Coblentz
Patch Duffy
& Bass LLP

2026 Spring Privacy Report

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

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com

Spring 2026

Contents

Introduction

Privacy, cybersecurity, and AI regulation continue to be front and center in all aspects of business operations. Two additional states, Oklahoma and Alabama, have recently passed comprehensive consumer privacy laws, increasing the patchwork enforcement framework across the country, while federal laws continue to be proposed but may not be any closer than before. At the same time, regulators have accelerated enforcement actions against companies that do not comply with state laws, and privacy litigation continues to flood dockets with claims for violations of the California Invasion of Privacy Act (CIPA) and the Video Privacy Protection Act (VPPA). Companies are also facing increased regulatory scrutiny over the collection and use of health data and minors' data, while also navigating uncertain waters with respect to the intersection of artificial intelligence governance and consumer privacy.

This report examines some of the significant developments shaping the privacy and AI landscape this year. First, the report examines the AI legal and regulatory landscape at the state and federal levels. Second, it analyzes state enforcement of the California Consumer Privacy Act (CCPA), as well as obligations under recent CCPA regulations and other state laws. Third, it evaluates trends in the privacy litigation space, including litigation involving CIPA, VPPA, the California Comprehensive Computer Data Access and Fraud Act (CDAFA), and the Illinois Biometric Information Privacy Act (BIPA).

California Privacy Enforcement: What's New Since Our Mid-Year Privacy Report

> *Regulators are less interested in 'paper compliance' than whether consumer choices actually work across real-world tech stacks, devices, and vendors.*

Since our 2025 mid-year report highlighted the CPPA's (now CalPrivacy's) early enforcement playbook (Honda and Todd Snyder) and the California Attorney General's landmark Healthline settlement, California regulators have kept up the pace into early 2026. Recent enforcement matters confirm that regulators are less interested in "paper compliance" than whether consumer choices actually work across real-world tech stacks, devices, and vendors. They also show expanding attention to (1) streaming/CTV ecosystems, (2) mobile apps (including youth data), (3) job applicant/employee-related data, and (4) data broker obligations under the Delete Act.

Below is a brief summary of new enforcement actions and an analysis of enforcement themes.

Recent Enforcement Actions and Developments

- **General Motors: Disclosure and consent are necessary when providing consumer data to data brokers.**

  In May 2026, the California Attorney General announced a $12.75 million settlement—the highest amount levied to date—with General Motors (GM) for allegedly selling the driving data and location information for hundreds of thousands of California drivers without their consent. GM allegedly collected information, including names, phone numbers, home addresses, speeds, rapid acceleration, hard braking, and precise geolocation, through the OnStar system, while informing consumers its data would only be used for OnStar systems. Then, GM is alleged to have turned around and sold that information to two data brokers that were developing products for auto insurers based on driving behavior. Going forward, businesses should consider the amount of data they are collecting and not collect more than necessary. They should also obtain clear consent from consumers to disclose the data they collect—the Attorney General is focused on companies that sell information to data brokers without informing consumers. This enforcement action suggests that the Attorney General intends to take Delete Act compliance seriously as well.

- **Disney: "Account-wide" opt-outs across services and devices are expected and required.**

  In February 2026, the California Attorney General announced a $2.75 million settlement with Disney entities tied to Disney's streaming ecosystem. The core allegation was functional—namely, that consumers would try to opt out through toggles, a webform, or Global Privacy Control (GPC), but those signals allegedly did not fully propagate across the "bundle" of services and devices tied to the consumer's account—leaving gaps where sale/sharing continued.

  This is the clearest statement yet (in enforcement posture) that if a business can link devices/services to a consumer for advertising or measurement, regulators expect it to be able to link those same devices/services to the consumer's privacy elections—and to do so comprehensively.

- **PlayOn Sports: CalPrivacy tackles opt-out mechanisms in high school sports website.**

  In March 2026, CalPrivacy announced a $1.10 million decision against PlayOn Sports, a media company that sells digital tickets to certain high school events, including football games, theater performances, and school dances. According to CalPrivacy, high school students were required to

agree to the use of tracking technology and collection of personal information without a meaningful way to opt out of that data collection in order to use the website. This enforcement action represented CalPrivacy's first foray into enforcing the CCPA expressly on behalf of minors, describing the high school students as a "uniquely vulnerable population."

- **Ford Motor Co.: Opt-out requests need not be verified.**

  In March 2026, CalPrivacy also announced a $375,000 decision against Ford Motor Company, finding that the automaker created "unnecessary friction" by improperly processing consumer requests to opt out of the sale or sharing of personal information. In particular, Ford used a standardized form for all CCPA requests, including the right to opt out, and then required consumers to respond to a follow-up email to verify their identity. While companies can require verification for certain CCPA requests, including the rights to know, correct, and delete, the CCPA does not provide a similar verification process for opting out of data selling or sharing. Companies may consider utilizing different workstreams for opt-out requests and other CCPA-related requests to avoid this issue.

- **Tractor Supply Co.: Opt-out mechanisms must work properly.**

  In September 2025, CalPrivacy announced a $1.35 million decision against rural lifestyle retailer Tractor Supply Company after a single consumer reported Tractor Supply's privacy practices to the agency. CalPrivacy determined that Tractor Supply violated the CCPA in numerous ways. Critically, the CalPrivacy decision stated that Tractor Supply had a webform that did not in practice allow consumers to opt out of the sale or sharing of personal information. According to CalPrivacy, consumers could fill out a webform purporting to allow them to opt out of data sharing/selling, but Tractor Supply took no action to effectuate those requests. Additionally, CalPrivacy stated that Tractor Supply lacked CCPA-compliant contracts with service providers and other third parties, and that Tractor Supply did not provide all requisite notices under the CCPA, including to job applicants. As a result of these issues, Tractor Supply received the largest fine levied to date by CalPrivacy.

- **Jam City: Don't forget about mobile app opt-outs and under-16 protections.**

  In November 2025, the AG announced a $1.4 million settlement with a mobile app gaming company. The AG's announcement emphasized two points: (1) if personal information is sold/shared through mobile apps, consumers need compliant opt-out methods *in-app*, and (2) the CCPA's heightened protections for consumers under 16 (affirmative opt-in for sale/sharing) are an active enforcement area. This builds directly on the mid-year theme that enforcement is moving from websites into the app ecosystem and is increasingly focused on whether the consumer experience is simple and effective.

- **CalPrivacy (CPPA): Delete Act/data broker enforcement.**

  In January 2026, CalPrivacy announced enforcement actions against a marketing firm and a technology firm for each failing to register as a data broker. CalPrivacy claimed that the marketing firm was selling personal information about individuals with certain health conditions for targeted advertising and emphasized that simply packaging personal information into "custom audiences" or value-added products does not avoid data broker obligations. This connects to the broader enforcement theme that regulators are looking through form to function: if the business model involves the buying or selling of consumers' personal information, it must comply with the CCPA and the Delete Act.

