
2026 Fall Privacy Report

Navigating the Evolving Legal
Landscape of Data Privacy,
Cybersecurity, and AI



Contents

03	Introduction
	Artificial Intelligence
04	AI Compliance: What Businesses Need to Know and Do Now
09	Agentic AI Meets CFAA and CDAFA: Ninth Circuit Issues Ruling Involving Agent Liability
	State Consumer Privacy Laws
11	States Target Sensitive Data, Location Data, and Data Brokers
13	Four New State Privacy Laws in 2026: What Businesses Need to Know
17	New Jersey Enacts the Nation’s Broadest Data Broker Law: What Your Business Should Know
19	Connecticut Expands Privacy Requirements for Sensitive Data, AI, and Profiling
21	Delaware Significantly Expands Its Privacy Law: What Your Business Should Know
	CalPrivacy and CCPA Enforcement
24	CalPrivacy’s Data Broker Enforcement Blitz Signals Increased Scrutiny
27	CCPA Cybersecurity Audit Requirements: Building an Audit-Ready Security Program
31	California DROP Deletion Requests Are Underway
32	CalPrivacy Targets Gig Economy Platforms In First CCPA Sectoral Audit
	Children’s Privacy
33	Children’s Privacy in 2026: Enforcement Moves Into Product Design
	Privacy Litigation Trends
37	CIPA Litigation and Reform: Variety Media, SB 690, and the Future of Website Tracking Claims
39	California’s ALPR Law in Focus: A Posted Privacy Policy Matters More Than Ever
42	Privacy, Cybersecurity & AI: Questions to Consider Going Into 2027
44	Contact

Introduction

For businesses, the rules governing AI and personal information are being rewritten in real time, and the cost of falling behind has never been higher. AI touches nearly every aspect of daily life and has become near ubiquitous in businesses across the country. At the same time, consumers are becoming increasingly savvy about their individual privacy rights, demanding more information and stronger protections from the businesses to which they provide personal information. Reflecting the importance of these two issues, states are rapidly enacting, updating, and amending their privacy and AI laws. There are now 24 states with comprehensive consumer privacy laws, with piecemeal, topic- or industry-specific privacy and AI laws popping up across the country as well. Children's data and other sensitive data collection and use are particular areas of concern and focus. The federal government continues to weigh federal legislation, but has not, to date, passed any federal laws on either AI or privacy, leaving enforcement largely to the states and their patchwork of requirements. Adding to the complexity, courts and regulators are applying decades-old statutes to new technologies, and regulators and private plaintiffs are more active than ever in examining and testing the bounds of privacy laws and consumer privacy rights. The result is a legal landscape more complex than ever before. What are businesses to do? How do businesses keep up with the ever-changing legal landscape?

This report untangles the web of recent AI and privacy laws and provides concrete takeaways to help businesses navigate this landscape.

- First, the report examines the relatively nascent state of AI laws around the country.
- Second, it surveys the recent additions and amendments to the slate of comprehensive state consumer privacy laws.
- Third, it reviews the California Privacy Protection Agency's (CalPrivacy) recent enforcement actions and priorities, as well as upcoming obligations under the California Consumer Privacy Act (CCPA).
- Fourth, it analyzes recent trends in children's privacy, a hot-button issue and subject of recent litigation settlements and legislation.
- Fifth, it evaluates trends in the litigation space, including the recently passed California SB 690 and the fate of California Invasion of Privacy Act (CIPA) claims.
- Finally, it concludes with a checklist to help businesses manage upcoming deadlines and obligations.

AI Compliance: What Businesses Need to Know and Do Now

“

You cannot govern what you have not mapped.

Businesses can no longer wait to take AI compliance seriously. While there is still no federal AI statute, more than 60 state laws now regulate various aspects of commercial AI, and there is already substantial litigation involving business use of AI tools, largely brought under privacy, wiretap, and biometric statutes that predate the technology by decades. The good news for businesses is that most of what these new AI regimes require is familiar: inventory, notice, consent, vendor terms, retention limits, and human review.

If your business has not evaluated its own AI compliance, both in terms of the tools used internally and any products, services, or tools deployed as part of its business operations, now is the time to do so.

1. Laws to Know

Federal

Recent federal policy has moved toward light-touch AI regulation and a single national framework. The current administration is challenging state AI laws and pressing Congress to preempt them, but that effort has not yet displaced any state laws. Taking a lesson from privacy law, businesses should not take a wait-and-see approach in reliance on a future federal AI regime or preemption that may never happen. For now, companies should make plans to comply with state AI and privacy laws and rules that apply to their products, users, and data.

Notably, the FTC can act under Section 5 of the FTC Act even when no AI-specific statute applies. Businesses can face enforcement for undisclosed or misleading AI practices, including sharing user data with outside AI developers in a way its privacy disclosures do not explain.

States—Four Primary Areas of Legislation

- **Chatbots—the most active area of AI lawmaking.** California, New York, Connecticut, Colorado, Washington, and several other states have adopted chatbot laws and rules. The details vary, but three obligations are common: (1) disclose when a user is interacting with AI, (2) maintain protocols to detect and respond to self-harm concerns, and (3) protect minors.

Coverage turns on how a state defines a chatbot. Some rules reach ordinary customer-service bots, while others focus on companion systems that simulate relationships or remember prior interactions. These laws generally apply based on where your users are located, not where you are incorporated, so a nationwide chatbot should be built to the strictest applicable standard.

- **Automated decisions about people.** New AI laws and rules are focusing on significant decisions made by AI or automated means. If AI helps decide who gets hired, fired, admitted, housed, insured, or provided services, the company using it should be prepared to disclose the use, explain the decision process, and document testing and oversight. Where states are splitting is the threshold question: how much AI involvement triggers those duties.

California's CCPA rules reach technology that replaces or *substantially replaces* human decisionmaking, meaning the output is used without meaningful human involvement. A reviewer who understands the output, weighs other relevant information, and has authority to change the result keeps the use outside the rules. Rubber-stamping does not.

Colorado's proposed SB 26-189 sets a broader trigger: AI that *materially influences* a consequential decision in seven areas including employment, housing, lending, insurance, and healthcare.

The proposed law would also require notice after an adverse outcome and let individuals correct the underlying data and seek human reconsideration. The statute does not define “materially influences,” and the Attorney General has asked for comment on competing standards.

The practical consequence: keeping a human in the loop may take you outside some state laws but not others. Inventory where AI *informs* decisions about people, not only where it makes them on its own.

- **Sectoral laws, content regulation, and AI-as-privacy.** Specific review of AI laws based on industry sector is important, as states continue to regulate AI more restrictively in contexts such as healthcare, employment, and insurance, requiring express notice and consent and restricting uses in various contexts. States are also regulating AI *content*, including restricting deepfakes, digital replicas, and AI use in election contexts. And many states, including California, continue to regulate many aspects of AI as part of privacy law compliance.
- **Developer and frontier-model laws.** Finally, we continue to see state laws governing large-scale AI systems. California, New York, and Illinois are imposing safety frameworks, incident reporting, and independent review requirements on developers of powerful frontier AI systems. And while this may not apply to most businesses, everyone who deploys or uses large AI models should monitor these trends.

California-Specific Laws

The CCPA’s rules on automated decisionmaking technology (ADMT) and privacy risk assessments create the clearest near-term deadlines for AI compliance for many businesses:

- **ADMT—January 1, 2027.** If you use automated technology to make or materially influence significant decisions about California residents (employment, lending, housing, education, healthcare, or essential services), you need published pre-use notices, working opt-out and access workflows, and an explanation of the logic and effects. Employees, applicants, and

contractors are included beyond commercial consumers.

- **Risk assessments—underway since January 1, 2026.** As of now, businesses subject to the CCPA must conduct risk assessments for high-risk processing activities and must submit attestations and summaries to the CCPA by April 1, 2028. High-risk processing includes ADMT uses.

California’s Legislature closed its 2026 session with a package of AI and privacy measures, including several laws aimed at regulating business/employer use of AI:

- **SB 947**—Bars sole reliance on automated systems for employee discipline or termination; requires human corroboration, post-use notice, and employee data access. Operative July 1, 2027.
- **SB 951**—Amends Cal/WARN to require additional disclosures when layoffs are caused substantially by AI or automation.
- **AB 1883**—Categorically prohibits employer use of AI tools to infer emotional states or collect neural data, with no wellness-program exception.
- **AB 1331**—Prohibits workplace surveillance tools in restrooms.
- Other measures include **SB 923** (expanded deletion rights), **AB 1609** (chatbot disclosures), and additional rules on data sharing and professional AI use.

The EU AI Act

If your business offers AI-enabled products or services to people in the EU, the EU AI Act can reach you without an EU entity. The EU AI Act applies based on where a system is placed on the market or where its output is used. Compliance obligations scale with risk, and the heaviest requirements fall on “high-risk” uses, which for most US companies means hiring and HR screening tools, credit decisions, and education or admissions systems.

2. Litigation and AI Tool Trends

AI notetakers are a current hot spot. If your company uses an AI notetaker, treat the tool as more than a transcription service. In August 2026, a California court allowed claims against Otter.ai to proceed after plaintiffs alleged that its speaker-tagging feature created voice profiles without the required consent. The same theory has been asserted against other tools, including one tool that took notes without

visibly joining the meeting. Before deployment, confirm what data or inputs the tool/vendor records, how long it keeps the data, and whether it uses it for anything beyond providing the service. If so, a court may view it as a separate party and not merely your service provider, and thus subject to heightened notice and consent obligations.

Exposure is not limited to the AI tool/vendor. A company that deploys the tool may also be named, particularly if it helped decide how recordings or voice data were collected, used, or retained. Illinois's BIPA allows private suits and statutory damages of \$1,000 per negligent violation and \$5,000 per intentional or reckless violation, or actual damages if greater. Recent class actions involving voiceprints from public recordings show how quickly these theories can spread. Speaker identification, voice authentication, and emotion detection are all risk areas.

Chatbots and website tracking. Claims under California's CIPA involving website chat functions, session replay, and tracking pixels continue to increase and provide statutory damages of \$5,000 per violation with no proof of harm required. California's SB 690 would limit some pen-register and trap-and-trace claims involving websites and apps, but it does not eliminate the broader litigation risk under wiretapping/electronic communication legal theories.

Employment. Using a well-known AI hiring tool or vendor does not shield an employer from discrimination claims. AI screening tools used on an employer's behalf can expose the employer to liability. Businesses using these tools should run bias audits through counsel where appropriate, and document the scope, methodology, and results.

AI-driven pricing. Dynamic pricing, which involves adjusting prices based on supply, demand, time of day, or competitor pricing, is a long-established business practice, and AI generally makes it faster and more efficient. But risk arises when a system uses personal consumer data, such as browsing behavior, purchase history, location, income proxies, or demographic information, to estimate an individual's willingness to pay and set a price accordingly. That is personalized, or "surveillance," pricing.

In August 2026, the FTC proposed an enforcement policy statement making these practices a key focus. Its position is that a business using consumer data to personalize prices should clearly disclose that the price is personalized, the basis for the personalization, and the types of data used; failing to do so may violate Section 5 as deceptive or unfair.

State consumer-protection statutes, privacy laws, and emerging state personalized-pricing legislation create additional risk, and models trained on historical data may produce prices that correlate with race, income, age, or other protected characteristics, creating civil-rights liability even without discriminatory intent. For business clients, the practical line is straightforward: dynamic pricing based on market conditions is generally permissible; personalizing prices from individual consumer data without disclosure is where the legal risk sits. If your business uses AI in pricing, review what data feeds the model and whether consumers know about it.

AI in Litigation and Discovery

Courts are treating AI prompts and outputs as ordinary business records rather than a protected category. For business teams, that means assuming employee chats, meeting transcripts, and AI tool logs may be requested in litigation.

