general in Connecticut, Utah, Florida, and Kentucky each filed or settled the first enforcement action ever brought under their respective state omnibus privacy laws. They signal that the enforcement transition underway in California and Texas is spreading.

Connecticut—TicketNetwork, Inc. ($85,000; First CTDPA Penalty)

In what would become the first monetary penalty under the Connecticut Data Privacy Act (CTDPA), AG Tong sent TicketNetwork a cure notice in November 2023, making it one of more than two dozen companies to receive such notices. It was the only one that failed to act.

Its privacy notice was described by the AG as “largely unreadable,” its consumer rights mechanisms were “misconfigured or inoperable,” and—critically—the company repeatedly misrepresented to the AG that it had resolved the issues when it had not.

The CTDPA cure period expired January 1, 2025, giving Tong direct enforcement authority to issue this penalty against TicketNetwork.

Connecticut is one of the few states that releases an annual enforcement report, giving us a peek behind the curtain to additional enforcement activity from AG Tong’s office. His office disclosed 70 CTDPA complaints and over 1,830 data breach notifications in its 2025 enforcement report.

Lastly, AG Tong joined a multi-state investigative sweep into GPC compliance in September 2025.

Utah—Snap, Inc. (First UCPA Lawsuit)

The Utah AG filed the first lawsuit ever under the Utah Consumer Privacy Act (UCPA), alleging Snapchat failed to inform consumers about data sharing with third parties, collected sensitive biometric and geolocation data through the My AI feature without providing an opt-out, and processed children's data without parental consent. The case was in active litigation as of this writing.

Sources: CT AG press release, Jul. 8, 2025 (portal.ct.gov); CTDPA Annual Enforcement Report, 2025; UT AG press release, Jun. 30, 2025 (attorneygeneral.utah.gov)

Florida—Roku, Inc. (First FDBR Lawsuit)

Normally, the privacy community doesn't include the Florida Digital Bill of Rights (FDBR) when discussing state privacy laws since it only applies to businesses with over a $1 billion in annual revenue. However, in October, the Florida AG filed the first enforcement action under the FDBR, targeting Roku for collecting personal and sensitive data from users identified as children without parental authorization, failing to disclose data sales including geolocation, collecting voice recordings via remotes without consent, and failing to implement user profiles that would identify and protect child users. Penalties sought reach $150,000 per violation involving children. As of this writing, the Roku case is still in active litigation.

The AG separately established a CHINA Prevention Unit (February 5, 2026)—the first state-level unit specifically dedicated to foreign adversary data threats—and issued subpoenas to Lorex, Contec, Shein, and TP-Link, among others. These subpoenas generally rely on the Florida Deceptive Trade Practices Act, but also invoke the FDBR when applicable. The Shein subpoena, for example, called out FDBR violations.

Sources: FL AG press release, Oct. 13, 2025 (myfloridalegal.com); FL AG press release, Feb. 5, 2026; KY AG press release, Jan. 8, 2026 (ag.ky.gov); Oregon DOJ quarterly OCPA enforcement reports (doj.state.or.us)

Kentucky—Character Technologies, Inc. (Character.AI; First KCDPA Lawsuit)

Eight days after the Kentucky Consumer Data Protection Act took effect, the AG filed the first action under the law—against Character.AI for failing to implement age verification and failing to obtain parental consent for users under 13. The filing established that Kentucky is not planning a gradual ramp-up period before enforcement begins. The case was in active litigation as of this writing.

Oregon—Numerous Cure Letters & Complaints

Oregon has published the most transparent enforcement data of any state in the nation. Its quarterly OCPA enforcement reports disclosed 214 consumer complaints and 38 closed cure letter matters in the law's first year (July 2024–June 2025), growing to more than 265 complaints by September 2025.

The most common deficiencies cited in cure letters included:

- Failure to disclose consumer rights
- Inadequate description of third-party data sharing
- Privacy notices that enumerate other states' rights but omit Oregon
- Opt-out mechanisms that are buried or technically burdensome
- Failure to provide "back-end" behavioral data (shopping patterns, marketing profiles) in response to access requests

As of January 1, 2026, the OCPA cure period has expired. It's up to the AGs discretion whether to grant a business the opportunity to fix its violations or to immediately levy out penalties, a decision that will no doubt be influenced by the business's cooperation and existing compliance efforts.

Minnesota—Numerous Cure Letters & Complaints

Minnesota's AG reported receiving over 200 consumer complaints in the law's first six months, most of which centered around deletion rights. The AG's office also sent dozens of enforcement notices during this period, with companies making quick corrections in most cases. As of January 31, 2026, the MCDPA has no cure period, leaving it up to the AG whether to provide companies the opportunity to fix their violations.