Privacy Enforcement Themes to Keep Top of Mind

- **Regulators expect "functional" opt-outs, including end-to-end propagation across vendors, devices, and services.** These latest enforcement actions make clear that the regulators expect companies to create a straightforward and streamlined consumer opt-out process. If, for example, a consumer opts out of data sharing/selling, that request must be fulfilled across the company's entire ecosystem unless the consumer specifically limits the request. The

company cannot unilaterally exempt certain verticals or parts of the business. Additionally, the opt-out methods must meaningfully allow consumers to opt out of data sharing/selling. Webforms, Global Privacy Controls, and other opt-out methods must be checked regularly to ensure functionality. Regulators have been quick to act where those methods do not work as expected.

- **Regulators expect low-friction user experience—and will treat friction as a compliance risk.** Both CalPrivacy and the AG have focused on the specific opt-out mechanisms for data collection or data selling/sharing, targeting companies that appear to have made it difficult or impossible to opt out of data sharing/selling while still using mobile apps. For example, the regulators have looked unfavorably on cookie banners that cover critical website functions and that must be accepted before the consumer can use the website. This is especially the case where the user must accept cookies, rather than choosing whether to accept or reject cookies. And on the topic of cookie banners, companies should consider evaluating their cookie banners to ensure symmetry of choice for both allowing and rejecting cookies.

- **Youth and sensitive-context data remain high priority.** CalPrivacy noted in its announcement of the PlayOn decision that students are "uniquely vulnerable," and any websites they use should not "fuel advertising and commercial surveillance" at the expense of enhancing their educational opportunities. Similarly, the AG has cracked down on companies allegedly selling children's information as well as disseminating sensitive consumer health information. Companies should consider reviewing their data collection practices to determine whether they collect, share or sell these types of data, and if so, evaluate whether proper disclosures are in place.

Your Key Next Steps

- **Audit your opt-out functionality across all web, mobile, and platform integrations** and ensure a consistent and defensible approach. The opt-out process should be straightforward and streamlined.

- **Inventory service provider/contractor/third-party contracts** for required restrictions and flow-down obligations—especially in advertising and analytics. The regulators continue to monitor the adequacy of the contracts governing these relationships.

- **Reassess youth and student-data touchpoints**, including age-gating logic, opt-in mechanisms, SDK behavior, retention, and security controls.

- **Evaluate data broker status** (including "custom audience" and profiling services) and confirm registration/fees where required. Additionally, prepare for an influx of Delete Request and Opt-out Platform (DROP) requests. DROP was released to the public in January 2026, and data brokers must begin deleting data within 90 days, starting August 1, 2026.

- **Don't forget about applicant/HR privacy.** Because employees and job applicants are covered by the CCPA, take time to review or revise notices and rights processes for those individuals.

For a summary of recent enforcement actions, please see the "California Enforcement Actions" table on the following page.

California Enforcement Actions

Date	Company	Agency	Fine / Payment	Key Issues
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

AI Privacy and Regulation Update

> *Less federal oversight does not necessarily mean lower risk. In practice, it often means less uniformity, more uncertainty, and greater pressure to track what states, regulators, and private plaintiffs are doing without a lot of central guidance.*

Artificial intelligence regulation has entered a new phase. What started as policy conversations about innovation, ethics, and voluntary guardrails is now a real compliance issue centered on privacy, transparency, discrimination risk, and accountability for automated outcomes. For businesses, the question is no longer just whether to use AI, but how to use it responsibly, lawfully, ethically, and efficiently, while building trust with consumers.

California remains one of the key states to watch. The state has continued to expand its privacy framework in ways that directly affect AI systems, including through the CPPA's finalized rules on automated decision-making technology, risk assessments, and cybersecurity audits, as well as statutes addressing AI disclosures, training-data transparency, and synthetic content. Those developments are important —not just because of California's market power, but because they reflect a broader regulatory instinct: treating AI as part of the privacy and consumer protection landscape, especially when automated tools rely on personal information.

At the same time, federal AI policy has become more unsettled. Rather than moving toward one comprehensive federal law, the national approach has continued to shift with changing administrations, executive branch priorities, and agency agendas. President Trump recently issued a "National Policy Framework for Artificial Intelligence" intended to preempt state law and address seven objectives that, in many ways, directly contradict the AI framework set out by the Biden administration and states that have already implemented AI regulations. In particular, rather than tighten restrictions on AI systems, the Trump framework would avoid broad content standards with the goal of avoiding excessive litigation. Even if the framework is not enacted, the uncertainty leaves businesses in an awkward position. Less federal oversight does not necessarily mean lower risk. In practice, it often means less uniformity, more uncertainty, and greater pressure to track what states, regulators, and private plaintiffs are doing without a lot of central guidance.

This reality helps explain why states continue to move aggressively to fill the gap. Some are adopting broad, risk-based AI frameworks. Others are focusing on narrower but still important issues, such as chatbot disclosures, profiling, health-related uses, insurance determinations, and AI tools used in employment decisions. The regulatory picture is developing issue by issue and sector by sector, rather than through a single national standard. That legal and regulatory patchwork—which is familiar in the privacy landscape—is harder for businesses to manage, but it is quickly becoming the reality for AI.

One notable theme is that states are increasingly using existing legal frameworks to address AI risk, rather than waiting for entirely new AI statutes. In employment, for example, states are starting to apply discrimination principles directly to automated hiring and screening tools. In privacy, states are using profiling, sensitive-data, and transparency rules to reach AI systems that make or support consequential decisions. That means companies must not only monitor new AI laws, but also consider how older laws may apply to the new technologies they are using.

We are also likely to see different rules for different AI uses. Not every AI-enabled tool will draw the same level of scrutiny. Consumer-facing tools that support routine tasks are likely to face lighter oversight than systems used for underwriting, hiring, eligibility, diagnosis, or other decisions that can significantly affect individuals. That risk-based approach is consistent with both the EU model and California's Automated Decisionmaking Technology (ADMT) rules, which focus more closely on significant decision-making contexts.

For companies, the practical takeaway is that compliance efforts should be prioritized based on use case, not just on whether a tool is labeled "AI."

Globally, the EU AI Act remains the leading comprehensive model, with obligations tied to risk classification and substantial requirements for high-risk and general-purpose AI systems. Other jurisdictions are taking different approaches, but the overall direction is the same: more formal governance and more regulatory interest in documentation, transparency, and accountability. For companies operating across borders, that means AI compliance cannot be treated solely as a U.S. state-law issue. It increasingly requires a governance structure that can respond to different legal triggers while maintaining a consistent baseline of documentation and control.