- **Prompts entered into public AI tools are generally not confidential.** Asking a chatbot a legal question does not create an attorney-client communication, and using a consumer-grade tool undercuts any later claim that the exchange was privileged.
- **Employee prompts can become evidence against the company.** Courts have relied on chatbot conversations to establish what decision-makers were actually thinking, including where the stated business rationale differed from the exchange.
- **Deleting AI logs creates a second problem.** Once litigation is reasonably anticipated, AI records carry the same preservation obligations as email, and destroying them invites spoliation arguments on top of whatever the underlying dispute is.
- **Work product protection may survive when counsel directs the use.** Where an attorney structures the prompts or supervises the work, protection is more likely — but the law is unsettled, and the conservative assumption is that prompts, outputs, transcripts, and logs are discoverable unless counsel has directed otherwise.

- **Update preservation infrastructure now.** Litigation holds, custodian interviews, and discovery templates should expressly cover AI prompts and outputs, meeting transcripts and summaries, and related metadata — categories most existing templates do not name.
- **Recording expands the record.** Every AI-generated transcript or summary is a new discoverable document, and one that may not match the formal minutes of the same meeting.

Regulators are Active

State attorneys general are leading AI enforcement by using consumer-protection, civil-rights, and privacy laws that already exist. A coalition of AGs recently warned major AI companies about harmful outputs, and individual states have pursued chatbot operators and AI developers through investigations, injunctions, criminal referrals, and new legislation. Businesses should take note that regulators do not need to wait for AI-specific statutes before acting. They are adapting current laws to these new technologies.

3. Internal AI Use: Risks and Safeguards

Businesses should start from the assumption that AI is already in your workplace. Global survey data puts regular, intentional AI use at roughly three in five workers, and vendors are enabling AI features inside software you already license, sometimes without explicit notice. It is unlikely any business can still represent that they do not use AI, and broad AI tool bans are no longer practical.

Adopt a policy, but do not impose a ban. Prohibition on use of AI tools drives AI use underground, where it cannot be supervised. A workable policy identifies approved and prohibited tools and uses, states what may never be entered into an AI tool, addresses confidentiality and privacy, requires verification, assigns accountability for final work product, and explains consequences. Without a policy, every employee sets their own rules, with many using AI quietly and never disclosing it. Businesses should take a practical approach and reasonably regulate internal AI use. AI policy updates and employee trainings should be expected regularly as AI tools and the legal landscape continue to evolve rapidly.

Watch for AI tools that act, not just advise. Agentic AI systems can approve transactions, send communications, screen applicants, manage workflows, or make decisions with limited human involvement. These tools are arriving quickly, often embedded in software businesses already use, and the compliance stakes rise when the system acts rather than merely provides information. Inventory where AI is taking actions and ensure that appropriate human oversight and audit trails scale with the tool's level of autonomy.

Use enterprise tools, not free or consumer accounts.

Businesses should contract for closed AI systems that prohibit vendor retention, training on your data, and third-party disclosure. The gap between a company's enterprise account and an employee's personal free account now has real, legal consequences. Policies should make the distinction explicit and enforce it.

Make a deliberate decision about meeting assistants.

We previously addressed these tools here, but the information bears mentioning again. Treat these tools as communications-capture tools rather than productivity software:

- Designate meetings where they are never permitted—privileged advice, investigations, HR and accommodation discussions, board deliberations, transactions, and anything involving client-confidential, patient, or applicant information.
- Provide participant-facing notice and capture consent, keeping in mind all-party consent states and external participants who never agreed to your vendor's terms.
- Disable speaker identification where a plain transcript will suffice. That setting is often the difference between a transcript and a biometric identifier.
- Confirm that administrators can set defaults centrally instead of leaving recording, sharing, and training settings to individual users.
- Reconcile AI summaries against formal minutes. Discrepancies get scrutinized, and verbatim transcripts preserve offhand remarks that curated minutes would omit.

Set retention and deletion rules. Don't just let AI tool data sit in your systems. Set retention rules and deletion schedules for each category of data these tools generate, including the audio, transcripts and summaries, voice profiles, associated metadata, downloaded exports, and copies that linger in CRM or collaboration systems even after the original is deleted.

Maintain human oversight for important AI-generated output. Several new laws now require it, and many business contracts are now demanding it.

4. Three Priorities Before January 1, 2027

- 1. Build your AI inventory.** You cannot govern what you have not mapped. Document every AI tool, system, and AI-enabled feature in use, as well as the data it touches, and the risk tier.
- 2. Map your exposure.** Based on your AI inventory, identify applicable laws and legal requirements. California's ADMT compliance, Colorado's replacement automated-decision law, new state chatbot requirements, and many other laws are going into effect January 1, 2027, and many other laws are already in effect.
- 3. Name one accountable owner.** When legal, HR, security, and the IT function each hold a piece of ownership, the seams between them are where problems go unnoticed. A single senior executive with a clear escalation path closes those seams.

The Bottom Line

AI can no longer be ignored. Whether or not your company has formally adopted it, AI is almost certainly already in use—in tools your employees chose, and in features your vendors switched on without asking. The starting point is not a policy. It is a set of questions every business should be able to answer:

- What AI are we using, including features enabled by default in software we already license?
- Have we disclosed that use to the people it affects—customers, employees, applicants, and meeting participants?
- What do our AI vendors do with our data, and can we turn it off?
- How long do we keep AI-generated content, and can we delete it when we need to?
- Who inside the business owns AI compliance and has authority to act?

Few companies can answer all five questions today. The ones that can will find most new obligations are variations on work they have already done—and the ones that cannot will likely discover the gaps through a regulator's inquiry or a plaintiff's discovery request. Ensuring your business can answer these questions now will put you in a good position to deal with the continuing evolution of AI laws and regulations.

Agentic AI Meets CFAA and CDAFA: Ninth Circuit Issues Ruling Involving Agent Liability

The U.S. Court of Appeals for the Ninth Circuit recently issued a novel ruling that an agentic AI tool did not trigger liability under the Computer Fraud and Abuse Act (CFAA) and the California Comprehensive Computer Data Access and Fraud Act (CDAFA)—statutes that often appear as companion claims in privacy cases involving unauthorized access to computers, devices, or data.

On August 4, 2026, in *Amazon.com Services, LLC v. Perplexity AI, Inc.*, No. 26-1444, the Ninth Circuit vacated the trial court’s award of a preliminary injunction to Amazon, holding that Amazon was unlikely to succeed on the merits of its CFAA and CDAFA claims because it could not show Perplexity’s agentic AI tool “accessed” Amazon computers, a requirement of both statutes.

While the Court expressly limited its narrow ruling, this first-of-its-kind decision offers a glimpse into how courts may approach agentic AI issues in similar contexts, and raises broader questions about when agentic AI may trigger liability for statutory or other privacy-related violations.

Background

This case involved Perplexity’s AI-enabled web browser, Comet, which it developed and publicly released. Comet runs locally on a user’s machine and includes an AI agent (which the Court refers to in its opinion as “the Assistant”) that performs tasks at the user’s direction, including online shopping.¹

Amazon allegedly told Perplexity, prior to Comet’s release, that its AI products would not be allowed to access the Amazon.com store.² After Perplexity released Comet, Amazon detected that the Assistant was shopping its store on behalf of Comet users, and Amazon again informed Perplexity that the Assistant was not authorized to use the store or make purchases for its customers.³

Amazon then filed suit against Perplexity for violations of the CFAA and the CDAFA and moved for a preliminary injunction to prohibit the use of Perplexity’s agentic web browser AI tool on Amazon’s website.⁴

Amazon claimed that Perplexity violated the CFAA, a federal anti-hacking statute, and its California state-law analogue, the CDAFA.⁵ Both are criminal statutes that provide a private right of action for civil claims. The CFAA prohibits intentionally accessing and obtaining information from computers without authorization, and makes relief available to plaintiffs who have suffered damage or loss of at least \$5,000 per year as a result of a violation.⁶ The CDAFA similarly prohibits knowingly accessing without permission any computer system or network, but it does not impose a minimum loss threshold.⁷

Amazon claimed that by way of the Assistant, Perplexity’s servers had accessed Amazon’s servers without Amazon’s authorization.⁸ Perplexity countered that its own computers never gained “access” to any Amazon computer or server, because when the user deploys the Assistant, any Amazon data is first transmitted to the user’s computer—and any “intent” would belong to the user, not Perplexity, as the Assistant is computer software.⁹

¹ *Amazon.com Services, LLC v. Perplexity AI, Inc.*, 184 F.4th 1083, 1087–88 (9th Cir. 2026).

² *Id.* at 1088.

³ *Id.*

⁴ *Id.*

⁵ *Id.*; 18 U.S.C. § 1030; Cal. Penal Code § 502.

⁶ 18 U.S.C. § 1030(a)(2), (g).

⁷ Cal. Penal Code § 502. For more information on the recent rise in CDAFA claims in the privacy context, including with regard to website tracking technologies, see our prior article [here](#).

⁸ *Id.* at 1089–90.

⁹ *Id.* at 1089.

The Court Rejects Amazon's Argument

The Court ruled in favor of Perplexity, vacating the preliminary injunction and concluding that Amazon was unlikely to succeed on the merits because it failed to show that Perplexity “accessed” Amazon’s servers as required under the CFAA and the CDAFA.¹⁰ The Court determined that the evidence did not support Amazon’s argument that Perplexity itself directly communicated with Amazon’s servers, as it is the user who controls the Assistant to carry out shopping tasks on Amazon.com.¹¹ It further explained that the plain language of the CFAA does not allow for “access” by the Assistant, as “access” only applies to a person—and “[h]owever advanced the Assistant currently is, it is a tool, not a person for statutory purposes.”¹²

The Court reiterated that agentic AI is an emerging technology, and that this decision does not “establish a new legal regime governing agentic AI”—nor does it address the potential for liability in other contexts such as tort claims.¹³ It also acknowledged that “[t]he legal understanding of agentic AI will doubtless change as AI technology grows increasingly sophisticated.”¹⁴ However, this case represents an early marker in what is sure to become a hotly contested issue going forward.

Key Takeaways

As the Court noted, this ruling is limited and does not insulate agentic AI developers or deployers from potential liability under these statutes or other laws, nor from claims based on violations of a website’s terms of service.

It does, however, provide a novel illustration of a court conducting a piecemeal analysis of how an agentic AI tool operates to determine liability, including an examination of who controls—and may ultimately be responsible for—the actions that the agent undertakes. As this case shows, each outcome may depend on highly factual questions, including how the tool is built and whether the agent is acting only on behalf of the user.

As the law evolves to keep pace with the rapid advancement of agentic AI, companies should stay informed about key judicial decisions and legislative activity and their potential implications for the AI tools that they develop and deploy.

¹⁰ *Id.* at 1090–91.

¹¹ *Id.* at 1091.

¹² *Id.*

¹³ *Id.* at 1092.

¹⁴ *Id.*

States Target Sensitive Data, Location Data, and Data Brokers

“

A traditional state-by-state applicability analysis may not capture all of a business's privacy obligations.

States continued to adopt more targeted privacy requirements in 2026, including new restrictions on precise geolocation and sensitive personal data and expanded requirements for data brokers. These laws are important even for businesses that have already determined whether they are subject to each state's comprehensive privacy law because some requirements apply based on the type of data or activity involved rather than traditional consumer-volume or revenue thresholds.

Recent developments in Vermont, Maryland, Virginia, and New Jersey illustrate this broader shift toward regulating specific categories of data and data-processing activities.

Vermont Expands Data Broker Requirements

Vermont expanded its data broker requirements in 2026, adding new disclosure and financial requirements for registered data brokers.

The amendments expand required registration disclosures to include certain sensitive-data practices and disclosures to government bodies, law enforcement, foreign actors, and generative AI developers.