Other State Privacy Laws

No public enforcement actions were identified under the omnibus privacy laws of Virginia, Montana, Iowa, Indiana, Nebraska, Tennessee, Delaware, New Jersey, Maryland, New Hampshire, or Rhode Island during the period.

Colorado joined the September 2025 GPC investigative sweep alongside the CPPA, the California AG, and the Connecticut AG. The 60-day CPA cure period expired January 1, 2025. No public monetary settlements or named enforcement actions under the CPA were announced during the period, though the AG has sent warning and education letters since July 2023.

Maryland's MODPA is often characterized as the most unique privacy law in the US, but its enforceability only kicked in on April 1, 2026. Similarly, Indiana's, Kentucky's, and Rhode Island's laws only took effect on January 1, 2026, leaving little time for enforcement actions in this report's period of focus. Kentucky showed that swift enforcement is possible, however, issuing its first action just 8 days after the law entered into force (see previous).

Sources: Minnesota AG privacy enforcement updates (ag.state.mn.us)

Data Broker Enforcement and the DELETE Act

California, Vermont, Oregon, and Texas all have data broker laws and define a “data broker” somewhat differently. But generally speaking, a data broker is a business that knowingly collects and sells to third parties the personal information of a consumer with whom it does not have a direct relationship.

Just as with comprehensive data privacy laws, California has been the most active enforcer of data broker laws. The CPPA launched its Data Broker Enforcement Strike Force on November 19, 2025, issuing public enforcement actions against multiple unregistered brokers, including:

- Accurate Append, penalized $55,400.
- ROR Partners, penalized $56,600.
- Rickenbacher Data/Datamasters, penalized $45,000 plus a prohibition on sales of all Californians’ data. The company bought and sold lists of people based on sensitive health data, such as whether they had Alzheimer's disease, drug addiction, and bladder incontinence.
- S&P Global, penalized $62,600 for a registration failure its own legal team attributed to administrative error.

The most significant near-term development is the August 1, 2026 deadline for California data brokers to honor deletion and opt-out requests through the DROP platform—the DELETE Act's centralized consumer request system. DROP launched January 1, 2026, with more than 215,000 Californians signing up in the first month.

Non-compliance with Californians’ deletion requests triggers $200 per-record-per-day fines. This is the most operationally demanding privacy deadline facing data brokers in 2026, and the enforcement consequences are severe.

Neither Oregon, Vermont, or Texas engaged in significant data broker enforcement during this period, though Texas did revise its data broker law to expand its scope (previously, it had the narrowest scope out of these four states).

More than

215K

Californians registered for DROP in its first month.

Sources: cppa.ca.gov/announcements, Nov. 19, 2025; CPPA Stipulated Final Orders (Rickenbacher/Datamasters, S&P Global, Jan. 8, 2026); CPPA Board meeting materials, Nov. 2025

CIPA, Wiretap, and VPPA Litigation

State AG enforcement actions are not the only privacy risk businesses need to be aware of.

The plaintiff bar—driven by the chance to win statutory damages rather than regulatory priorities—has produced thousands of class action lawsuits under California's Invasion of Privacy Act (CIPA), other state wiretap laws, and the federal Video Privacy Protection Act (VPPA). These cases target the same technologies that drive privacy law exposure: tracking pixels, SDKs, session replay tools, and AI chatbots.

Fortunately, managing consent properly reduces risk across all three legal frameworks simultaneously–but crucially, wiretap laws rely on an explicit, opt-in standard for consent. Thus, you could be compliant with state privacy laws like the CCPA while still being at risk under wiretap laws like CIPA if you rely on opt-out consent.

CIPA—A 1967 Wiretap Law That Now Governs Modern Ad Tech

California's Invasion of Privacy Act (CIPA)—a 1967 wiretapping statute—is now one of the most actively litigated privacy laws in the country. The $5,000 per-violation statutory damages make CIPA financially dangerous at class scale even where underlying privacy violations appear minor.

Source: ByteBackLaw.com, Nov. 20, 2025

Businesses that have not implemented functioning opt-in consent mechanisms—where tracking genuinely does not fire until the user affirmatively consents—face exposure under CIPA on top of regulatory risk under California's comprehensive privacy law.

A California jury demonstrated in August 2025 what that exposure looks like in practice, returning a unanimous verdict against Meta in Frasco v. Flo Health for capturing reproductive health data through an embedded SDK without user consent. With a certified California class and $5,000 per violation, the potential damages exposure was described by Meta itself as reaching multiples of billions of dollars.

California SB 690, which would have created a safe harbor for routine commercial web tracking, failed to advance in 2025 and won't take effect before 2027.
For now, the liability risk is real and the compliance answer is straightforward: consent management that actually works reduces CIPA exposure in the same motion as it addresses CCPA obligations.