We can also expect regulators to dig deeper into how AI works in practice. They want to know what data a system uses, how its outputs are reviewed, whether human oversight is real or just nominal, and whether the system creates privacy, fairness, or transparency concerns. As a result, AI governance is starting to look a lot like privacy compliance: inventorying systems, documenting use cases, assessing risk, limiting data use, testing for problems, and putting controls in place that can be defended later. Accountability in how AI is actually used matters more than simply having a policy on paper. It is also worth noting that enforcement risk is not limited to agency action. As AI becomes more embedded in decision-making, private plaintiffs are also testing new theories in private litigation, including through discrimination claims for AI use in employment and hiring decisions, or wiretapping claims for AI notetaking tools or other online services.

Ultimately, AI regulation is not emerging through just one statute, one agency, or one theory of liability. It is developing through privacy law, consumer protection, sector-specific regulation, administrative rulemaking, state legislation, and private litigation, often all at once. In the U.S., California remains one of the clearest signals of where this is heading, but it is not alone.

Businesses adopting AI should expect questions not just about what the technology can do, but about what data is used, how it is governed, whether and how humans remain accountable, and whether AI use matches reasonable expectations of privacy and fairness. As AI becomes embedded in business operations, companies will be best positioned to manage risk when governance is built into everyday decision-making and workflows, rather than addressed only after problems arise.

CalPrivacy to Begin CCPA Compliance Audits

CalPrivacy (formerly the California Privacy Protection Agency) recently announced that it intends to begin auditing businesses' compliance with the California Consumer Privacy Act (CCPA).

In February 2026, CalPrivacy formed its Audits Division to conduct compliance audits. The agency expects those audits to begin later this year and will focus on obtaining and analyzing privacy and technology records to ensure businesses are adhering to the CCPA's requirements. CalPrivacy also expects the Audits Division to work closely with the Enforcement Division, which has been settling enforcement proceedings in recent months.

While CalPrivacy has not identified the initial focus areas of its audits, businesses should confirm compliance with all aspects of the CCPA. Recently, the CalPrivacy Enforcement Division has paid particular attention to children's data, minimizing friction for exercising CCPA rights, and data broker obligations. Under the CCPA, businesses must also have a comprehensive privacy policy, updated on an annual basis.

Navigating California's Data Broker Requirements in 2026

> *2026 introduces significant new operational obligations, including DROP-based deletion workflows.*

California's data broker regulations continue to evolve, raising important compliance questions for businesses that compile and license personal data, including what constitutes a data broker and what obligations attach to those businesses. Those questions are often not straightforward, especially where personal information is collected through publicly available databases. Companies operating in B2B data markets should review and assess their obligations under the California Consumer Privacy Act (CCPA) and California's Data Broker Law as updated by SB 362 and SB 361.

SB 362 and SB 361 amended California's Data Broker Law by adding new obligations for businesses that qualify as data brokers: SB 362 (the "Delete Act") established a centralized deletion mechanism and new operational requirements, including the Delete Request and Opt-out Platform ("DROP") system, while SB 361 (the "Defending Californians' Data Act") expanded registration disclosure and transparency obligations.

When Does a Business Qualify as a Data Broker?

A "data broker" is a business that knowingly collects and sells personal information about consumers with whom it does not have a direct relationship. This definition incorporates key terms from the CCPA, including "personal information" and "sale."

A critical threshold issue is whether the data being collected and sold qualifies as "personal information." "Sale," here and under the CCPA, means to sell, rent, disclose, make available, or otherwise disseminate a consumer's personal information in exchange for monetary or other valuable consideration. And "personal information" is information that identifies, relates to, or could reasonably be linked with a consumer or a consumer's household.

The CCPA excludes certain publicly available information from the definition of personal information, including information lawfully made available from federal, state, or local government records, certain information made available to the general public by the consumer or from widely distributed media, and certain information made available by a person to whom the consumer disclosed the information, if the consumer has not restricted it to a specific audience.

As a result, a business that collects and sells only publicly available information may not be handling "personal information" for purposes of the data broker definition. However, there is no categorical exemption for businesses that rely on public records. The analysis turns on whether the data retains its status as publicly available information or is transformed through the business's aggregation, enhancement, or licensing practices.

For companies that compile professional contact data from licensing boards or government registries, this distinction can be outcome-determinative. While the CCPA excludes certain publicly available information from the definition of personal information, the analysis may become more complex where that data is aggregated, enhanced, or combined with other sources, raising questions as to whether the resulting dataset continues to qualify as publicly available information.

Do Data Brokers Have to Delete Public Record Data?

An important nuance is that DROP changes how consumers submit deletion requests, but it does not eliminate existing statutory limitations on consumer rights under the CCPA.

Upon receiving a DROP request, a data broker must delete the consumer's personal information in its possession. Critically, however, under the CCPA, publicly available information is excluded from the definition of personal information for certain purposes. As a result, CCPA consumer rights, including the right to deletion, generally do not apply to such information.

CalPrivacy guidance reinforces this point, stating that businesses may deny consumer requests, including deletion requests, where the information at issue is "publicly available information" or otherwise exempt from the CCPA. More broadly, data brokers may retain personal information if an applicable CalPrivacy deletion exception applies. These exceptions include, among others, completing transactions, security and fraud prevention, legal compliance, and internal operational uses. When an exception applies, the business must limit use of retained data to the purpose justifying retention.

At the same time, businesses should avoid treating this as a blanket exemption. Whether information qualifies as publicly available is a fact-specific inquiry, particularly where data is aggregated, enhanced, or combined with other datasets. If a business holds both exempt publicly available information and non-exempt personal information about a consumer, the non-exempt data may still need to be deleted in response to a request.

In addition, even where a deletion request is denied, other obligations may still apply. For example, if a business sells or shares personal information, it must still inform consumers of their right to opt out of such sale or sharing.

Accordingly, while DROP introduces new operational requirements for processing deletion requests, it does not expand the scope of what information must ultimately be deleted under the CCPA. Depending on the volume and type of data collected, this process could take time, so businesses may want to start categorizing their data now, ahead of the August 1 deadline to begin processing deletion requests.

"Direct Relationship" Interpretation

The Data Broker Law also requires that the business lack a "direct relationship" with consumers. The recent Delete Act regulations add crucial context defining a direct relationship as one in which the "consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services."

This definition is important for businesses that collect data through indirect or passive means, including third-party tracking technologies, data append services, or third-party datasets. A business should not assume that collecting data directly from a consumer necessarily creates a direct relationship. The consumer's interaction must be intentional and directed to the business's own products or services.