These requirements may be particularly relevant for data brokers that maintain detailed consumer profiles or provide personal information to multiple types of recipients. The specific inclusion of disclosures to generative AI developers also illustrates the increasing overlap between state privacy and AI regulation.

Vermont's amendments also require registered data brokers to maintain a \$20,000 bond for liabilities arising under the law.

Businesses that buy, sell, or license personal information should determine whether they qualify as a data broker under Vermont law and, if so, confirm that their registration disclosures and financial requirements reflect the amendments.

Maryland Expands Its Definition of Precise Geolocation

Maryland expanded the definition of precise geolocation information under its privacy law. The definition now includes information identifying the location of a consumer, mobile device, or vehicle within a radius of 1,750 feet.

Businesses that collect location information should review whether data they previously treated as general location information may now fall within Maryland's definition of precise geolocation information and become subject to additional restrictions.

Virginia Prohibits the Sale of Precise Geolocation Information

Virginia has adopted a more direct restriction on precise geolocation data by prohibiting businesses from selling or offering to sell precise geolocation information.

Businesses that collect location information should therefore understand not only whether they collect precise geolocation data, but also how that information moves through advertising, analytics, vendor, and other third-party relationships.

The Maryland and Virginia developments demonstrate the growing importance of treating location information as a distinct category when conducting data inventories and reviewing third-party data flows.

New Jersey Prohibits Sale of Sensitive Personal Data

New Jersey has taken an even broader approach to sensitive information by prohibiting the sale of sensitive personal data.

Significantly, the prohibition applies regardless of the number of New Jersey consumers whose information a company processes. A business may therefore fall outside the applicability thresholds of New Jersey's comprehensive privacy law and still be subject to the sensitive-data sale prohibition.

As we discussed in our [separate article](#) on New Jersey's new data broker law, the restriction applies broadly to sensitive information, including certain health, financial, biometric, precise geolocation, and other sensitive personal data.

What Businesses Should Do Now

These developments reinforce the need to look beyond the applicability thresholds of state comprehensive privacy laws. Businesses should:

- **Map sensitive and location data.** Identify sensitive personal data, precise geolocation information, biometric data, and other specially regulated information and understand how that information is used, sold, licensed, and shared.
- **Review data sales and third-party disclosures.** Determine whether advertising, analytics, licensing, or other data-sharing arrangements involve information subject to state-specific restrictions.
- **Review data broker requirements separately.** Businesses that buy, sell, or license personal information should evaluate data broker laws on a state-by-state basis rather than assuming their status under one state's law determines their obligations elsewhere.
- **Do not rely solely on comprehensive-law thresholds.** Identify requirements that apply based on the type of data or processing activity even where the business does not otherwise meet a state's general privacy-law thresholds.

The growing number of targeted state requirements means that a traditional state-by-state applicability analysis may not capture all of a business's privacy obligations. Businesses should increasingly consider both where they operate and the specific types of data and processing activities involved.

Four New State Privacy Laws in 2026: What Businesses Need to Know

“

Meaningful differences among states still require businesses to evaluate their practices state by state.

Less than a decade after California enacted the California Consumer Privacy Act (CCPA) in 2018, privacy legislation has spread to nearly half of the United States. With Alabama, Louisiana, Oklahoma, and Vermont joining the list this year, 24 states now have their own comprehensive consumer privacy laws, with at least three more regulating privacy through more targeted legislation.

With privacy a clear legislative priority across the country, businesses should expect privacy compliance to remain an increasingly important operational and legal issue. But the growing number of laws is not the only challenge.

Although the four new laws generally follow the framework established by existing state privacy laws, they differ in important ways. Businesses with multistate privacy programs should consider whether those differences require updates to their existing notices, consumer-rights procedures, data inventories, and risk-assessment processes.

Oklahoma Consumer Data Privacy Act, effective January 1, 2027

Oklahoma's law applies to businesses that operate in Oklahoma or target its residents and either:

- control or process the personal data of at least 100,000 consumers; or
- control or process the personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.

“Consumer” excludes individuals acting in a commercial or employment context, and “sale” is limited to exchanges for monetary consideration only. The law also exempts financial institutions and data subject to the GLBA, HIPAA-covered entities, and business associates, nonprofits, and higher education institutions.

Consumers receive familiar rights to access, correct, and delete personal data and opt out of targeted advertising, sales, and certain profiling. Businesses must obtain consent before processing sensitive data and conduct data protection assessments for certain higher-risk processing. Comparable assessments prepared for other state laws may be used.

There are, however, several differences businesses should note. Oklahoma requires authentication for

consumer rights requests, including opt-out requests, and does not require businesses to recognize universal opt-out mechanisms. Its definition of personal data also expressly includes pseudonymous data when it is used with additional information that reasonably links the data to an identified or identifiable individual. And while the law generally excludes photographs and audio or video recordings from its definition of biometric data, that exclusion does not apply when data generated from those materials is used to identify a specific individual.

The Oklahoma Attorney General has exclusive enforcement authority. Businesses receive 30 days to cure alleged violations, and statutory damages may reach \$7,500 per violation.

Alabama Personal Data Protection Act, effective May 1, 2027

Alabama's law applies to Alabama businesses, or businesses targeting Alabama residents, that:

- control or process the personal data of more than 25,000 consumers, excluding data processed solely for payment transactions; or
- derive more than 25% of gross revenue from the sale of personal data.

The law also exempts businesses with fewer than 500 employees that do not sell personal data, among other entity- and data-level exemptions.

The law provides familiar consumer rights, including access, correction, deletion, and copies of their personal data, as well as opt-outs from targeted advertising, sales of personal data, and certain profiling. Businesses must obtain consent to process sensitive data. Alabama also provides additional protections for minors: businesses generally must obtain consent before using the personal data of consumers ages 13 through 15 for targeted advertising or selling that data.

However, Alabama differs from the other new laws in several respects. Its definition of a “sale” is broader than monetary consideration, but it generally does not treat certain disclosures or transfers for analytics or marketing services as sales of personal data. Alabama’s law also does not require formal data protection assessments, does not require businesses to recognize universal opt-out signals, and does not provide a consumer right to appeal a decision on a rights request.

Enforcement is limited to the Alabama Attorney General, with a 45-day cure period that does not sunset.

Louisiana Data Privacy Act, effective January 1, 2027

Louisiana’s law applies to businesses that operate in Louisiana or target its residents and meet any one of the following thresholds:

- annual gross revenue exceeding \$25 million;
- annually processing, buying, receiving, selling, or commercially sharing the personal information of at least 75,000 Louisiana consumers, households, or devices; or
- deriving at least 50% of annual revenue from the sale of consumer personal information.

Because the revenue threshold applies independently of the amount of personal information processed, the law may reach some businesses, including certain B2B companies, that would not otherwise expect to fall within a state comprehensive privacy law.

As with Oklahoma and Alabama, the law provides familiar consumer rights, including access, correction, deletion, portability, and opt-outs from targeted advertising, sales of personal data, and certain profiling. Although Louisiana does not provide consumers with the right to revoke consent, businesses must obtain consent before processing sensitive data and must conduct data protection impact assessments for certain higher-risk processing. Similar to Oklahoma, Louisiana also permits businesses to rely on comparable assessments prepared to comply with other state privacy laws.

There are several other Louisiana-specific requirements to be aware of. The law requires authentication for consumer rights requests, including opt-outs, and requires recognition of universal opt-out mechanisms. The privacy policy must also include specific disclosures if a business sells sensitive personal data or biometric personal data. Unlike Texas, Louisiana does not expressly include certain pseudonymous data within the definition of personal data.

The law is enforceable only by the Louisiana Attorney General and provides a 30-day cure period, although that cure period sunsets on July 31, 2027.

Vermont Data Privacy and Online Surveillance Act, effective January 1, 2028

Vermont’s law is broader in several respects than the other state privacy laws enacted in 2026. It applies to Vermont businesses that:

- control or process the personal data of at least 35,000 consumers;
- control or process the sensitive data of at least 3,000 consumers; or
- offer for sale the personal data of at least 3,000 consumers.

Vermont also provides narrower exemptions than many other states, including no blanket nonprofit exemption and a narrower financial-institution exemption.

Consumers receive the familiar rights to access, correct, delete, and obtain copies of personal data and to opt out of targeted advertising, sales, and certain profiling. Vermont goes further, however, by

providing additional rights relating to profiling and automated decisions, including rights in certain circumstances to question a profiling result, obtain information about the reasons for the decision, and review the personal data used. Businesses must also conduct data protection assessments for certain higher-risk processing and separate impact assessments for certain profiling used to make decisions with legal or similarly significant effects.

The law also contains several requirements that businesses should flag for their existing compliance programs. Vermont uses a broader definition of biometric data that does not require the data to be processed for purposes of uniquely identifying an individual. Its definition of publicly available information is also narrower and generally excludes information aggregated into a consumer profile and inferences derived from that profile. In addition, privacy policies must disclose whether the business collects, uses, or sells personal data to train large language models.

Vermont provides additional protections for minors and consumer health data. Businesses generally may not sell personal data or use it for targeted advertising when they have actual knowledge, and willfully disregard, that a consumer is between 13 and 17 years old. The law's consumer health data requirements are particularly broad because they apply without a minimum processing threshold and restrict, among other things, access to consumer health data, certain geofencing around health care facilities, and sales of consumer health data without consent.

The Vermont Attorney General has exclusive enforcement authority. Businesses receive 60 days to cure violations during the first 18 months after the law takes effect.

Common Requirements and Important Differences

The four laws generally follow the now-familiar state privacy framework: covered businesses must provide privacy notices, honor consumer rights, and address sensitive data, targeted advertising, sales of personal information, and certain profiling.

The laws differ in important ways that may require updates to existing multistate privacy programs. Applicability thresholds vary substantially, from Oklahoma's 100,000-consumer threshold and Alabama's 25,000-consumer threshold to Louisiana's \$25 million revenue threshold and Vermont's separate thresholds for personal data, sensitive data, and data offered for sale. The states also take different approaches to nonprofit and small-business exemptions, universal opt-out mechanisms, authentication of consumer rights requests, and the treatment of pseudonymous and biometric data.

The laws also differ in their assessment requirements. Louisiana, Oklahoma, and Vermont require data protection assessments for specified higher-risk processing, and Vermont separately requires impact assessments for certain profiling activities. Alabama does not require formal data protection assessments. Businesses should also consider whether existing assessments can be used to satisfy the requirements of multiple states.

Finally, businesses should not assume that a single privacy program will address all four laws without modification. Vermont in particular adds requirements relating to profiling, minors, consumer health data, biometric data, and disclosures concerning the use of personal data to train large language models. These differences reinforce the need to review existing privacy notices, consumer-rights procedures, data inventories, assessment processes, and other compliance controls as new state laws take effect.

The continued expansion of state privacy laws makes a consistent multistate framework increasingly valuable, but meaningful differences among states still require businesses to evaluate their practices state by state.