VPPA—Appellate Courts Narrow, SCOTUS Steps In

The Video Privacy Protection Act (VPPA)—a 1988 statute passed after a newspaper published Supreme Court nominee Robert Bork's video rental history—has been the vehicle for thousands of class actions alleging that website tracking pixels reveal users' video-viewing habits to third parties without consent.

Fortunately for businesses, appellate courts moved significantly to narrow VPPA liability during the research period.

In Solomon v. Flipps Media (2d Cir., May 2025), the Second Circuit held that social media ID strings and URL character sequences transmitted via the Meta Pixel do not constitute information that would allow an ordinary person to identify a specific individual's viewing behavior. The court stated its ruling “effectively shut the door for pixel-based VPPA claims.” It reaffirmed this position in Hughes v. NFL (June 2025).

It’s important to note that this only applies to the Second Circuit; other circuit courts can and have accepted VPPA cases and made different interpretations on this and other VPPA questions.

That’s exactly why the Supreme Court agreed to review Salazar v. Paramount Global on January 26, 2026. In this case, the Supreme Court weighed in to resolve a circuit split over whether VPPA's definition of “consumer”—someone who “subscribes to goods or services from a video tape service provider"—covers subscribers to any service (like a newsletter) or only subscribers to audiovisual goods and services.

Sources: Morgan Lewis, Jul. 21, 2025; WilmerHale, Oct. 20, 2025 and Jan. 23, 2026; WilmerHale, Jan. 23, 2026; Privacy World, Dec. 29, 2025

As of this writing, the Supreme Court has not issued a decision on this matter. The outcome will determine whether the VPPA can be used against newsletter operators, news publishers, and media companies whose video content is incidental to their primary service.

Wiretap and VPPA Suits: The Bottom Line

Court procedure may not make for thrilling reading to most, so what’s the takeaway?

Businesses need to be aware that privacy risk exposure in the US isn’t limited to regulators and state privacy laws. It also comes from plaintiff class action firms hunting for non-consented tracking technologies on websites. The same technologies that create state privacy law exposure—pixels, SDKs, session replay, ad-tech integrations—create CIPA and VPPA exposure. Fortunately, consent management and vendor auditing reduce risk across all of these frameworks at once.

Section 2

Common Themes and Violation Patterns

Across every enforcement action in this period, eight violation patterns repeat themselves with enough frequency to constitute the regulator's de facto enforcement agenda. Some are familiar; some represent meaningful expansions of what compliance actually requires.

Here are the patterns we identified and cover in this section:

1. **Opt-out mechanism failures**
2. **GPC/universal opt-out mechanism (UOOM) non-compliance**
3. **Dark patterns and consent asymmetry**
4. **Vendor and third-party contract failures**
5. **Children's privacy and sensitive data mishandling**
6. **Privacy notice deficiencies**
7. **Purpose limitation**
8. **Non-cooperation and aggravated enforcement outcomes**

1. Opt-Out Mechanism Failures

Present in every major California enforcement action and in the Texas Smart TV ACR suits, opt-out failures are the single most consistent reason why businesses draw regulators' attention. But the enforcement findings reveal something more specific than "opt-outs don't work." They reveal a category of failure where the opt-out exists in the interface but fails in the technology.

In **Healthline**, investigators found 118 tracking cookies continued transmitting data even after consumers exercised all three available opt-out methods simultaneously—a Do Not Sell link, a GPC signal, and a cookie banner. In **Disney**, opt-outs applied only to the specific streaming service and device on which they were submitted; a logged-in user who opted out on Disney+ was not opted out on Hulu or ESPN+. In **Sling TV**, connected TV apps—the primary way most subscribers watch—had no opt-out mechanism at all. In **Jam City**, 20 of 21 mobile apps had no opt-out controls.

The enforcement pattern is consistent: regulators are technically testing mechanisms, not reviewing policies. Companies that rely on a consent management platform to display a banner—without verifying that the downstream suppression of tracking technologies actually works—are operating with false confidence.

2. GPC/Universal Opt-Out Mechanism (UOOM) Non-Compliance

The September 2025 joint investigative sweep—in which the CPPA, the California AG, the Colorado AG, and the Connecticut AG simultaneously sent letters to businesses failing to honor Global Privacy Control (GPC) signals—was the Consortium of Privacy Regulators' first coordinated enforcement initiative. It will not be the last.

GPC non-compliance appeared explicitly in both the **Tractor Supply** ($1.35M) and **Healthline** ($1.55M) settlements. As of this writing, twelve state privacy laws require businesses to recognize a universal opt-out mechanism signal.