Even with this definition, important questions remain. For example, businesses may still need to assess how the concept applies in attenuated B2B contexts, whether particular interactions with individual business representatives are sufficient, and how data obtained outside a first-party interaction should be treated. These issues require careful, fact-specific analysis.

2026 Compliance Timeline and Requirements

While determining whether a company is a data broker can be complicated, once that determination has been made, the compliance timeline and requirements are more straightforward. Businesses that qualify as data brokers face several key obligations beginning in 2026:

- **Registration:** Data brokers must register annually with CalPrivacy (formerly the CPPA) by January 31 following each year in which they meet the definition.
- **DROP System:** As part of registration, businesses must create an account on CalPrivacy's Delete Request and Opt-Out Platform (DROP), which took effect on January 1, 2026. Then, beginning August 1, 2026, data brokers must access the DROP system at least once every 45 days and process verified deletion requests through it, subject to

statutory exceptions. While this obligation does not affect whether the Company must register for 2026, it is a new material operational compliance requirement after registration.
- **Metrics Reporting:** By July 1 each year, data brokers must publish detailed metrics in their privacy policies regarding consumer requests, including the number of requests received, fulfilled, and denied, and response times.
- **Audits:** Starting January 1, 2028, data brokers must undergo independent third-party audits every three years and maintain audit records for six years.

SB 362 and SB 361 expand disclosure and operational requirements, including more detailed reporting on the categories of personal information collected and consumer request handling.

Enforcement Risk and Prior-Year Exposure

CalPrivacy has made data broker compliance a clear enforcement priority. The agency has conducted enforcement sweeps and entered into settlements with data brokers for violations of the Delete Act, signaling increased scrutiny.

Failure to comply with registration requirements can result in:

- Administrative fines of $200 per day of non-compliance;
- Payment of unpaid registration fees; and
- Recovery of CalPrivacy's investigative and enforcement costs.

Separate penalties may apply for failure to comply with deletion requirements, including fines of $200 per day per unfulfilled deletion request.

In addition, CalPrivacy and the California Attorney General may seek civil penalties of up to $2,663 per violation and $7,988 per intentional violation, including for violations involving minors. Importantly, these penalties may apply not only to current violations, but also to prior-year conduct within the applicable statute of limitations.

Key Takeaways

For B2B businesses that license or monetize data, several takeaways emerge:

- Public record sourcing does not automatically resolve data broker status.
- Whether data qualifies as "publicly available" under the CCPA is a critical threshold issue.
- The meaning of "direct relationship" requires careful, fact-specific legal analysis.
- 2026 introduces significant new operational obligations, including DROP-based deletion workflows.
- Enforcement is active, and non-compliance carries meaningful financial and operational risk.

Given these developments, businesses should evaluate their data practices now to determine whether they may qualify as data brokers and to prepare for upcoming registration and compliance requirements.

CCPA Risk Assessment Requirements: What Businesses Need to Do Now

> *This framework transforms risk assessments into regulator-facing documents, not just internal analyses.*

Since CalPrivacy (formerly the CPPA) finalized sweeping updates to the California Consumer Privacy Act (CCPA) regulations in July 2025, risk assessments are now a centerpiece of data privacy compliance. The message from regulators is clear: California is moving decisively toward a proactive, risk-based privacy regime, and businesses will be expected to evaluate and document their higher-risk data practices before they occur.

For many organizations, this marks a significant evolution in compliance expectations. Risk assessments are no longer a matter of internal best practice. They are now a formal, enforceable requirement that will demand new processes, closer coordination across teams, and greater executive oversight and accountability.

Risk Assessments As a Core Compliance Obligation

Beginning January 1, 2026, businesses subject to the CCPA must conduct risk assessments for processing activities that present a "significant risk" to consumers' privacy. These assessments must be completed before the relevant processing takes place, reflecting a shift away from reactive compliance and toward forward-looking risk management.

The scope of what constitutes "significant risk" is broad. In practice, it will capture many common data-driven activities, including the sale or sharing of personal information, the use of sensitive personal data such as precise geolocation or health information, and the deployment of automated decision-making technologies in consequential contexts like hiring, lending, or housing. Profiling in workplace or educational environments, as well as certain AI and analytics tools that infer consumer characteristics, also fall within the scope.

For companies that rely heavily on data analytics, targeted advertising, or use of automated decision-making technology, this means that risk assessments are likely to become a routine and recurring part of operations, rather than an occasional compliance exercise.

A Structured and Substantive Analysis

The CCPA regulations set forth the specific information an assessment must contain. Businesses will need to prepare a written analysis that clearly explains the purpose of the processing, the categories of personal information involved, and how the data will be used, retained, and shared. Business employees whose job duties include participating in the processing of personal information subject to a risk assessment must be included in the business's risk assessment process.

At the heart of the requirement is a balancing test: organizations must weigh the benefits of the processing, both to the business and to consumers, against the foreseeable risks to individual privacy. In doing so, the analysis must:

- Identify the specific business purpose for processing;
- Identify the categories of personal information involved, including any sensitive personal information, and the minimum information necessary for achieving the stated business purpose;
- Identify any safeguards in place to mitigate risks; and

- Document operational details of the processing, including:
  - How the information is collected, used, and disclosed;
  - The duration of retention (or how such duration will be determined);
  - How the business interacts with customers;
  - How many customers are affected;
  - What disclosures the business makes to customers about the processing; and
  - What third parties (service providers, contractors, or otherwise) will have access to that information and what purpose that access will serve.

This assessment requires thoughtful judgment and attention to detail as those with knowledge of the processing consider questions about the business's data processing practices.

As noted, risk assessments must be completed prior to initiating any processing activity that presents a significant risk to consumer privacy. Additionally, businesses must update their risk assessments within 45 days when there is a material change relating to the processing activity, or, at minimum, every three years.

Reporting Obligations

CalPrivacy has coupled these substantive requirements with new reporting and certification obligations. Businesses will be required to submit summaries of their risk assessments by April 1 the year after they have been completed, starting April 1, 2028. The summary must certify under penalty of perjury that the substance of the risk assessment is correct. While full assessments do not need to be routinely filed, they must be maintained and produced upon request.

This framework transforms risk assessments into regulator-facing documents, not just internal analyses. As a result, companies should expect that their reasoning, methodologies, and conclusions could be scrutinized in an enforcement context by CalPrivacy.

Implementation Timelines and Transition

The regulations provide a phased timeline, but the runway is shorter than it may appear.

The obligation to conduct risk assessments began in January 2026, and existing data processing activities must be evaluated and a risk assessment prepared by the end of 2027, covering processing during 2026 and 2027. But for any new processing activities started after January 1, 2026 that trigger compliance obligations, a risk assessment must be completed before that new processing can begin. The first round of annual reporting is set to occur on April 1, 2028, with ongoing summary submissions required each year thereafter.