State Comparison Chart

State	Effective Date	Scope	Consumer Rights	Cure Period	Enforcing Party	Other
Oklahoma	1/1/2027	Process data of 100,000+ consumers; or Process data of 25,000+ consumers and derive 50%+ gross revenue from sale of personal data	Access, Correct, Delete Personal Data Opt out of targeted advertising Consent required before processing sensitive data	30 days	Attorney General	Businesses not required to recognize universal opt-out mechanisms
Alabama	5/1/2027	Process data of 25,000+ consumers, excluding payment transactions; or Derive >25% gross revenue from sale of personal data	Access, Correct, Delete, Portability of Personal Data Opt out of targeted advertising Consent required before processing sensitive data Consent required for targeted advertising of 13- to 15-year-olds	45 days	Attorney General	Definition of “sale” is broader than monetary consideration Businesses not required to recognize universal opt-out mechanisms
Louisiana	1/1/2027	Annual Gross Revenue >\$25M; Process data of 75,000+ consumers; or Derive >50% gross revenue from sale of personal data	Access, Correct, Delete, Portability of Personal Data Opt out of targeted advertising Consent required before processing sensitive data	30 days, sunseting 7/31/2027	Attorney General	Privacy policy must include specific disclosures for selling sensitive personal data or biometric data
Vermont	1/1/2028	Process data of 35,000+ consumers; Process sensitive data of 3,000+ consumers; or Sell personal data of 3,000+ consumers	Access, Correct, Delete Personal Data Opt out of targeted advertising Consent required before processing sensitive data Question certain profiling results Obtain information about automated decisions No selling data or targeted advertising for 13- to 17-year-olds	60 days, sunseting 6/30/2029	Attorney General	Privacy policy must disclose whether business collects, uses, or sells personal data to train LLMs

New Jersey Enacts the Nation's Broadest Data Broker Law: What Your Business Should Know

New Jersey passed a data broker law (A.5328) that is in effect immediately and is more comprehensive than any similar state law passed to date. The law has two main parts, both with wide reach and significant consequences for noncompliance. Any company that sells personal data of New Jersey consumers should review this law to determine whether its requirements apply.

Part 1—Prohibition on the Sale of Sensitive Personal Data

A.5328 prohibits the sale of New Jersey consumers' sensitive personal data. "Sale" broadly includes sharing, disclosing, or transferring personal data for monetary or other valuable consideration. "Sensitive data" includes information concerning race or ethnicity, religious beliefs, health, financial accounts, sex life or sexual orientation, citizenship or immigration status, transgender or non-binary status, genetic or biometric identifiers, known children, and precise geolocation.

This prohibition does not include a consent exception and applies to any company that sells sensitive personal data of New Jersey consumers, even if the company does not meet the applicability thresholds under New Jersey's general privacy law.

Selling, offering to sell, or licensing sensitive personal data may result in a civil penalty of \$50,000 per record. Because personal data typically moves in high volumes, this could result in substantial penalties for noncompliance.

Part 2—Annual Registration and Fees for Data Brokers and Data Collectors

Unlike other state data broker laws, New Jersey's law creates a new category of entity—"data collectors"—separate from data brokers. Data collectors are entities that have a direct relationship with consumers but sell or license their personal data to a data broker.

Both data brokers and data collectors must register annually with the New Jersey Division of Consumer Affairs in the Department of Law and Public Safety and provide information about their data practices. Registration fees range from \$5,000 to \$1.5 million, depending on the number of consumers involved.

Failure to register, pay the registration fee, or provide and maintain required information may result in a civil penalty of \$2,500 per day.

Below are questions to help you determine whether your company is a "data broker" or "data collector" under New Jersey law.

Is Your Company a "Data Broker" Under New Jersey Law?

- Does your company knowingly collect or purchase personal data of New Jersey consumers?
- Does your company sell or license that data to a third party?
- Does your company have a direct relationship with the New Jersey consumers whose personal data it collects or purchases?

If you answered "yes" to the first two questions and "no" to the third, your company is likely a "data broker" and may be subject to the annual registration and fee requirements.

Is Your Company a "Data Collector" Under New Jersey Law?

- Does your company knowingly collect personal data of New Jersey consumers?
- Does your company sell or license that data to a data broker?
- Does your company have a direct relationship with the New Jersey consumers whose personal data it collects or purchases?

If you answered “yes” to all three questions, your company is likely a “data collector” and may be subject to the annual registration and fee requirements.

What Businesses Should Do Now

Although the public registration requirements do not take effect until March 27, 2027, companies should assess now whether their practices involving the sale, licensing, or sharing of personal data may trigger the law. The potential penalties are significant, and New Jersey regulators are actively reviewing compliance across all sectors.

Connecticut Expands Privacy Requirements for Sensitive Data, AI, and Profiling

Connecticut amended its comprehensive privacy law in 2026, lowering the Connecticut Data Privacy Act's (CTDPA) applicability thresholds and expanding requirements for sensitive data, artificial intelligence, profiling, automated decision-making, facial recognition, precise geolocation, and consumer rights, setting the state near the forefront of U.S. privacy laws.

Businesses that previously determined the CTDPA did not apply, as well as businesses that have not recently revisited their Connecticut privacy programs, should reassess their obligations under the new, more stringent standards.

More Businesses Will Be Subject to the CTDPA

The amendments lower the CTDPA's general applicability threshold from 100,000 to 35,000 consumers.

They also replace the prior alternative threshold, which applied to businesses that processed the personal data of at least 25,000 consumers and derived more than 25% of gross revenue from the sale of personal data, with broader triggers tied to offering personal data for sale and processing sensitive personal data.

Sensitive Data and Consumer Protections Expand

Connecticut expands the types of information subject to heightened protections and the rights available to consumers. The amendments expand the definition of sensitive personal data and consumer access rights to include certain inferences generated from personal data and raise the age threshold for certain processing of minors' data from 16 to 18 years old.

Under these amendments, businesses may no longer sell sensitive personal data without consent and are prohibited from selling the personal data of minors under 18, regardless of consent.

The amendments also narrow the definition of publicly available information and expand deletion rights for certain information obtained from public sources. Among other changes, information created by combining personal data with publicly available information, certain genetic data, and information posted where a consumer has a reasonable expectation of privacy may no longer qualify as publicly available. Consumers may also request deletion of publicly available information that is combined to create a publicly accessible consumer profile or made available for sale, as well as inferences generated from that information.

New Requirements for AI, Profiling, and Automated Decision-Making

Like California, Connecticut continues to expand its regulation of AI, profiling, and automated decision-making.

The amendments add a new disclosure requirement relating to artificial intelligence and expand consumer rights involving profiling and automated decision-making. These changes are relevant to businesses using AI and automated systems that generate inferences or other information about individuals or use those outputs in decisions affecting individuals.

Facial Recognition and Precise Geolocation Face Additional Restrictions

Separate Connecticut amendments effective October 1, 2026 add requirements relating to facial recognition technology and precise geolocation information.

The amendments restrict the sale of precise geolocation data and add protections addressing facial recognition technology. Businesses that collect or use this information may therefore have additional obligations depending on how the information is collected, used, disclosed, or sold and should pay particular attention to any new obligations that may arise.

Assessment Requirements Expand

Connecticut's amended assessment requirements apply to processing activities created on or after August 1, 2026.

The amendments require assessments for certain processing activities, including activities involving sensitive data, profiling, automated decision-making, or other higher-risk processing. Businesses already conducting privacy, data protection, or AI assessments under other state laws may be able to leverage those processes to satisfy Connecticut's requirements.

What Businesses Should Do Now

Businesses that operate in Connecticut or process Connecticut residents' personal data should:

- **Recheck applicability.** Determine whether the lower thresholds or new applicability triggers bring the business within the scope of the CTDPA.
- **Review sensitive and higher-risk data.** Identify sensitive data, precise geolocation information, facial recognition information, and inferences collected or generated by the business.
- **Review AI, profiling, and automated decision-making.** Identify relevant activities and determine whether they trigger additional disclosure, consumer-rights, or assessment requirements.
- **Review notices and consumer-rights procedures.** Confirm that existing notices and procedures address the amended requirements, including changes relating to inferences and other newly regulated information.
- **Review assessment requirements.** Identify new or planned processing activities that require assessments and determine whether existing assessments can be leveraged.

Delaware Significantly Expands Its Privacy Law: What Your Business Should Know

On September 2, 2026, Delaware amended its comprehensive privacy law, the Delaware Personal Information Privacy Act (DPDPA), by signing House Bill 380 (HB 380) into law. HB 380, which goes into effect on January 1, 2027, marks the most significant revision to the DPDPA since its enactment in 2023.

HB 380 lowers the law's applicability thresholds, narrows certain exemptions, creates new obligations for businesses that receive personal information from covered companies, and expands requirements governing sensitive information, profiling, and automated decision-making.

Businesses that previously determined the DPDPA did not apply, as well as businesses with existing Delaware privacy programs, should review their practices to determine whether the amended law changes their obligations.

More Businesses Will Be Subject to the DPDPA

HB 380 substantially lowers the DPDPA's applicability thresholds:

- The general threshold decreases from 35,000 to 10,000 consumers annually.
- The threshold for businesses deriving more than 20% of gross revenue from the sale of personal information decreases from 10,000 to 5,000 consumers.
- Certain third parties that receive personal information from a controller may now be subject to the DPDPA without a minimum consumer threshold.

Financial Institution and Other Exemptions Are Narrowed

HB 380 narrows certain exemptions, including:

- **The GLBA financial-institution exemption is narrowed.** HB 380 replaces the broad entity-level exemption with more targeted exemptions for specified financial entities and activities, bringing Delaware closer to California's approach. Information subject to the GLBA remains exempt, but the exemption no longer automatically extends to all affiliates and subsidiaries.
- **The employee-information exemption is narrowed.** Personal information used in connection with certain profiling and reports in the employment context will now be subject to the DPDPA.

Businesses that previously relied on an entity-level exemption should confirm that the exemption continues to apply after January 1, 2027.

Expanded Protections for Sensitive Information

HB 380 expands the definition of sensitive data to include the following categories, bringing it closer to the CCPA's definition of sensitive personal information:

- Inferences used to reveal or identify sensitive characteristics, including health conditions, religious beliefs, racial or ethnic origin, sexual orientation, or immigration status;
- Neural information;
- Certain financial account credentials; and
- Certain government-issued identification numbers.

Controllers must obtain consent before processing sensitive information, and the processing must be reasonably necessary and proportionate to the purposes disclosed to the consumer.

Sales of sensitive data are also subject to additional restrictions. A permitted sale must be strictly necessary to provide or maintain a product or service requested by the consumer, and the controller must provide clear and conspicuous notice, obtain express consent, and maintain a record of that consent for five years.

New Vendor Due Diligence and Contracting Requirements

HB 380 adds requirements for businesses that disclose personal information to third parties:

- Controllers must enter into contracts with covered third parties that limit their use of personal information and include specified privacy protections, including audit and remediation rights.
- Controllers must conduct reasonable due diligence, including questionnaires and, where appropriate, additional measures based on the sensitivity of the data and the nature of the processing.
- Third parties must cooperate with those diligence efforts and provide information needed for the controller's assessment.
- A third party without a required contract may not further process the personal data it receives and must comply with applicable contractual and diligence requirements.

Businesses should review vendor-management and contracting processes for relationships involving disclosures of personal information to third parties.

Profiling and Automated Decision-Making

HB 380 expands requirements for profiling and automated decision-making:

- New requirements apply to certain "reports," including recommendations, summaries, automated decisions, and other communications based on personal information or profiling.
- Where a report is provided to a third party for use in a decision producing legal or similarly significant effects, the controller may need to ensure that the third party provides adverse-action notice, identifies the personal data relied upon, provides information about consumer rights, and offers human review where technically feasible.
- The right to opt out of profiling used in connection with automated decisions producing legal or similarly significant effects is expanded by removing the current "solely" automated-processing limitation.

These provisions may be relevant to businesses using AI or other automated tools in employment, financial services, insurance, housing, and other contexts involving significant decisions about individuals.

Assessment Requirements Also Expand

HB 380:

- Lowers the threshold for information protection assessments from 100,000 to 50,000 consumers; and
- Requires a separate impact assessment for profiling used in furtherance of automated decisions producing legal or similarly significant effects.

The profiling assessment must address, among other things, intended use, foreseeable harms and mitigation, data inputs and outputs, performance and transparency, post-deployment monitoring, and safeguards.

Businesses already conducting privacy or AI impact assessments under other state laws should determine whether those processes can be adapted to address Delaware's requirements.