12 states

currently require businesses to honor GPC/UOOM signals

Source: Perkins Coie Inside Privacy Blog, Oct. 1, 2025

3. Dark Patterns and Consent Asymmetry

The **Sling TV** settlement is the period's clearest enforcement example of dark pattern design. The California AG found that Sling TV combined its CCPA opt-out with a general cookie preferences center—meaning consumers who wanted to exercise their right to opt out of the sale or sharing of their personal information were routed into a cluttered interface designed for a different purpose, rather than given a clear, standalone opt-out mechanism. On top of that, Sling TV's connected TV apps had no opt-out mechanism at all. The opt-out existed on the website, but viewers watching television had no access to it.

This is consent asymmetry in the most straightforward sense: the interface was structured to make data sharing the path of least resistance and privacy exercise the path of most friction. Sling TV also required consumers to submit their name, address, email address, and phone number to complete an opt-out request—information the company had no legal basis to demand for that purpose, and a requirement that would cause many consumers to abandon the process entirely.

The CPPA's January 1, 2026, regulations codify what the Sling TV settlement illustrated in practice: the number of steps required to opt out must equal or be fewer than the number of steps to accept, and banner closure alone cannot constitute consent. These are now enforceable regulatory standards, not just enforcement signals.

4. Vendor and Third-Party Contract Failures

Vendor contract violations were a core finding in several of the largest California settlements.

Three of the largest California settlements included vendor contract violations as primary findings. Regulators are not just checking for the existence of contracts—they are reviewing the actual language. **Healthline**, **Tractor Supply**, and **Honda** each featured material vendor contract deficiencies: Healthline's ad contracts permitted data use for 'any business purpose'; Tractor Supply's contracts failed to specify permitted purposes or prohibit cross-contextual behavioral advertising; Honda could not produce compliant contracts with its ad-tech service providers at all.

5. Children's and Sensitive Data Mishandling

Children's privacy was an enforcement priority in four states during the report period: California, Utah, Florida, and Kentucky. No other theme spans as many jurisdictions or carries as strong bipartisan political support.

Jam City sold data of users aged 13–16 without affirmative consent, which is the CCPA's standard for this age group. Most businesses are still treating age gating as a COPPA (under-13) question rather than a state privacy law question. **PlayOn Sports** tracked minors at high school athletic events. **Roku** collected from 'known children' without parental authorization. **Character.AI** operated with no age verification. **Snap's My AI** feature collected biometric and geolocation data from minors without an opt-out.

Sensitive data enforcement—covering health, precise geolocation, and biometric data—is equally prominent. Healthline's health-article URL sharing drew the largest AG penalty of the year. The **Flo Health** CIPA case produced a jury verdict on health data shared via SDK. The **Google** settlement covered geolocation and voiceprint collection.

With the **General Motors** settlement, the AG's complaint specifically cited the collection and sale of precise geolocation data without the required purpose limitation, and the injunctive terms include a five-year prohibition on selling driving data to consumer reporting agencies.

6. Privacy Notice Deficiencies

Privacy notice failures function as a near-universal secondary violation—present in almost every enforcement action in the period.

Connecticut's first CTDPA penalty went to **TicketNetwork** in part because its privacy notice was "largely unreadable." **Tractor Supply** failed to notify job applicants—not just consumers—of their CCPA rights. Oregon's enforcement reports show that notices listing other states' rights but omitting Oregon are a common trigger for complaints. **Tractor Supply** also had a stale notice that hadn't been updated annually as required.

The new CPPA regulations effective January 1, 2026, added specific notice requirements for mobile apps: privacy policy links must be accessible within the app's settings, not just on a website. For companies whose mobile app is their primary consumer touchpoint, this is a compliance gap that is now actively enforceable.

7. Purpose Limitation–Emerging but Significant

Healthline and **General Motors** are both among the most consequential CCPA enforcement decisions of the year. With these actions, the California AG established for the first time that purpose limitation has substantive teeth under CCPA.

In the Healthline enforcement, sharing article URLs that reveal a user's health condition (an article titled "Newly Diagnosed with HIV?" for example) with advertising partners was a CCPA violation—even when the privacy policy technically discloses data sharing. The purpose for which the data was originally collected (health information delivery) did not include advertising. The AG found that Healthline's ad contracts permitted use of shared data for "any business purpose," which is precisely what CCPA's purpose limitation restricts.

If adopted broadly across enforcement actions–even under most data privacy laws from states outside of California–this theory would invalidate a common compliance strategy in digital advertising: the use of broad, general disclosures of data sharing paired with "all-purpose" contracts with ad-tech partners.

Similarly, the General Motors settlement shows that data collected for a consented service (OnStar) cannot be repurposed for unrelated commercial monetization (sales to data brokers for insurance rate-setting). This is a broader application of purpose limitation than Healthline, where the issue was ad-tech contract language. Here, the issue is what happens to service data after the service is rendered.