Given the breadth of in-scope activities and the level of detail required, many organizations will need substantial lead time to build and operationalize compliant programs.

Preparing for Risk-Based Privacy Practices

The practical impact of these requirements will extend across the enterprise. Legal and privacy teams will need to develop standardized frameworks and documentation processes, while product, engineering, and data teams will need to integrate risk analysis into development lifecycles. Security functions will play a key role in aligning technical safeguards with identified risks, and senior leadership may be called upon to review and certify compliance.

Organizations that have not yet formalized their data governance practices may face particular challenges, especially in mapping data flows and documenting decision-making. At the same time, companies with more mature privacy programs will need to revisit and enhance their existing processes to meet CalPrivacy's more prescriptive and transparent requirements.

Looking Ahead

California's regulations reinforce its position at the forefront of U.S. privacy law and reflect a broader global trend toward risk-based regulation. For businesses, the takeaway is clear: now is the time to conduct risk assessments on relevant processing activities and to start preparing plans to submit summary assessments to CalPrivacy.

Organizations that act now to build scalable, defensible risk assessment programs will be better positioned not only to meet regulatory expectations, but also to support responsible innovation in an increasingly complex data landscape.

California Age-Appropriate Design Code Act

The Ninth Circuit recently issued a decision partially lifting a broad preliminary injunction staying enforcement of the California Age-Appropriate Design Code Act ("CAADCA"). As a result, portions of the law are now in effect and create ongoing obligations for businesses that provide online services, products, or features "likely to be accessed by children." Those provisions are described below.

By way of background, the California legislature in 2022 enacted the California Age-Appropriate Design Code Act ("CAADCA"), which established certain standards to protect children's privacy online. Importantly, the law defined a child as anyone under 18 years old. This creates a separate age threshold from the CCPA, which imposes certain obligations for children under 13 and under 16 years old. Practically since the CAADCA was enacted, the law has faced legal challenges and has been preliminarily enjoined by courts, but as a result of the recent Ninth Circuit decision, the preliminary injunction as to the entire law has been lifted and portions of the law are now in effect.

Although litigation is ongoing and the implementation of the law continues to develop, the CAADCA imposes the following obligations for businesses:

- Estimate the age of child users or apply a "high level" of privacy protection to all users;
- Set privacy settings for children to the highest level by default;
- Use age-appropriate language for privacy policies aimed at children;
- Allow parents to monitor the child's online activity and provide a signal to the child when being tracked;
- Provide tools to help users exercise their privacy rights;
- Minimize and limit the usage of personal information collected to estimate a child's age; and
- Not process a child's precise geolocation by default or absent a signal that the geolocation is being collected.

There are also a number of provisions that are not in effect and remain subject to the Ninth Circuit's preliminary injunction:

- Businesses are not presently required to conduct Data Protection Impact Assessments ("DPIA") for any product or service likely to be accessed or used by children. The Ninth Circuit held that this was a violation of First Amendment rights.

- There are a number of prohibitions in the CAADCA on collecting or using children's personal information (1) that the business knows "is materially detrimental to the physical health, mental health, or well-being of a child" or (2) absent a compelling reason that the collection or use "is in the best interests of children." The Ninth Circuit held that the quoted language was unconstitutionally vague and those prohibitions are not enforceable.

In addition to the evolving legal landscape in California, other state legislatures have started drafting their own child privacy laws. Similar laws have been enacted in Arkansas, Colorado, Louisiana, Maryland, Mississippi, Montana, Nebraska, New York, Texas, Utah, and Vermont, although no two laws are the same. And while legal challenges have been raised with respect to many of these laws, the focus on children's privacy rights remains clear. We expect these laws to be the focus of state regulators and privacy advocates for the foreseeable future.

Wiretap Litigation Update

Plaintiffs have continued to file privacy litigation at a furious pace, asserting claims under the California Invasion of Privacy Act (CIPA), the federal Video Privacy Protection Act (VPPA), and, increasingly, the federal Electronic Communications Privacy Act (ECPA). Plaintiffs have paid particular attention to the healthcare and financial services spaces, focusing on purported collection of sensitive personal information, but suits against other consumer retailers and service providers have not slowed either. These suits remain centered on modern tracking technologies like pixels, session replay tools, cookies, and embedded analytics software.

Case law on these issues remains in flux, although suits are beginning to trickle up to the appellate level for review. With respect to the VPPA, the Supreme Court is set to hear a case about how broadly the definition of "consumer" should be interpreted. Additionally, the Ninth Circuit attempted to clarify Article III standing in CIPA and ECPA claims, but lower courts have split when applying its holding. And the California federal court/state court divide continues to deepen when determining if cookies and pixels are covered by the CIPA pen register and trap and trace law. Against this backdrop of uncertainty, the California legislature is weighing whether to amend CIPA through SB 690, but there has been no movement at this point in the legislative cycle.

Supreme Court Grants Certiorari in VPPA Case

In January 2026, the Supreme Court agreed to hear *Salazar v. Paramount Global*, arising from the Sixth Circuit, to settle a circuit split about whether the VPPA requires that a "consumer" subscribe to audiovisual goods or services from a video tape service provider.

The VPPA prohibits a "video tape service provider" from disclosing any personally identifiable information about a "consumer." A "video tape service provider" is someone that rents, sells, or delivers "prerecorded video cassette tapes or similar audio visual materials." A "consumer" is "any renter, purchaser, or subscriber of goods or services from a video tape service provider."

The plaintiff alleged that he watched video content on a college sports news site, 247Sports.com, and that his Facebook ID and video-viewing history were disclosed to Facebook by Paramount Global, the sports news site's parent company. This disclosure, he claimed, violated the VPPA because 247Sports.com was a video tape service provider and improperly disclosed to Facebook the videos he watched on the website.[1]

The Sixth Circuit disagreed, holding that the plaintiff was not a "consumer" under the statute because while he subscribed to the 247Sports.com newsletter, that was separate from the subscription of audiovisual materials on the website. The Sixth Circuit split from the Second Circuit, which held the opposite, that newsletter subscriptions were sufficient to be a "consumer" under the VPPA, even if the newsletter had no audiovisual content.[2]

The case is likely to be heard during the Court's 2026/2027 term, and if the Court adopts the narrow definition of consumer, the result could significantly slow future VPPA litigation.

Ninth Circuit Clarifies Standing Issues with Respect to Statutory Wiretap Claims

The Ninth Circuit limited Article III standing in privacy cases in its August 2025 decision *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025). In that case, the plaintiff alleged that while browsing for pet food on a pet supply website, her browsing activity was captured by Microsoft's session replay technology. Her claims for violation of Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA) and intrusion upon seclusion were dismissed by the trial court for lack of Article III standing.