Other Changes to Consumer Rights and Privacy Practices

HB 380 makes several additional changes, including:

- Consumers generally will be entitled to identify the specific third parties that received their personal information, rather than only categories of third parties.
- Controllers must stop processing information subject to withdrawn consent within 15 days.
- Controllers must obtain consent from minors ages 13 to 18 before processing their personal information for profiling.
- Privacy notices must be reasonably particular to the product or service offered to the consumer, which may require businesses with materially different products or services to reconsider using a single general notice.

What Businesses Should Do Before January 1, 2027

Businesses operating in Delaware or processing Delaware residents' personal information can use the remainder of 2026 to:

- **Recheck applicability.** Reevaluate the lower consumer thresholds, new third-party provisions, and existing exemptions.
- **Identify sensitive information and inferences.** Determine whether systems generate newly covered sensitive information and whether consent mechanisms remain sufficient.
- **Review third-party relationships.** Identify relevant disclosures and update contracts and diligence procedures.
- **Inventory profiling and automated decision-making.** Identify systems that may trigger the new requirements.
- **Review assessment requirements.** Determine whether existing or planned processing requires an information protection or profiling impact assessment and whether assessments prepared for other states can be leveraged.
- **Update privacy notices and consumer-rights procedures.** Confirm that notices, opt-out mechanisms, consent processes, and rights-request procedures address the amendments.

CalPrivacy's Data Broker Enforcement Blitz Signals Increased Scrutiny

After a relatively quiet summer, the California Privacy Protection Agency (CalPrivacy) announced three enforcement decisions against data brokers over a three-week span. In each instance, the data broker allegedly collected and sold consumer personal information without timely registering with the CalPrivacy Data Broker Registry. Thousands of dollars in fines were levied against the three data brokers.

Each enforcement action was led by CalPrivacy's Data Broker Enforcement Strike Force, a group constituted in November 2025 to specifically address compliance with the data broker registration requirement of the Delete Act. CalPrivacy has signaled that the Data Broker Enforcement Strike Force may bring additional actions in the coming months.

Below is a brief summary of the three enforcement actions as well as concrete steps for data brokers to take going forward.

LocateSmarter LLC

On August 11, 2026, [CalPrivacy announced](#) a \$116,490 fine against Iowa-based data broker LocateSmarter LLC. The enforcement decision alleged that LocateSmarter failed to register timely as a data broker despite collecting and selling consumer personal information, including names, dates of birth, Social Security numbers, telephone numbers, email addresses, employment information, and driver's license information. LocateSmarter allegedly used the personal information to make inferences with its collected personal information, including whether a consumer was "litigious." However, despite allegedly selling consumer personal information, LocateSmarter did not register as a data broker by the January 31, 2026, deadline. CalPrivacy also faulted LocateSmarter for requiring unnecessary data to opt out of the company's sale of personal information, including requiring consumers to provide the last four digits of their Social Security numbers. While the CCPA allows companies to verify a consumer's rights to delete, know, or correct, the CCPA prohibits companies from requiring verification for the right to opt out of sale or sharing of data. This decision was CalPrivacy's first arising under both the CCPA and the Delete Act.

Cybba, Inc.

Just two days later, on August 13, 2026, [CalPrivacy announced](#) an enforcement action and \$52,400 fine against Boston-based Cybba, Inc. for failing to register timely as a data broker. Cybba provides digital marketing and targeted advertising services on social media, and in doing so, allegedly collected and sold personal information including geolocation data, internet activity data, inferences, identifiers, and commercial data. However, Cybba did not register with CalPrivacy as a data broker by January 31, 2025.

SalesIntel Research, Inc.

In early September 2026, [CalPrivacy announced](#) a third enforcement action for failing to register with the agency's Data Broker Registry. This action involved a \$36,400 fine against Virginia-based SalesIntel Research, Inc., a company that, among other things, provides targeted advertising and data enrichment services to its customers. SalesIntel advertises that it has 200 million professional contacts and 54 million verified mobile phone numbers in its database. It uses that information for several of its services, including cleaning the data in its clients' customer relationship management platforms and supplementing those platforms with additional data in the SalesIntel database. SalesIntel also offers products based on its personal information database to "de-anonymize" website traffic and to derive inferences from a person's

online behavior and activities. Yet, like LocateSmarter and Cybba, SalesIntel failed to register as a data broker by the deadline to do so.

These enforcement actions coupled with the attention on the Delete Request and Opt-out Platform (DROP) signal CalPrivacy's growing scrutiny over data broker registration and compliance.

Your Key Next Steps

Evaluate your data broker status. Under the California Delete Act, a data broker is any "business that knowingly collects and sells the personal information of a consumer with whom the business does not have a direct relationship." If you meet this definition, absent one of the noted exceptions, you should register on the CalPrivacy Data Broker Registry.

Additionally, as noted in [our article](#) on the New Jersey Data Broker Law, businesses may have additional obligations in other states, even where they sell data from consumers with whom they have a direct obligation.

Confirm registration deadlines and maintain an annual compliance calendar. If your business qualifies as a data broker, determining that registration is required is only the first step. The recent enforcement actions demonstrate that CalPrivacy is willing to impose penalties for late registration even where a data broker ultimately registers. Businesses should identify applicable registration and renewal deadlines, assign responsibility for completing required filings, and establish controls to ensure filings are made on time.

Evaluate CCPA obligations as well as Delete Act obligations. Regulators are looking at all facets of a business. CalPrivacy is not single-track focused on these issues. The LocateSmarter action demonstrates that CalPrivacy will combine infractions under the CCPA, Delete Act, and other privacy laws or regulations when bringing an action.

California Enforcement Actions

Date	Company	Agency	Fine / Payment	Key Issues
9/1/2026	SalesIntel Research	CalPrivacy	\$36,400	Data Broker Registration
8/13/2026	Cybba	CalPrivacy	\$52,400	Data Broker Registration
8/11/2026	LocateSmarter	CalPrivacy	\$116,490	Data Broker Registration Level of Verification for Opt-Out Requests
5/8/2026	General Motors	Attorney General	\$12.75M	Data Minimization Sale of Information to Data Brokers
2/27/2026	PlayOn Sports	CalPrivacy	\$1.1M	Ability to Opt Out of Data Collection Protection of Children's/Students' Data
2/27/2026	Ford Motor Co.	CalPrivacy	\$375,000	Friction in Opt-Out Requests
2/11/2026	Disney	Attorney General	\$2.75M	Honoring Opt-Out Requests Across Platforms
12/30/2025	Datamasters	CalPrivacy	\$45,000	Data Broker Registration
12/30/2025	S&P Global	CalPrivacy	\$62,600	Data Broker Registration
11/21/2025	Jam City	Attorney General	\$1.4M	Methods of Opt-Out Requests Protection of Children's Data
10/30/2025	Sling TV / Dish	Attorney General	\$530,000	Honoring Opt-Out Requests Protection of Children's Data
9/26/2025	Tractor Supply Co.	CalPrivacy	\$1.35M	Honoring Opt-Out Requests
7/28/2025	Healthline Media	Attorney General	\$1.55M	Honoring Opt-Out Requests
5/1/2025	Todd Snyder	CalPrivacy	\$345,178	Accessibility of Cookie Preferences Level of Verification for Requests
3/7/2025	American Honda Motor Co.	CalPrivacy	\$632,500	Level of Verification for Opt-Out Requests Symmetry in Cookie Management

CCPA Cybersecurity Audit Requirements: Building an Audit-Ready Security Program

“

A control that exists but cannot be demonstrated may create the same audit challenge as a control that does not exist.

CalPrivacy's cybersecurity audit regulations took effect on January 1, 2026, establishing the first comprehensive cybersecurity audit regime imposed by a state privacy law of general application. The regulations require businesses whose processing of personal information presents a "significant risk to consumers' security" to complete annual, evidence-based cybersecurity audits and to certify completion to the agency under penalty of perjury.

These new rules elevate cybersecurity compliance beyond security and information-technology functions. Covered businesses will be expected to demonstrate, with evidence, that their cybersecurity programs are appropriately designed and actually operating during the period under review, and to document any security weakness and remediation commitments. Cybersecurity is therefore becoming a business integration and governance concern.

Which Businesses Are Covered

The audit requirement does not apply to every business subject to the CCPA. A business should complete its cybersecurity audit if it engages in processing that is considered a "significant risk" and the business either:

- derives at least half of its annual revenue from selling or sharing consumers' personal information; or
- has more than \$25 million in annual gross revenue and processes personal information at sufficient scale—either personal information relating to at least 250,000 consumers or households, or sensitive personal information relating to at least 50,000 consumers.

Importantly, the CCPA defines "consumer" broadly to include employees, applicants, and business contacts, so businesses may meet these thresholds even if they are not processing customer data at the threshold level. Also, and importantly, these thresholds include processing of employee, applicant, and business contact information, and the thresholds are not limited to sensitive information

and include personal information, which includes ordinary identifiers like IP addresses and names.

The first step for any potentially covered business should be a deliberate coverage analysis based on actual data volumes rather than assumptions about the nature of the company's business.

The Compliance Timeline

Initial audit deadlines are staggered by revenue, with the biggest companies facing the nearest deadlines:

Annual Gross Revenue	First Audit Report Due	Audit Period Covered
Over \$100 million (as of January 1, 2027)	April 1, 2028	January 1, 2027 – January 1, 2028
\$50 million to \$100 million (as of January 1, 2028)	April 1, 2029	January 1, 2028 – January 1, 2029
Less than \$50 million (as of January 1, 2029)	April 1, 2030	January 1, 2029 – January 1, 2030

After April 1, 2030, a business that meets the significant-risk criteria and reporting thresholds as of January 1 of a given year must complete an audit covering the following 12 months and complete its report by April 1 of the year after that.

Auditor Qualifications and Independence

The cybersecurity audit must be performed by a qualified professional with cybersecurity and audit expertise, using recognized professional standards.

The auditor may be internal or external, but must exercise objective and impartial judgment, be free of conflicts, and remain uninfluenced by the business, including its owners, managers, and employees. Critically, the auditor may not participate in activities the auditor may assess in a current or future audit. That bars the same person or team from developing the business's security procedures, preparing its documentation, implementing or maintaining the program, or making recommendations about the program beyond articulating audit findings. Companies that have relied on a single trusted consultant to both build and evaluate their security posture will need to separate those roles. In addition, where a company performs a pre-audit check with an external auditor to assess its security program, the company should use a separate auditor for the cybersecurity audit that is reported to CalPrivacy to ensure the appropriate level of independence.

Where an internal auditor is used, the highest-ranking auditor must report to an executive who does not have direct responsibility for the cybersecurity program, and that executive must handle the auditor's performance review and compensation, again, to ensure independence.

Further, businesses must cooperate in the audit process where necessary. Businesses must provide all requested relevant information, disclose relevant facts in good faith, and not misrepresent them. And findings may not rest primarily on management assertions or attestations—they must be grounded in specific evidence such as documents, testing and sampling, and interviews. Both the business and the auditor must retain audit-related records for at least five years.

Scope: Eighteen Components, Applied by Risk

The audit's overall objective is to assess how the cybersecurity program protects personal information against unauthorized access, destruction, use, modification, or disclosure, and against unauthorized activity resulting in loss of availability. The audit must evaluate whether the program is appropriate to the business's size, complexity, and nature and scope of processing, and how the business implements and enforces it.