8. Non-Cooperation and Aggravated Enforcement Outcomes

Across the enforcement actions in this period, the difference between a cure letter and a six- or seven-figure penalty was often not the severity of the underlying violation—it was how the company responded when regulators came knocking. Regulators in every state with an active enforcement program exercised prosecutorial discretion, and the companies that fared worst were not necessarily the most egregious violators. They were the ones that stonewalled, misrepresented, or ignored.

The Connecticut AG made this explicit in the TicketNetwork settlement. AG Tong noted that his office had issued more than two dozen cure notices across four separate privacy notice sweeps—and that TicketNetwork was the only recipient that failed to come into compliance.

The violations themselves—an unreadable privacy notice, missing consumer rights disclosures, non-functional opt-out mechanisms—were the same categories of deficiency identified across dozens of other companies. Nearly all of those companies corrected the issues promptly and avoided penalty entirely.

TicketNetwork's $85,000 settlement was not a function of uniquely bad violations; it was the price of misrepresenting compliance to the AG and running out the clock on the cure period.

Contrast this with the PlayOn Sports action. The CPPA's stipulated final order noted that PlayOn had self-remediated its violations in December 2024—before the agency made contact—and credited this in its findings. The company still paid $1.1 million, higher than TicketNetwork's five-figure penalty. But the order's explicit acknowledgment of the pre-contact remediation suggests the penalty would have been higher absent it, and the agency's willingness to say so publicly is itself a signal about what it values in a company's response posture.

For privacy professionals, the operational implication is straightforward: incident response planning should include a regulatory engagement protocol that is at least as developed as the technical remediation plan. Knowing who will communicate with the regulator, what the company's posture will be, and how quickly remediation can be documented and demonstrated can be a material factor in enforcement outcomes.

> **[TicketNetwork] repeatedly represented that they had resolved deficiencies when they had not done so, and failed to timely respond to follow-up correspondence."**
>
> **— OAG, Connecticut, press release, Jul 8, 2025 (portal.ct.gov/ag)**

Section 3

Actionable Guidance for Businesses

Based on these enforcement actions and the patterns across them, we can recommend seven compliance actions to reduce your risk. We've prioritized these through a mixture of effort, impact on your compliance, and risk exposure. That said, this is a generic prioritization, and every organization is different; your processing activities will inform which compliance actions you should take first.

Here are the actions we've identified as priorities and cover in this section:

1. **Opt-out and GPC implementation**
2. **Consent interface design**
3. **Vendor and third-party governance**
4. **Children's and sensitive data management**
5. **Privacy notice governance**
6. **Subject rights response workflows**
7. **Regulatory engagement and audit response planning**

Priority 1: Opt-Out and GPC Implementation

Why it's first:

Every major California settlement involved opt-out failures. GPC non-compliance drove a four-state coordinated sweep. The fine exposure is substantial and the technical bar has been set explicitly by enforcement outcomes.

- **Conduct a technical audit**. Test whether GPC signals are recognized and honored across all your digital properties and whether opt-out selections actually suppress tracking technologies—not just update a preference record. Use third-party scanning tools if needed—Osano, for example, provides a website privacy auditing tool known as Compliance Check.
- **Implement quarterly scanning**. The Tractor Supply consent order specifically required quarterly scanning and a current inventory of all tracking technologies deployed. Treat this as a minimum standard.
- **Account-level opt-out for logged-in users**. The Disney settlement established that if your platform links consumer devices for advertising purposes, it must link them for privacy selections. Opt-outs must follow the user account, not the device or session.
- **System-level opt-out is mandatory**. Similarly, offering an opt-out mechanism on your website doesn't mean you no longer need one in your mobile app or connected TV app. Each platform where tracking occurs needs its own accessible opt-out mechanism.
- **Stop requiring verification before opt-out**. CCPA prohibits requiring consumers to verify their identity before an opt-out request is honored. The Ford and, from earlier in 2025, Honda actions both cite this. Remove verification gates from opt-out flows entirely.

Priority 2: Consent Interface Design

Why it matters:

The CPPA's January 2026 regulations codified enforcement standards that were already being cited in settlements. Dark pattern violations now have a clear regulatory definition.

- **Audit for consent symmetry**. Count the steps to accept tracking and the steps to opt out. They must be equal, or opt-outs must be easier. Document this audit.
- **For opt-in consent, banner closure is not consent**. If you collect sensitive categories of personal data, many state data privacy laws require you to collect affirmative, opt-in consent before you can collect that data. You may choose to adhere to an opt-in standard to protect yourself from wiretap lawsuits as well. If you adhere to an opt-in standard of consent, know that closing a consent banner does not count as consent. Treat a consumer who closes a banner without selecting an option as a consumer who has not consented.
- **Do not gate service access on consent**. Under CCPA, you cannot deny goods or services, or offer degraded service, because a consumer opted out of data sharing. Requiring users to click “agree” before purchase flows or core features is a direct violation.