[1] *Salazar v. Paramount Global*, 133 F.4th 642 (6th Cir. 2025).

[2] *Salazar v. National Basketball Ass'n*, 118 F.4th 533 (2d Cir. 2024).

The Ninth Circuit affirmed the trial court, concluding that the plaintiff failed to allege a "concrete" injury to support her claim and that a bare statutory violation of WESCA did not satisfy the tests set forth in *Spokeo* and *TransUnion*.[3] Drawing upon *TransUnion*, the Ninth Circuit analyzed whether the plaintiff alleged an injury bearing "a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[4] The Ninth Circuit analogized the plaintiff's claim to the common law torts of intrusion upon seclusion and public disclosure of private facts, both of which require that any intrusion or disclosure be "highly offensive to a reasonable person," and found plaintiff's claims to be lacking.[5] Notably, the plaintiff did not identify any "embarrassing, invasive, or otherwise private information collected by" Microsoft's software.[6] Plaintiff instead pleaded that the technology gathered her pet-store preferences and her street name, none of which was protected or highly offensive. Rather, the interactions were more similar to "a store clerk's observing shoppers in order to identify aisles that are particularly popular or to spot problems that disrupt potential sales."[7] The court noted that the result may differ in other circumstances if a greater volume of data is collected from across the internet and used to create user profiles.

Companies were quick to invoke *Popa* to dismiss claims, but the district courts continue to be split on the issue. Some courts have applied *Popa* broadly, finding that the disclosure of website browsing data was not highly offensive:

- *Garcia v. Blackhawk Network, Inc.*, 2026 WL 925028 (C.D. Cal. Apr. 1, 2026) (Staton, J.), holding that "informing a third party about Plaintiff's interactions with [a] website" was not embarrassing, invasive, or otherwise private;
- *Maghoney v. Dotdash Meredith, Inc.*, 2026 WL 497402 (S.D. Cal. Feb. 23, 2026) (Battaglia, J.), holding that searches for allegedly sensitive health-related terms on a public-facing website were not highly offensive; and
- *Khamooshi v. Politico LLC*, 2025 WL 2822879 (N.D. Cal. Oct. 2, 2025) (Kim, M.J.), holding that browsing activity, geolocation data, and "device fingerprints" were not sufficiently embarrassing, invasive, or otherwise private to support Article III standing.

Other courts distinguish *Popa* by finding the type of data and sheer volume of data allegedly collected cross the "highly offensive" line:

- *Harris v. iHeartMedia, Inc.*, 2026 WL 247875 (N.D. Cal. Jan. 29, 2026) (Lee, J.), holding that the plaintiff had standing because the data was allegedly used to create a "cradle-to-grave profile" of his web browsing activities across the internet;
- *Shah v. MyFitnessPal, Inc.*, 2026 WL 216334 (N.D. Cal. Jan. 27, 2026) (Pitts, J.), holding that plaintiffs had standing because they were allegedly told that sensitive information would not be shared with third parties even though it later was shared; and
- *Semien v. PubMatic Inc.*, 2026 WL 216333 (N.D. Cal. Jan. 27, 2026) (Illston, J.), holding that plaintiffs' allegations that the defendant compiled detailed user profiles by tracking interactions across numerous websites and collected sensitive personal information without consent was sufficient to confer standing.

This decision may not be the panacea companies hoped for, but it, at minimum, increases the burden for plaintiffs at the pleading stage and provides a new line of attack in these challenging CIPA cases.

Divide Grows Between California State and Federal Courts in Pen Register, Trap and Trace Suits

There also appears to be a growing split between state and federal courts in California over whether tracking technology, including cookies and pixels, are pen registers or trap and trace devices that can form the basis of a CIPA section 638.51 claim. Interestingly, both state and federal courts ground their analysis in the statutory text and the legislative history yet reach conflicting results.

[3] *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016); *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021).
[4] *Popa*, 153 F.4th at 789.
[5] *Id.* at 791.
[6] *Id.*
[7] *Id.*

Section 638.51 prohibits using a pen register or trap and trace device without a court order. The state court decisions interpreting this section typically draw on the language from section 638.52 to limit the definition of pen register and trap and trace to telephone lines.[8] This cross-referenced language demonstrates that pen registers and trap and trace devices are separate from software or technology that operates on a computer or other device.[9] State courts also refer to the legislative history of section 638.51 that described the purposes as allowing law enforcement officers to monitor ***telephonic*** communications after obtaining a court order.[10]

While federal courts are obligated to interpret California laws like CIPA the same way the California Supreme Court would, there are no California Supreme Court or Court of Appeals decisions interpreting section 638.51, leaving the federal courts to apply their own standard. The federal courts have, by and large, found that sections 638.50 and 638.51 lack any limitation to telephone, and thus the legislature intended the law to apply broadly to include "evolving privacy threats."[11] This broad statutory language, these courts hold, "is consistent with the California Legislature's stated intent to protect privacy interests."[12]

These conflicting decisions have led to confusion and uncertainty for companies trying to comply with CIPA. For now, section 638.51 liability may depend on the forum in which a suit is filed and the preferences of the individual judge.

No Update on California Wiretap Law Amendment

Meanwhile, plaintiffs and defendants alike continue to watch the California legislature to see whether it will pass legislation to amend CIPA. SB 690, which was introduced in February 2025 but advanced to the 2026 legislative session, would significantly curb the ongoing deluge of CIPA litigation. Specifically, the bill would exempt from CIPA liability the use of recording or tracking technologies that serve a "commercial business purpose," targeting the near-ubiquitous pixels, cookies, and other website tracking technology.

SB 690 garnered strong support in 2025, but there has been no action thus far in the legislative cycle.

Until either the legislature or appellate courts provide clearer guidance, companies should continue to treat website tracking litigation as an active and evolving risk area. Regular review of tracking technologies, consent flows, vendor contracts, and privacy disclosures remains important, especially for businesses operating in sensitive sectors or using tools that collect data across multiple websites or services.

---

[8] An order authorizing installation of a pen register or trap and trace device must specify: "(1) The identity, if known, of the person to whom is leased or in whose name is listed ***the telephone line*** to which the pen register or trap and trace device is to be attached. . . . [and] (3) The number and, if known, physical location of ***the telephone line*** to which the pen register or trap and trace device is to be attached . . . ." Cal. Pen. Code § 638.52(d) (emphasis added).

[9] *See Schallert v. Orkin LLC*, 2025 WL 4332757, at *4 (L.A.S.C. Dec. 15, 2025).