The areas addressed are:

- Authentication and password standards
- Encryption at rest and in transit
- Account management and access controls
- Personal information and asset inventories
- Secure configuration and patch management
- Vulnerability scanning and penetration testing
- Audit log management
- Network monitoring and defenses
- Antivirus and antimalware protections
- System segmentation
- Control of ports, services, and protocols
- Cybersecurity threat awareness
- Education and training
- Secure development and code review
- Oversight of service providers, contractors, and third parties
- Retention schedules and secure disposal
- Incident response management
- Business continuity and disaster recovery

The 18 items are evaluation points rather than a checklist, and the auditor—not the business—determines which are applicable based on the size and nature of the business's processing. Scope also follows the data rather than the corporate perimeter. Any environment where California personal information is stored, processed, or accessed—cloud services, end-user devices, backups, and third-party environments—falls within the audited information system, regardless of who owns the infrastructure.

What the Audit Report Must Contain

The audit report must describe the information system and the policies assessed, identify the criteria used, and specify the evidence examined, with an explanation of why that scope, criteria, and evidence support the findings. It must address the applicable components, describe how policies are implemented and enforced, and explain their effectiveness. The report must also identify up to three titles of individuals responsible for the cybersecurity program, name the auditor and describe their qualifications, and include the highest-ranking auditor's signed certification attesting to an independent, objective, evidence-based review.

Annual Certification to CalPrivacy

For each year an audit is required, the business must submit a written certification to CalPrivacy through its website by April 1 of the following year. The certification—not the audit report—is what goes to the agency, though the report itself is subject to production on request.

The certification must be completed by a member of executive management who is directly responsible for audit compliance, has sufficient knowledge of the audit to provide accurate information, and has authority to submit it. It must identify the business and a contact person, state that the audit was completed, identify the audit period by month and year, and include an electronically signed attestation, under penalty of perjury, that the information is true and correct and that the business made no attempt to influence the auditor's decisions or assessments.

The personal attestation requirement is the mechanism that moves this obligation from the security team to the executive suite. An officer signing under penalty of perjury will reasonably want to understand how scoping decisions were made, what gaps were found, and how auditor independence was preserved.

Leveraging Existing Work

Businesses need not start from scratch. CalPrivacy has confirmed that an audit, assessment, or

evaluation prepared for another purpose may be used if, alone or with reasonable supplementation, it fully satisfies every requirement. Many companies complete periodic audits of their data security infrastructure already, and CalPrivacy does not want to significantly disrupt those processes already in place.

Coordinating with Risk Assessments and the Audits Division

Much of the underlying work overlaps with CalPrivacy's [risk assessment requirements](#), including mapping processing activities, inventorying data, identifying controls, and documenting the rationale for decisions. Companies should build these programs together rather than in sequence.

Your Key Next Steps

- **Determine whether the requirements apply.** Confirm revenue and data-processing volumes, including employee, applicant, and business contact information where applicable.
- **Identify the company's first audit period.** Work backward from the beginning of that period—not the report deadline—to determine when controls and supporting evidence must be operational.
- **Assess the current cybersecurity program against the audit requirements.** Companies with existing assessments should identify what can be reused and where additional work will be required.
- **Test whether controls are producing evidence.** A control that exists but cannot be demonstrated may create the same audit challenge as a control that does not exist. Companies should confirm now that logging, testing, monitoring, and documentation will support the eventual audit.
- **Resolve auditor independence.** Determine who will perform the audit and ensure that advisory, implementation, and audit responsibilities are appropriately separated.
- **Review third-party risk management.** Identify where personal information resides outside the company and whether vendor oversight and contractual protections are sufficient to support the audit.
- **Consider an internal mock audit before the formal audit period.** Identifying deficiencies early

gives the business time to remediate them before they become findings in a formal audit report.

- **Identify the responsible executive.** The person who will eventually make the required certification should have visibility into the program and the audit process well before the certification deadline.

Because decisions made at the outset can affect audit scope, privilege, remediation strategy, and the record ultimately available to regulators, businesses should involve privacy and cybersecurity counsel early in the process. The Coblentz Data Privacy and Cybersecurity team can help companies assess whether the requirements apply, structure their readiness efforts, and coordinate with security teams and auditors before the formal audit period begins.

California DROP Deletion Requests Are Underway

California's Delete Request and Opt-out Platform, or DROP, is now active. DROP allows California residents to submit a single request to delete personal information held by registered data brokers rather than submitting separate requests to each broker.

Data brokers were required to begin accessing DROP and processing requests on August 1, 2026. As of August 28, approximately 500,000 Californians had registered with DROP, 654 data brokers were participating, and approximately 25% of participating brokers reported processing deletion requests.

The California Privacy Protection Agency (CalPrivacy) says 99.9% of consumers had their profiles deleted by at least one data broker, and the typical DROP user had information deleted by more than 40 brokers.

What Data Brokers Need to Do

DROP adds another channel through which data brokers must receive and process consumer deletion requests. California data brokers need procedures to regularly access DROP, retrieve requests, determine whether the request matches information in their records, and take the required action.

The practical challenge is matching each request to the correct consumer information. DROP allows consumers to provide additional identifiers, so brokers should be able to search across relevant datasets using the information provided and apply the request to the appropriate records.

Businesses subject to California's data broker requirements should confirm that their processes address:

- **DROP access.** The business can retrieve and process requests submitted through the platform.
- **Identity matching.** The business can use the identifiers provided by consumers to locate relevant records across its datasets.
- **Downstream deletion.** Applicable information is deleted from relevant systems and addressed with service providers and other vendors as required.
- **Recordkeeping.** The business maintains appropriate records of requests and their outcomes.

Businesses that buy, sell, or license personal information should also evaluate whether they qualify as a California data broker and therefore may be subject to DROP requirements.

For companies already subject to California's data broker requirements, the immediate question is whether their existing deletion procedures account for requests arriving through DROP and whether their systems can reliably locate and remove the information covered by those requests.

CalPrivacy Targets Gig Economy Platforms in First CCPA Sectoral Audit

“

Access is a foundational right, allowing individuals to identify potential issues and meaningfully exercise other rights such as correction, deletion, and appeal.

On July 21, 2026, the California Privacy Protection Agency (CalPrivacy) announced that its newly formed Audits Division has begun its first formal privacy audit, focused on gig economy platforms operating in California. This sectoral audit was initiated in response to hundreds of consumer complaints, as well as comments received during public rulemaking. It reflects CalPrivacy's continued focus on active enforcement following [several high-profile actions earlier in 2026](#).

What Is a “Gig Economy Platform”?

Gig economy platforms are digital applications and websites that connect independent workers with customers for short-term or project-based tasks. Common examples include ridesharing, food delivery, and task-based service platforms.

Gig economy platforms collect personal information from both customers and the gig workers who provide services through their platforms. The personal information collected by these platforms may be extensive and highly sensitive, and may be used by algorithmic systems to make significant decisions affecting gig workers, including dispatch assignments, performance ratings, compensation, and account suspension or deactivation.

What Is the Focus of CalPrivacy's Audit?

The audit will evaluate whether major gig economy platforms are complying with all obligations under the California Consumer Privacy Act (CCPA) and will focus on whether these platforms provide individuals with meaningful access to and control over their personal information. This emphasis reflects CalPrivacy's view that access is a foundational right, allowing individuals to identify potential issues and meaningfully exercise other rights such as correction, deletion, and appeal.

The CCPA's protections apply to consumers, as well as to employees, job applicants, and independent contractors such as gig workers. Consistent with other California efforts to protect gig workers, the Audits Division also plans to closely examine whether platforms using algorithmic systems as described above are complying with workers' access rights.

Failure to comply with workers' access rights not only violates the CCPA, but may also directly affect workers' livelihoods. Without access to the information underlying significant decisions, workers may be unable to understand or challenge negative outcomes.

What Businesses Should Do Now

Companies that operate a gig economy platform in California or one that targets California residents should review their compliance with the CCPA, including their processes for responding to consumer and worker rights requests.

Companies should confirm that they have systems in place that allow both consumers and workers to exercise their rights under the CCPA and that access requests are completed within the applicable 45-day statutory period.

Children's Privacy in 2026: Enforcement Moves Into Product Design

“

Privacy compliance cannot end with a written policy or front-end user interface.

Last year, we highlighted significant changes to the Children's Online Privacy Protection Act (COPPA) Rule and the growing number of state laws focused on age-appropriate design. In 2026, the focus has shifted from lawmaking to enforcement. Two major settlements announced in August illustrate the scale of that shift: Meta agreed to pay up to \$18 billion to resolve claims brought by nearly all U.S. states concerning the treatment of young users on Facebook and Instagram, while TikTok and ByteDance reached a \$400 million settlement with the Department of Justice over alleged COPPA violations.

The significance of the settlements goes beyond monetary awards. The Meta settlement imposes restrictions on how teenagers may use Facebook and Instagram, while the TikTok settlement was contingent on whether parental-consent and deletion mechanisms worked as required. Together, the settlements show federal regulators and State Attorneys General examining not only what companies say about children's privacy, but also how products are designed, how age-related information is acted upon, and what happens to children's data after it is collected. At the same time, California recently passed a new suite of laws to protect children from perceived harms from social media and artificial intelligence, and Congress is considering legislation that would extend federal protections to teenagers and regulate advertising, recommendation systems, AI chatbots, gaming platforms, and other features used by minors.

Meta Settlement Pushes Children's Privacy Into Product Design

On August 26, 2026, Meta agreed to pay up to \$18 billion over ten years to resolve claims by nearly all U.S. states concerning Facebook and Instagram. The settlement ended a federal trial involving claims by California, Colorado, Kentucky, and New Jersey that Meta violated state consumer-protection laws by designing its platforms in ways that harmed young users and misleading the public about their safety. The litigation also included claims by 29 states that Meta violated COPPA by knowingly collecting personal information from children without parental consent and using that information to train generative AI models.

What makes the settlement particularly significant from a privacy-compliance perspective is the nature of the relief. For the next decade, Meta agreed to limit teenagers' use of Facebook and Instagram to two hours per day and to block use between midnight and 6:00 a.m. unless a parent expressly consents.

Meta will also disable most push notifications to teenagers during school hours and strengthen protections intended to keep minors from accessing age-restricted content. The settlement does not, however, require Meta to discontinue personalized recommendations or targeted advertising. At least \$5 billion of the settlement funds are contingent upon YouTube, TikTok, and Snap implementing similar controls. YouTube's CEO has dismissed the idea of joining the settlement.

These requirements illustrate how closely children's privacy and product design are becoming intertwined. Historically, a company evaluating COPPA compliance might have focused principally on whether it provided the required notice, obtained parental consent, and appropriately collected and retained children's personal information. The Meta settlement reaches further into the user experience itself: when a minor can access the service, how long the minor can use it, when the platform may prompt the minor to return, and what content the minor may encounter.

The allegations concerning generative AI are also notable. The states alleged that Meta used personal information collected from children to train its generative AI models. The settlement does not establish that any particular use of minors' data for model training violates COPPA, but the allegation puts AI training squarely within the range of downstream data uses that regulators may examine. Companies developing or deploying AI therefore should understand whether datasets used for model development or improvement include information collected from children and whether the permissions and disclosures governing the original collection support those later uses.

TikTok Settlement Reinforces COPPA's Operational Requirements

The TikTok settlement, announced only days before the Meta resolution, presents a different but complementary lesson. On August 21, 2026, the Department of Justice announced a \$400 million settlement with TikTok, ByteDance, and affiliated entities to resolve litigation arising under COPPA. TikTok agreed to pay \$300 million immediately and another \$100 million upon entry of an order vacating an earlier consent decree involving its predecessor, Musical.ly, although at a September 21, 2026 hearing the court indicated it did not immediately plan to vacate the consent decree. The DOJ described the settlement as one of the largest recoveries ever obtained in a COPPA case.

The government's allegations focused on familiar COPPA requirements rather than a novel theory of liability. The 2024 lawsuit alleged that TikTok and ByteDance collected personal information from children under 13 without obtaining the required parental consent, failed to honor parents' requests to delete their children's accounts, and failed to delete accounts even after learning that the users were under 13.