Priority 3: Vendor and Third-Party Governance

Why it matters:

Two of the largest California settlements included vendor contract violations as primary findings. Regulators are reviewing the actual contract language. Both Healthline and Tractor Supply ($1,550,000 and $1,350,000, respectively) featured non-compliant vendor contracts.

- **Audit contract specificity, not just existence.** CCPA-compliant service provider agreements must specify the purposes for which data can be used and prohibit its use outside those purposes. Furthermore, cross-contextual behavioral advertising is forbidden for service providers entirely.
- **Maintain a classified tracking technology inventory.** The Tractor Supply consent order required a live inventory of all tracking technologies deployed, each classified by whether it constitutes a sale or sharing of personal information and whether it is covered by a CCPA-compliant contract. This is a best practice for all businesses, though only explicitly required for Tractor Supply.

Priority 4: Children's and Sensitive Data Management

Why it matters:

Four states brought children's privacy actions in a single year (California, PlayOn Sports and Jam City; Florida and Roku; Kentucky and Character.ai; Utah and Snap). The CCPA's affirmative consent requirement for ages 13–16 is being enforced. Sensitive data categories draw the highest penalties.

- **Age-gate for under-16, not just under-13**. Under the CCPA, businesses that have actual knowledge they are serving consumers aged 13–16 must obtain affirmative authorization before selling or sharing their personal information—a requirement that goes beyond COPPA's under-13 framework and that most businesses have not operationalized. A small number of other states have adopted enhanced protections for minors in similar age ranges, though the specific requirements vary.
- **Audit all sensitive data flows**. Geolocation, health, biometric, and financial data each require specific disclosure and consent frameworks under comprehensive privacy laws. Map where these categories appear in your data flows and verify the applicable consent mechanisms are in place.
- **Don't rely on T&Cs acceptance for sensitive data consent**. The Flo Health CIPA case and Utah's Snap case both involved sensitive data collected under a general terms-of-service agreement rather than meaningful, specific consent. That consent model is not defensible for sensitive categories.

Priority 5: Privacy Notice Governance

Why it matters:

Privacy notice failures appear in virtually every enforcement action in the research period and are the most common trigger for cure letters in states that are still in that phase.

- **Audit state-by-state coverage.** Oregon's cure letters most commonly targeted notices that listed other states' rights but omitted Oregon. Audit your notice against each state whose consumers you serve. The patchwork nature of US privacy law means this requires ongoing attention as new laws take effect.
- **Update annually, and track it.** CCPA requires annual updates to privacy notices. Tractor Supply was cited for this. Maintain dated version history as documentation.
- **Cover all audiences.** Tractor Supply was the first CCPA action involving job applicant notice failures. Your privacy notice obligations extend to employees and job applicants, not just website visitors. Review HR-facing notices.
- **Add in-app policy links.** The CCPA's January 2026 regulations require mobile apps to link to the privacy policy from within the app's settings. If your mobile app is a primary consumer touchpoint, this is now an enforceable requirement.

Priority 6: Subject Rights Response Workflows

Why it matters:

Misconfigured request portals are a direct CCPA violation. Incomplete responses—particularly around behavioral and inferred data—are a pattern in Oregon's cure letters.

- **Test your request portal technically.** Treat portal functionality as a monitored system with alerting, not a set-it-and-forget-it form.
- **Include behavioral and inferred data in access responses.** Oregon's enforcement data shows that businesses consistently fail to include marketing profiles, shopping behavior histories, and inferred interest categories in access request responses—providing only basic account information instead. That is not a complete response under most comprehensive privacy laws.
- **Do not require verification for opt-out.** The CCPA prohibits identity verification as a prerequisite to opt-out. For other request types, verification must be proportionate to the sensitivity of the data requested.

Priority 7: Regulatory Engagement and Audit Response Planning

Why it matters:

The enforcement actions in this report did not all result in penalties because violations were uniquely severe. They resulted in penalties—or escalated to public enforcement—in significant part because of how companies responded when regulators made contact. TicketNetwork misrepresented its compliance status and failed to respond to follow-up correspondence. Tractor Supply challenged the CPPA's subpoena authority, triggering a judicial action before ultimately settling. The companies that avoided monetary penalties generally did the opposite: they engaged promptly, remediated demonstrably, and gave regulators no reason to escalate.

With cure periods now expired in most active privacy law jurisdictions, and the CPPA disclosing hundreds of open investigations, the question is no longer whether your organization might receive regulatory contact. It is whether you are prepared to respond in a way that reduces rather than compounds your exposure.