[10] *Id.; see also Rodriguez v. Ink America Int'l Grp. LLC*, 2025 WL 4034985, at *4 (L.A.S.C. Dec. 10, 2025) (holding that the lack of reference to website tracking technology when the law was amended in 2016 and 2022 confirms that the legislature made a "deliberate choice not to sweep ordinary website analytics" into the law's provisions); *Schallert v. Palo Alto Networks, Inc.*, 2026 WL 54028, at *2 (L.A.S.C. Mar. 6, 2026) (same).

[11] *See Fregosa v. Mashable, Inc.*, 2025 WL 2886399, at *5 (N.D. Cal. Oct. 9, 2025).

[12] *Walsh v. Dollar Tree Stores, Inc.*, 2025 WL 2939229, at *18 (N.D. Cal. Oct. 16, 2025) (quoting *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024)).

Beyond CIPA: The Rise of CDAFA in Tracking Technology Litigation

The privacy litigation landscape in California continues to grow in complexity, with plaintiffs advancing new theories of liability based on the use of website tracking technologies. Although California Invasion of Privacy Act ("CIPA") claims under California Penal Code §§ 631 and 638.51 remain the dominant privacy theories in this space, plaintiffs are increasingly asserting claims under the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502 ("CDAFA").

Background

CDAFA is the California analog to the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"). The CFAA, an anti-computer-hacking statute, prohibits intentionally accessing and obtaining information from computers without authorization. Congress enacted the CFAA in 1986 when computer hacking was a growing problem. The statute provided only criminal penalties until 1994, when it was amended to add a private right of action, and then amended further throughout the 1990s and 2000s, most notably following 9/11. As a federal statute, CFAA focuses on interstate issues and activity that jeopardizes national security. CDAFA focuses only on conduct within California.

CDAFA was enacted in 1989 and prohibits 13 categories of activity. Broadly speaking, it penalizes knowingly accessing computers without permission to alter or damage data, wrongfully acquiring or retaining unauthorized access to computers to take or make use of data, and related conduct. Like its federal analog, it creates a private right of action for any "owner or lessee of a computer or computer system" that "suffers damage or loss by reason of a violation of [the CDAFA]."[1] CDAFA does not define "damage or loss," but expressly allows compensatory damages for "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."[2] Unlike the CFAA, which imposes a $5,000 loss threshold for civil claims, CDAFA contains no comparable minimum.

Despite the overlap in purpose between the CFAA and CDAFA, courts have recognized important differences between the two statutes. Notably, in *United States v. Christensen*, the Ninth Circuit explained that the CFAA criminalizes unauthorized access to data, while CDAFA criminalizes the unauthorized *taking or use* of data. 828 F.3d 763, 789 (9th Cir. 2015). In other words, CFAA focuses on whether permission was given for any access, whereas CDAFA focuses on knowing access (whether authorized or not) that *becomes unlawful* as a result of taking or using data without authorization. An example of the former is someone logging into another person's computer using a password they stole. Even if no data was taken or used, such access could lead to CFAA liability. An example of the latter is a website owner knowingly obtaining access to a user's geolocation data that the user permitted them to access, but then sharing that data with third parties without permission. Even though the collection was permissible, the distribution was not, potentially leading to CDAFA liability.

Under CDAFA, "access," broadly speaking, means gaining entry to, causing input to or output from, or communicating with a computer system or network.[3] The fact that a third-party technology was the one that actually collected the data does not mean that the website where the collection occurred cannot be held liable. If the website owner caused a third-party application to output user data, that constitutes knowing access and use.

In the recent wave of CDAFA tracking technology litigation, plaintiffs are asserting that defendants violate CDAFA by placing third-party tracking technologies on their websites, which obtain

[1] Cal. Pen. Code § 502(e)(1).
[2] *Id.*
[3] Cal. Pen. Code § 502(b)(1).

information about website users without their consent. Because plaintiffs have not consented to the collection or use of their data by these third parties, plaintiffs claim this is the type of unauthorized taking or use that CDAFA makes unlawful.

The "Without Authorization" Requirement

To state a CDAFA claim, plaintiffs must plead that the defendant "either acted without authorization or exceeded its authorization."[4] To have "authorization" means to be "specially recognized or admitted" to have access to that data.[5]

Historically, courts have interpreted acting "without permission" under CDAFA to require that the defendant accessed a computer, network, or website in a manner that overcame technical or code-based barriers.[6] Under this interpretation, a website does not act "without permission" merely by sharing information about users with third parties where no technical barriers prevented the website or third-party tracking technology from accessing that information.[7]

After *Christensen*, however, some courts have taken a broader approach, holding that overcoming technical or code-based barriers is sufficient to show that someone acted without permission, but not necessary.[8]

These recent interpretations make it easier for CDAFA claims to survive the pleading stage and have led to a growing number of CDAFA suits because there is no need to show a plausible circumvention of a technical barrier; a plaintiff must simply allege that data was plausibly taken or used without permission.

Consent

As with other privacy statutes, consent of the user to the data collection is an important consideration. Some courts have applied the defense narrowly in the CDAFA context. To rely on the consent defense, these courts have held that the website must "explicitly notify users of the practice at issue."[9] Accordingly, consent has been limited to the *specific disclosures* provided, which courts have held should have only one plausible interpretation. In other words, if the disclosure "does not specifically and unambiguously inform the user of the data collection practices," the consent defense may fail.[10]

At the same time, some courts have found general consent to be viable, recognizing the limits on how far CDAFA can be stretched. Under this reasoning, website owners do not have a duty "to disclose how permissions will be exercised," especially in light of the Supreme Court's decision in *Van Buren v. United States*, 593 U.S. 374 (2021), where the Court clarified that the CFAA does not attach to authorized uses of computer databases even when a defendant had "obtained information from the database for an improper purpose."[11] Since CFAA authorization is a "gates-up-or-down inquiry," meaning that "one either can or cannot access a computer,"[12] companies can argue that by extension, under CDAFA, if a plaintiff has given a website permission to collect their data, they cannot then argue that the subsequent use of that data for particular purposes exceeds the authorization originally granted.[13]

Ownership Interest

CDAFA also requires the plaintiff to have the required ownership or possessory interest in the computer or data at issue.[14] "[O]wnership is often linked to the entity who created the property at issue. For instance,