This settlement is a reminder that even as children's privacy regulation expands into platform design, advertising, and AI, the basic operational requirements of COPPA remain important enforcement targets. A parental-consent process must work as represented; a deletion mechanism must result in the required deletion; and information

showing that a user is a child must be handled consistently with the company's legal obligations.

The DOJ also noted that, after the lawsuit was filed, TikTok made significant changes to its compliance and privacy practices, including measures intended to strengthen protections for younger users, improve age-related controls, and increase parental oversight. The settlement resolved allegations only, without a determination of liability.

For businesses, the broader point is that privacy compliance cannot end with a written policy or front-end user interface. Companies should be able to demonstrate that age signals, parental permissions, account restrictions, deletion requests, retention rules, and related workflows operate consistently across the systems that actually process the data.

California Enacts Social Media and AI Laws to Protect Children

The enforcement activity comes as the California legislature has taken steps to expand protections for minors online. On September 10, 2026, Governor Gavin Newsom signed a package of laws focused on increasing children's privacy and preventing harms to children in both social media and artificial intelligence. These laws include:

- AB 1709, which aims to eliminate for users under 16 years old purportedly "addictive features" in social media platforms, including video autoplay features and other features designed to maximize engagement. The law also requires social media companies to verify a user's age and take reasonable steps to prevent children from accessing those features.
- SB 1119, or "Adam's Law," which adds guardrails around AI companion chatbots. Under the law, chatbot operators evaluate and address potential safety harms to children. Additionally, companies must determine a user's age, and, if under the age of 18, the company's chatbot must have parental controls, age-appropriate disclosures, and default usage limits of one continuous hour and two total hours per day. The law also restricts what these companion chatbots may say to children to limit emotional dependence on the chatbot and to avoid excessive praise or flattery.

- AB 2246, or the “Youth Social Media Protection Act,” which requires online services that are “likely to be accessed by children” to provide high-privacy settings for child users. The law also prohibits companies from profiling any children by default or collecting more personal information than is needed to deliver the service. This law replaces the [California Age-Appropriate Design Code Act](#).

Taken together, the laws dovetail with state and federal regulators’ increased scrutiny of social media companies and children’s privacy.

Congress Is Considering a Broader Federal Framework

While California has been quick to take action, the same cannot be said for a federal framework. Congress is once again considering, but has not passed, a substantial expansion of federal protections for minors online. On June 29, 2026, the House passed the Kids Internet and Digital Safety Act (KIDS Act), H.R. 7757, by a 267–117 vote. The package combines portions of a number of previously separate proposals, including the Kids Online Safety Act (KOSA), COPPA 2.0, legislation addressing messaging and gaming features, AI chatbot safeguards, and data-broker requirements.

For privacy teams, the COPPA 2.0 provisions are among the most consequential. The House package would bring 13-year-olds within the parental-consent framework and create protections for teenagers through age 17. It also would replace the current actual-knowledge approach of COPPA (i.e. COPPA applies only when an operator affirmatively knows a user is a minor) with a standard that encompasses circumstances in which an operator “knows or should have known” that a user was a child or teenager. The proposal would impose restrictions on individual-specific advertising to minors and add requirements concerning data minimization, retention, and certain transfers of minors’ information.

The package also illustrates how federal children’s-privacy legislation is expanding beyond traditional data-collection rules. Among other things, it would address minor-facing default settings and recommendation systems, communications and geolocation controls, and AI chatbots. The revised House bill generally preserves state laws that provide greater protection to minors, meaning that enactment would not necessarily eliminate the growing state-law compliance patchwork.

Significant differences remain between the House and Senate approaches. In particular, the House version expressly rejects a general duty of care, while the Senate version of KOSA uses a broader duty-of-care framework. The Senate Commerce Committee unanimously advanced KOSA on August 5, and the Senate previously passed its own version of COPPA 2.0 in March. Whether and in what form those competing approaches ultimately become law remains unresolved.

Takeaways

Companies that operate services used by children or teenagers—or that otherwise process minors’ personal information—should treat the recent settlements and legislation as an indication that children’s privacy is becoming an increasingly operational area of compliance. Going forward, companies should consider the following:

- **Treat children’s privacy as a product-governance issue.** Privacy, legal, engineering, product, and trust-and-safety teams should evaluate not only collection and disclosure practices, but also minor-facing defaults, notifications, recommendation systems, time-management tools, messaging features, and other design choices.
- **Test consent, age, and deletion workflows from end to end.** Companies should confirm that parental-consent mechanisms work as described, that information indicating a user is a minor is acted upon appropriately, and that deletion requests are carried through all systems in which the relevant information is maintained.

- **Map downstream uses of minors' data.**

Businesses should understand whether information collected from children or teenagers is later used for advertising, personalization, analytics, audience development, AI model training, or other secondary purposes, and whether those uses are consistent with the permissions and representations made when the data was collected.

- **Do not wait for Congress to act.** The KIDS Act and related Senate proposals could significantly broaden federal obligations, but the Meta and TikTok matters demonstrate that regulators already have substantial enforcement tools under existing law. Companies should continue to prepare for federal developments while also accounting for state laws that may impose additional or more protective requirements.

CIPA Litigation and Reform: *Variety Media*, SB 690, and the Future of Website Tracking Claims

For the last several years, the CIPA landscape has been defined by a surge of demand letters, inconsistent lower court rulings, a lack of appellate precedent, and continued uncertainty. But in mid-2026, two developments in CIPA litigation and reform introduced a new chapter for this now-popular statute—addressing certain long-standing questions, while raising several new ones. Companies should closely monitor these developments and continue to treat website tracking litigation as an evolving area of risk.

CIPA in the Age of Website Tracking Technology

The California Invasion of Privacy Act of 1967 (CIPA), Cal. Penal Code §§ 630, et seq., is a criminal statute prohibiting the unauthorized interception or recording of communications. Although CIPA was historically understood to apply to wiretapping and eavesdropping on telephone calls, CIPA claims have exploded over the last several years, with plaintiffs bringing claims based on alleged violations involving modern website tools. Relying on the statute's private right of action and statutory damages, plaintiffs have developed creative approaches and legal theories for alleged CIPA violations based on companies' use of common website tracking technologies such as cookies, pixels, and other third-party analytics software.

Plaintiffs commonly bring CIPA claims under two of the statute's provisions: (i) the wiretapping provision, § 631(a), which prohibits intercepting communications without authorization; and (ii) the pen register and trap and trace provision, § 638.51(a), which prohibits using a pen register or trap and trace device without a court order. The statute provides for damages of up to \$5,000 per violation under § 637.2, among other forms of civil relief, promoting the rise of this statute as a popular basis for individual and class action claims and often yielding low-effort settlements for plaintiffs.

For years, parties have contested in demand letter negotiations and state and federal courts whether a company's use of a cookie or pixel on its website can qualify as illegal wiretapping, or as a pen register or "trap and trace" technology, in violation of CIPA.

Without appellate guidance, courts have come out differently on these questions—resulting in unpredictable outcomes and ongoing uncertainty.

Two recent developments may finally bring some long-awaited answers and a clearer path forward—but will likely also lead to plaintiffs pivoting to new approaches to litigating the same alleged privacy violations under different theories and statutes.

California Court of Appeal Issues Tentative Ruling in *Variety Media*

On August 21, 2026, the California Court of Appeal issued its tentative ruling in the case of *Variety Media, LLC v. Superior Court*, No. B350578, which addressed whether internet-based tracking technology that collects information from visitors to a website qualifies as a "pen register" under CIPA.

The Court tentatively ruled that CIPA's definition of "pen register" may include this type of technology, and is not limited to telephone monitoring devices—rejecting the decisions from many state-level trial courts that the Legislature did not intend this provision to apply to internet-based technology. The Court also appears ready to deny the frequently asserted argument that applying CIPA's pen register provisions to internet communications would create an irreconcilable conflict with the California Consumer Privacy Act (CCPA), declaring that CIPA's consent requirement incorporates and exceeds the CCPA's requirements, rather than displacing them.

But the Court also gave hope to businesses, tentatively ruling that the collection of an IP address alone is not enough to support a CIPA pen register claim, because an IP address only identifies the source of the communication, not its destination as the pen register provision requires.

Because the Court has only issued a tentative ruling, this is not yet settled law. But the Court's comments during the August 21 oral argument largely indicated that it is inclined to adopt its tentative ruling. If the Court adopts the ruling, this would resolve several longstanding debates on CIPA claims—at nearly the same time that CIPA reform finally passed in the Legislature.

California Enacts SB 690

On September 30, 2026, California Governor Gavin Newsom signed into law SB 690, a long-awaited bill that eliminates the private right of action under CIPA's pen register/trap and trace provision (§ 638.51) so that it may only be enforced by the California Attorney General. SB 690 would apply retroactively to any actions filed within two years prior to its effective date of January 1, 2027.

Earlier versions of SB 690 provided for more substantial changes, including proposed amendments to §§ 631, 632, 632.7, and 638.50, that would have defined website analytics and marketing tools as disclosures made for a "commercial business purpose" and thus exempt from the law. This would have brought relief to a greater range of CIPA claims, including wiretapping claims, based on website tracking technologies beyond pen register and trap and trace claims. But the final version is far narrower, and does not include the "commercial business purpose" exemption.

Even so, the law as passed will still bring relief to companies who have faced a deluge of threatened and filed CIPA pen register claims in recent years.

What These Developments Mean for Website Tracking Litigation

Because SB 690 does not cover CIPA's wiretapping provision (§ 631(a)), these types of claims are expected to continue and increase even after SB 690 takes effect, along with other similar statutory and common-law privacy claims. Plaintiffs are also likely to continue bringing website-technology claims under other statutes including the Video Privacy Protection Act (VPPA), Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), California Comprehensive Data Access and Fraud Act (CDAFA), and more.

Companies should remain vigilant and continue to mitigate these risks by conducting regular audits and reviews of tracking technologies employed, consent flows, vendor contracts, and privacy notices. Companies should also confirm that any cookies, pixels, or other third-party analytics tools on their websites are used and operating as described in their privacy disclosures. At this time, the best practice to avoid these claims is to refrain from placing cookies or pixels until a user has affirmatively accepted them. Although this practice is not required by the CCPA, and may not be the right business decision for all companies, it appears at the moment to keep plaintiffs from sending demand letters and bringing suit.

California's ALPR Law in Focus: A Posted Privacy Policy Matters More Than Ever

Businesses that use automated license plate recognition (ALPR) technology should take a fresh look at their compliance with California's Automated License Plate Recognition law in light of three recent state and federal court decisions that have spurred a wave of new class action complaints and increased litigation risks for parking operators, shopping centers, property managers, and other businesses that use ALPR technology.

These three cases demonstrate the importance for ALPR operators and end-users to adopt and post a compliant ALPR policy. If a company does not have an ALPR policy in place, courts have held that a customer could be harmed by impairment of their "right to know" how any collected license plate data will be used, and have allowed those lawsuits to proceed past the pleadings stage and into discovery. On the other hand, if the company does have an ALPR policy, courts have required plaintiffs plead a higher actual harm standard, where a plaintiff must allege they suffered harm beyond a mere statutory violation.

The Statutory Requirement

California law requires ALPR operators and end-users to maintain reasonable security procedures and implement a usage and privacy policy governing the collection, use, maintenance, sharing, and dissemination of ALPR information.¹ The required policy must address specific topics, including authorized purposes for using ALPR information, who may access it, training requirements, security monitoring, sharing restrictions, data accuracy measures, retention periods, and destruction procedures. These policies must be publicly posted in writing, and, if the business has a website, conspicuously posted on that website. Plaintiffs harmed by an ALPR violation may recover actual damages, but not less than \$2,500 in liquidated damages, along with potential punitive damages, attorneys' fees, litigation costs, and injunctive relief. The question of what constitutes statutory harm has dominated the litigation landscape.