- **Designate a regulatory response lead before contact arrives.** Identify in advance who within your organization will manage communications with a privacy regulator—and ensure that person knows to engage outside counsel before responding. The instinct to handle an inquiry informally or delay a response while investigating internally has produced bad outcomes repeatedly in this enforcement period.
- **Do not misrepresent your compliance status.** This sounds obvious, but the TicketNetwork record shows it happens. If your organization has not fully remediated an identified issue, say so and provide a timeline. Regulators consistently treat partial compliance with transparency more favorably than misrepresented compliance that unravels under follow-up. AG Tong's public statement about TicketNetwork specifically called out the misrepresentation as the reason the AG proceeded to penalty rather than continued working toward cure.
- **Document remediation contemporaneously.** The Tractor Supply and PlayOn Sports orders both credit remediation efforts—but only because those efforts were demonstrable. Maintain records showing what was identified, when it was fixed, and what testing confirmed the fix. The CPPA and state AGs are asking for evidence of remediation, not assurances of it.

Section 4

How Osano Can Help

The enforcement actions documented in this report share a common thread: violations were not primarily the result of bad intent. They were the result of gaps between what a privacy program was supposed to do and what it actually did.

Healthline had opt-out mechanisms, but they didn't work—over a hundred tracking cookies kept firing after consumers exercised every available opt-out. Ford used a legacy privacy solution vendor to manage their opt-out form and deployed an out-of-the-box configuration, assuming it was compliant. In each case, the program looked fine on paper, but regulators tested the mechanisms and found otherwise.

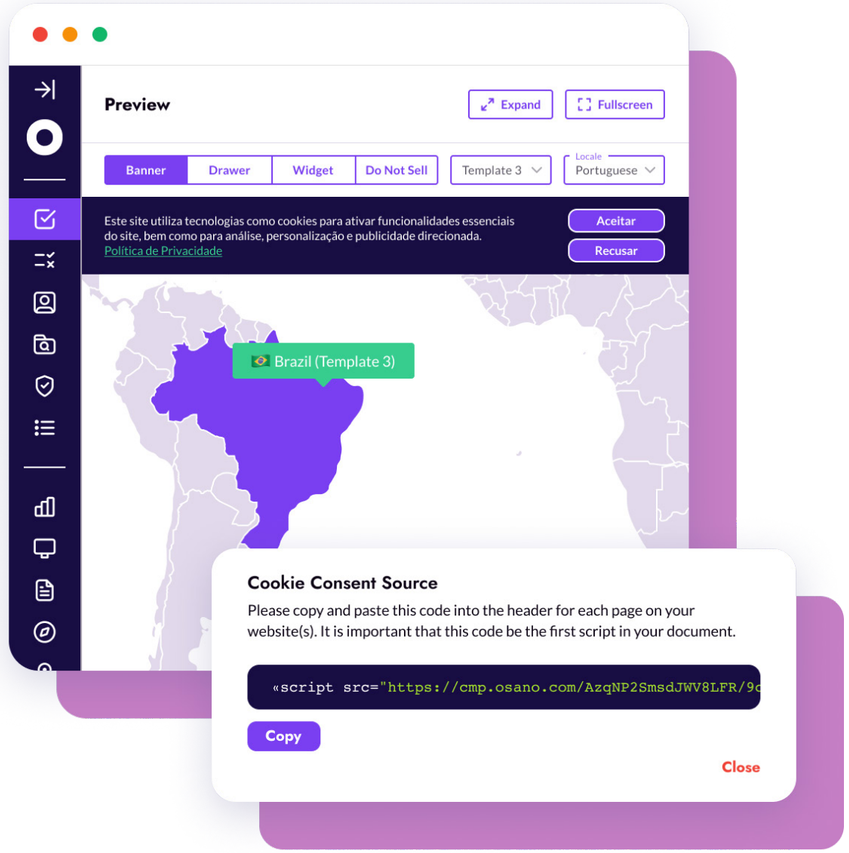
Closing those gaps is what the Osano platform is built for.