Bartholomew: Litigation Risks Increase

In the February 2026 *Bartholomew v. Parking Concepts* decision,² a plaintiff alleged that a parking garage operator collected his license plate information when he entered and exited a parking garage, but the operator failed to implement and make publicly available the required ALPR usage and privacy policy. The trial court sustained the parking garage operator's demurrer, and the Court of Appeal reversed in part.

Importantly, the Court of Appeal centered its decision on "harm." The ALPR statute authorizes a private civil action only by an individual "harmed" by a violation. The parking garage operator argued that a plaintiff must show misuse, mishandling, or measurable damages—not simply a lack of compliance with the statutory requirements. The Court of Appeal disagreed, concluding that collecting and maintaining ALPR information without implementing and making public the required policy could harm individuals by violating their statutory "right to know" who is collecting their ALPR data and how it is being used and maintained.

After the *Bartholomew* decision, plaintiffs' firms filed a flood of putative class actions against businesses and property owners that allegedly used ALPR technology without the required policy. Complaints were even filed against businesses that had posted ALPR policies, but which plaintiffs asserted insufficiently described the statutorily required elements.

Mata: Court of Appeal Narrows Bartholomew Holding

In July 2026, the California Court of Appeal handed businesses that use ALPR technology an important victory in *Mata v. Digital Recognition Network, Inc.*³ There, the court held that a plaintiff must suffer actual harm to have standing to bring a claim under the ALPR statute.

The plaintiff in *Mata* brought a putative class action against an ALPR provider that housed more than nine

¹ Cal. Civ. Code § 1798.90.5, *et seq.*

² 118 Cal. App. 5th 438 (2026).

³ 121 Cal. App. 5th 1075 (2026).

billion license plate images in its ALPR system. Importantly, the defendant, Digital Recognition Network (DRN), collected and maintained the images pursuant to an ALPR usage and privacy policy that it adopted years earlier in 2015.

The plaintiff alleged a single cause of action for violation of the ALPR statute, conceding that DRN's ALPR policy included the statutorily required information, but arguing that the purpose of DRN's policy was to "maintain the appearance of adhering" to the ALPR statute and "to pay lip service to privacy laws without having any intention of actually complying with them." Crucially, plaintiff did not plead, and could not prove, that he suffered any actual harm. DRN acknowledged that it captured the plaintiff's license plate data at least 15 times, but argued on summary judgment that the plaintiff had not had his identity stolen, nor had he suffered any physical injury, harm, or lost wages as a result of DRN's collection. Instead, the plaintiff testified that his only harm was that his "privacy ha[d] been violated on multiple occasions."

The trial court held, and the Court of Appeal agreed, that actual harm was a necessary component of the statutory standing inquiry. First, under the plain language of the statute, only an individual "who has been harmed by a violation of the statute" has a private right of action to bring a lawsuit. The court concluded that the required *harm* must be distinct from the statutory *violation* itself. Because the plaintiff alleged only that the violation invaded his privacy, he failed to establish the requisite harm. The legislature also provided examples of harm in the text of the ALPR statute, including "unauthorized access or use of ALPR information or a breach of security of an ALPR system." These examples go beyond a statutory violation.

Second, the legislative history supported that interpretation. One report from the legislative history referred to damages in actions brought by individuals harmed by the improper use of ALPR data, while another described claims by individuals whose information was unlawfully disclosed. Both examples involved misuse or disclosure of ALPR information—more than mere noncompliance with the statute.

The *Mata* court addressed *Bartholomew* and expressed skepticism about the "right to know"

harm, but distinguished *Bartholomew*'s limited holding and confined it to businesses without an ALPR policy. In other words, if a business fails to draft and display a written ALPR policy, the absence of that policy may satisfy the statute's harm requirement. In contrast, where a business adopts and conspicuously posts a written ALPR policy, then a plaintiff must show harm distinct from the asserted statutory violation, such as actual harm by the collection or use of the license plate data.

McGinity: Federal Court Follows *Bartholomew*

On August 5, 2026, a Northern District of California court added another decision supporting and adopting the *Bartholomew* analysis. In *McGinity v. Reimagined Parking LLC*,⁴ the plaintiff claimed he parked in a lot that used ALPR technology but that did not have or post an ALPR usage policy. The court denied the parking lot operator's motion to dismiss on the basis that the plaintiff "adequately alleged actionable harm to his 'right to know' about the use of ALPRs in the two garages at issue," following the *Bartholomew* reasoning that failure to have a posted ALPR policy constituted "harm" under the statute. The court noted its confidence that the California Supreme Court would conclude that a violation of a consumer's "right to know" would be an actionable harm under the ALPR statute.

What Businesses Should Do Now

Together, *Bartholomew*, *Mata*, and *McGinity* provide businesses with a clearer pathway of the ALPR law going forward. Businesses subject to the statute should promptly confirm that they have an ALPR policy in place. Doing so may reduce risk of lawsuits along the lines of *Bartholomew* and *McGinity* and will require plaintiffs to plead and prove actual harm beyond a mere statutory violation to succeed. Additionally, because these ALPR lawsuits are on the rise, businesses that fall within the law's purview should consider taking the following steps:

- Identify all locations where cameras or parking systems capture license plate information.
- Determine whether those systems create or access a searchable database of license plate information.
- Confirm whether the business is an ALPR "operator," "end-user," or both.

⁴ 2026 WL 2322918 (N.D. Cal. Aug. 5, 2026).

- Review vendor contracts to understand who collects, stores, accesses, shares, and deletes ALPR information.
- Adopt a written ALPR usage and privacy policy that includes all required statutory elements.
- Post the policy conspicuously on the business's website and make it available in writing.
- Review retention, access, audit, training, and security practices to ensure they match the posted policy.
- Periodically audit compliance, particularly when deploying new parking, security, or access-control technology.

Conclusion

The recent wave of ALPR litigation shows that businesses may face legal claims not only arising from the collection or use of license plate data, but also from the absence of a posted, statute-compliant policy. After *Bartholomew* and *McGinity*, one of the most important steps businesses can take to reduce litigation exposure is to adopt and post a compliant ALPR policy.

Privacy, Cybersecurity & AI: Questions to Consider Going Into 2027

The legal landscape is changing quickly, but businesses do not need to address every development at once. This checklist is designed to help you quickly spot where recent changes may affect your existing practices so that you can focus on the issues that create the most risk to your business.

How to use this checklist: Check the box next to each statement that applies, or might apply, to your business. Each item includes a short question to ask internally and a brief note on why it matters.

- ☐ **You, or your employees, vendors, or software platforms use AI.**
Ask yourself: Are employees, vendors, or existing software platforms using AI tools that have not been formally reviewed, particularly for hiring, customer interactions, pricing, decision-making, or meeting transcription, or to take actions on behalf of the business?
Why it matters: Unreviewed AI use in these areas can create legal obligations and liability your business may not know it has taken on.
- ☐ **You have not reassessed which state privacy laws apply to you this year.**
Ask yourself: Have you recently reassessed which state privacy laws apply to your business?
Why it matters: Lower thresholds, narrower exemptions, and new requirements taking effect in 2027 may bring businesses into scope for new laws.
- ☐ **You collect or share sensitive personal information.**
Ask yourself: Does your business use health, biometric, precise geolocation, financial, minors', or other sensitive information in advertising, analytics, AI, or vendor relationships?
Why it matters: Sensitive information is often subject to heightened consent, notice, and handling requirements, and misuse can carry greater risk.
- ☐ **Your vendors receive meaningful amounts of personal information.**
Ask yourself: Have your vendor diligence and contract requirements kept up with new privacy, security, and AI obligations?
Why it matters: Your business may be responsible for how vendors handle your data. Delaware, for example, now imposes expanded third-party contracting and diligence requirements.
- ☐ **Your website or app uses tracking technologies.**
Ask yourself: Do your cookies, pixels, chat tools, analytics, and other technologies operate consistently with your consent flows, banners, opt-outs, vendor terms, and privacy disclosures, and have you tested them recently?
Why it matters: A mismatch between what your disclosures say and what your technology actually does can create compliance and dispute risk.
- ☐ **You engage in higher-risk processing (such as selling or sharing personal information or processing sensitive personal information) or use automated decision-making technology.**
Ask yourself: Have you identified whether any of your higher-risk processing activities, including certain uses of automated decision-making technology, trigger the CCPA's risk assessment requirements?
Why it matters: Determining whether assessments are required, and preparing them, takes time and is best addressed as soon as possible.

☐ **You do business in California and process significant volumes of personal information.**

Ask yourself: Have you determined whether your revenue and data-processing volumes bring you within the new cybersecurity audit rules?

Why it matters: If the rules apply, you will need to know when your first audit period begins so you can plan ahead.

☐ **You have not reviewed your retention and deletion practices in the past year.**

Ask yourself: Do you know how long personal information, AI-generated content, recordings, transcripts, and other records are retained, including copies held by vendors or in other systems? Have you tested your retention and deletion processes recently?

Why it matters: You may need to delete information when required, which is difficult if you do not know where it is kept.

☐ **You buy, sell, license, or enrich personal information.**

Ask yourself: Do you purchase lists or data sets, receive personal information from partners, sell or license personal information to others, or combine outside data with your own records to build more detailed profiles?

Why it matters: Businesses that engage in these activities may be considered data brokers and required to register with regulators in California, New Jersey, or other states, with penalties for failing to do so.

☐ **You offer products or services accessible to or used by children or teenagers.**

Ask yourself: Do your age, consent, deletion, personalization, or AI practices account for younger users?

Why it matters: Regulators are increasingly focused on minors' privacy and product design.

If you checked any box, or answered "maybe" or "we have not looked at this recently," it may be worth taking a closer look to determine whether any action is needed.

Next step: Contact Coblentz's Data Privacy & Cybersecurity team. We can help determine which developments matter to your business, prioritize the issues that warrant attention, and identify practical next steps.

Contact

Coblentz's Data Privacy & Cybersecurity team advises clients on all aspects of data privacy and cybersecurity, from counseling and guidance for compliance with data privacy laws, including the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), to assisting with data breaches and security incidents.

Our team, led by Scott Hall, a Certified Information Privacy Professional/United States (CIPP/US), Certified Information Privacy Professional/Europe (CIPP/E), and Artificial Intelligence Governance Professional (AIGP), Phillip Wiese, a Certified Information Privacy Professional/United States (CIPP/US), and Meaghan Henderson, a Certified Information Privacy Professional/United States (CIPP/US) and Certified Information Privacy Professional/Europe (CIPP/E), helps companies navigate the complex and rapidly evolving privacy, cybersecurity, and artificial intelligence landscape.

We assist clients with privacy compliance programs and policy updates, advise on new and emerging privacy and AI laws, support incident response and breach-related obligations, and represent clients in privacy, cybersecurity, and data-related litigation and regulatory matters. Our team also helps clients manage the legal and business risks associated with the electronic collection, storage, use, sharing, and protection of information, including as new technologies and regulatory requirements reshape how businesses collect and use data.

Please contact a member of the team below for further information or assistance.

Authors



Scott C. Hall

**Head of Data Privacy and Cybersecurity Group
Partner**
San Francisco

Contact
415.772.5798
shall@coblentzlaw.com



Phillip J. Wiese

Special Counsel
San Francisco

Contact
415.268.0502
pwiese@coblentzlaw.com



Meaghan Henderson

Associate
San Francisco

Contact
415.268.4109
mhenderson@coblentzlaw.com



Katie Berens

Associate
San Francisco

Contact
415.268.0534
kberens@coblentzlaw.com



Katherine Gianelli

Associate
San Francisco

Contact
415.268.0594
kgianelli@coblentzlaw.com



Dillon Ostlund

Associate
San Francisco

Contact
415.268.0537
dostlund@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP

One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com