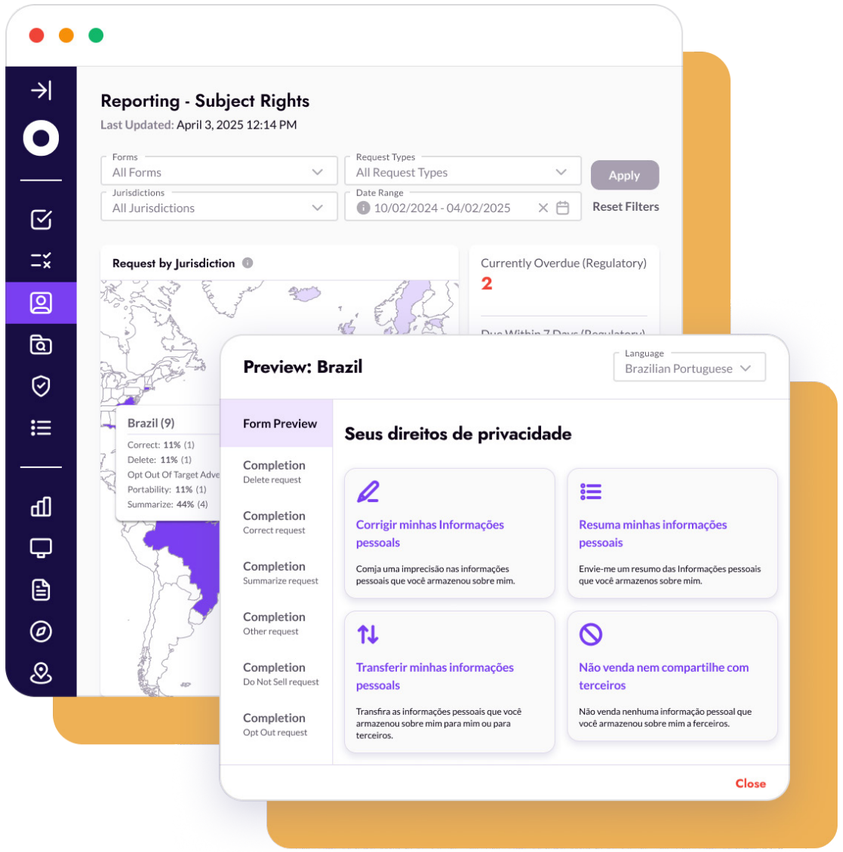
Manage Consent with Cookie Consent

When a consumer submits an opt-out request, passes along a GPC signal, makes a choice on a banner, or otherwise indicates their privacy preferences, both you and the consumer expect that opt out to work.

But the most common CCPA violation in this period was a consent interface that said one thing and did another. The CPPA regulations effective January 1, 2026, codified what the enforcement record had already established: consent mechanisms must work technically, not just visually.

Osano's Cookie Consent platform manages consent for data privacy laws across 50+ countries and all US state requirements. It displays the right notice to the right user, captures their choice, enforces it across your digital properties, and keeps a documented record of what was agreed to and when. For businesses facing GPC compliance obligations—now mandatory in 12 states—it provides the technical infrastructure to recognize and honor those signals automatically.





Respond to DSARs/SRRs with Subject Rights Management

Privacy laws don't just require consent collection. They give individuals the right to know what data a company holds about them, request its deletion, or opt out of its use—and they require businesses to respond within defined timeframes. During the past year, Oregon's enforcement data showed that misconfigured or inaccessible request forms are among the most common deficiencies identified in cure letters.

Osano Subject Rights Management enables you to manage consumer requests through a structured intake workflow with documented responses, automation, and a full audit trail. Requests are captured, queued, assigned, and tracked to completion—and common requests like summaries and deletions are automatically fulfilled pending human review. When a regulator asks how a specific deletion request was handled 18 months ago (and the enforcement record from this period shows they do ask), the answer is documented and retrievable.

Verify with Compliance Check

A consent management platform is configured once. Websites change constantly. New tags, scripts, and third-party tools can introduce compliance gaps overnight—a broken opt-out signal, a missing banner on a new landing page, a DSAR form that stopped working after a site update. The Tractor Supply consent order specifically required quarterly scanning of all digital properties and a current inventory of all tracking technologies deployed. That is now a documented regulatory expectation, not a best practice.

Compliance Check runs automated scans across multiple domains and flags issues before they become problems. Every scan is timestamped and exportable. When a regulator, auditor, or board member asks for proof that your privacy program is working—not just configured—you have it.

Requirement	Results	Status
Consent collection mechanism must exist	Cookie banner found	Pass
Consent collection must respect choice symmetry	Cookie banner buttons are missing or lack equal prominence	Fail
Privacy policy must exist	Privacy policy found	Pass
Privacy policy must have been updated in the last 12 months	Privacy policy last update date not found	Fail
Privacy policy must contain a subject rights intake method	Subject rights intake method found	Pass
Global Privacy Control signal must be honored	Global Privacy Control signal not honored	Fail

Scan Your Site

Test Out Compliance Check

With the past year establishing a rigorous enforcement cadence from privacy regulators in the US, the best time to get compliant was yesterday; the second best time is now. If you want to see where your organization stacks up against regulatory standards, you can conduct a free scan of your site with Compliance Check.

See if your site is honoring GPC signals, relies on dark patterns, and meets other data privacy requirements.

Scan Your Site

The Only Compliance Guarantee in the Industry

Managing consent, responding to subject rights requests, and verifying that the program works are not optional components of a privacy program. Every comprehensive state privacy law that took effect or was enforced during this period requires all three. The Osano Basic Privacy Bundle brings them together in a single platform you can deploy without adding headcount or operational complexity.

And if something goes wrong anyway: if you receive a fine or penalty from a regulatory agency while using the platform, Osano covers it—up to $500,000. No fines. No penalties. Guaranteed.