[4] *Wendover Prods., LLC v. Paypal Inc.*, 2025 WL 3251667, at *4 (N.D. Cal. Nov. 21, 2025).
[5] *See hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195–96 (9th Cir. 2022).
[6] *See, e.g., In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014); *Sunbelt Rentals, Inc. v. Victor*, 2014 WL 4274313 (N.D. Cal. Aug. 28, 2014).
[7] *See In re Facebook Priv. Litig.*, 791 F. Supp. 2d at 715.
[8] *See, e.g., Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1049 (S.D. Cal. 2023); *Esparza v. Kohl's Inc.*, 723 F. Supp. 3d 934, 945 (S.D. Cal. 2024).
[9] *Greenley*, 684 F. Supp. 3d at 1048 (citing *Brown v. Google LLC*, 525 F. Supp. 3d 1024, 1063).
[10] *Id.*
[11] *Wendover Prods. LLC v. Paypal Inc.*, 2025 WL 3251667, at *5 (N.D. Cal. Nov. 21, 2025) (citing *Van Buren*, 593 U.S. at 396).
[12] *Van Buren*, 593 U.S. at 390.
[13] Wendover Prods. LLC, 2025 WL 3251667, at *5 (plaintiffs admit "that PayPal uses the very same permissions it was granted to carry out the challenged conduct"—since neither CFAA nor CDAFA impose any duty "to disclose how permissions will be exercised," plaintiffs fail to demonstrate PayPal has acted without authorization).
[14] Cal. Penal Code § 502(e)(1).

where a plaintiff drafts emails or technical documents that are stored in a third-party's servers and then accessed by a defendant without authorization, a CDAFA claim is cognizable because the plaintiff author retains some ownership interest in the data at issue."[15]

That ownership theory becomes more difficult where the plaintiff asserts an interest in data collected or generated by someone else. As one court explained, "where a plaintiff's personal data (e.g., financial information, health data) is collected or generated by a third-party, and stored by a third-party, the plaintiff may retain some form of interest—for example, a privacy interest, but cannot necessarily claim an ownership interest in that data under the CDAFA."[16] So, under this theory, website owners that collect and store third-party information can argue that any plaintiffs suing under CDAFA do not have the type of ownership interest in such data that permits recovery under the statute.

Damage or Loss

Courts have also dismissed CDAFA claims where the alleged website tracking does not amount to the kind of access or use that CDAFA prohibits, meaning plaintiffs suffered no cognizable damage or loss. For example, courts may find that the installation of web tracking technologies on a website does not equate to trackers being installed on a user's own device or that the alleged data collection occurred on the user's own device rather than on the website the plaintiff was browsing (thus defeating any claim that there was unauthorized access of the plaintiff's computer).[17]

Plaintiffs have tried to frame their injury as the loss of the ability to control their data, the loss of the value of their data because it has been disseminated to third parties, and the loss of the ability to protect their data. Courts have rejected these damages theories, finding that damages or loss under CDAFA should be understood as damages to the underlying computer system or data on that computer, rather than the data that a plaintiff generates when on a defendant's website.[18] Plaintiffs have had some success by alleging that the company unjustly profited from the use of their data by selling it to third parties or using it for targeted advertising.[19] That said, other courts have rejected this theory as well, explaining that disgorgement could be viable if plaintiffs alleged an intent to personally sell their data, but that such an allegation would contradict related invasion of privacy claims that are often asserted in conjunction with CDAFA.[20]

Takeaways

CDAFA claims are likely to become a more common companion to CIPA and pen-register theories in website tracking litigation. Plaintiffs will try to frame pixels, cookies, session-replay tools, and other commonplace tracking technologies as code that knowingly accesses their data and takes or uses it without authorization. They will assert that they have suffered damages either because the value of their data has been diminished, they lost control of their data, or the defendant has been unjustly enriched by accessing and profiting from their data.

As these new privacy liability theories play out, businesses should be proactive about protecting themselves from becoming the target of one of these lawsuits. Consent remains important: companies should use clear and specific consent banners, avoid placing non-essential cookies and tracking technologies before authorization, and ensure that their privacy policies and related disclosures accurately describe the technologies in use and the types of tracking occurring. If sued, businesses should consider whether the plaintiff consented to the collection or use of their data, the alleged tracking actually accessed the plaintiff's computer, the plaintiff maintained the required ownership interest in the data, and the alleged injury is a cognizable damage or loss under CDAFA.

[15] *In re Cap. One Fin. Corp.*, 2025 WL 1570973, at *14 (E.D. Va. June 2, 2025).
[16] *Id.* (cleaned up).
[17] *See, e.g., Allison v. PHH Mortg.*, 2026 WL 899438, at *7 (N.D. Cal. Mar. 27, 2026).
[18] *See, e.g., Doe v. Cnty. of Santa Clara*, 2024 WL 3346257, at *9 (N.D. Cal. July 8, 2024); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1082 (N.D. Cal. 2023); *Cottle v. Plaid Inc.*, 536 F. Supp. 3d at 461, 487-88 (N.D. Cal. 2021).
[19] *See, e.g., Tsering v. Meta Platforms, Inc.*, 2026 WL 89320, at *5 (N.D. Cal. Jan. 12, 2026) (citing *Smith v. Rack Room Shoes, Inc.*, 2025 WL 2210002, at *3 (N.D. Cal. Aug. 4, 2025)).
[20] *See, e.g., Dellasala et al. v. Samba TV, Inc.*, 2026 WL 1138358, at *8-9 (N.D. Cal. Apr. 21, 2026); *Doe v. Tenet Healthcare Corp.*, 789 F. Supp. 3d 814, 844-45 (E.D. Cal. 2025).

BIPA Damages Limitation Applies Retroactively

The Seventh Circuit recently confirmed that the 2024 amendment to the Illinois Biometric Information Privacy Act ("BIPA") applies retroactively, effectively limiting the available statutory damages under the statute. Going forward, damages awards under sections 15(b) or 15(d) will be limited for each plaintiff to "at most, one recovery" regardless of the number of violations, avoiding what at least one defendant described as "potentially crippling financial liability" for even simple BIPA violations.

BIPA Overview

BIPA prohibits companies from collecting, obtaining, or disclosing an individual's biometric data, including biometric identifiers (e.g., eye or fingerprint scans, voice prints, face geometry, etc.) or biometric information (i.e., data derived from a biometric identifier) without first providing notice to and obtaining consent from the individual. Subsection 15(b) governs collection of biometric data and subsection 15(d) governs its disclosure. Plaintiffs could recover $1,000 for a negligent violation, or $5,000 for an intentional or reckless violation of the statute. Importantly, however, the law as originally written did not specify how to calculate damages or whether plaintiffs could recover for each time a company collected, obtained, or disclosed the biometric data. For example, BIPA was silent as to whether a plaintiff who clocked in using a fingerprint scanner twice a day for 30 days without providing consent could recover just once, up to $5,000, or for sixty separate violations, as much as $300,000. Plaintiffs have used this ambiguity to extract large settlements from companies.

In 2023, the Illinois Supreme Court confirmed that damages should be awarded on a "per-scan" basis.[1] In other words, each time a company collected, obtained, or disclosed an individual's biometric data without consent, it could be liable for statutory damages. The Illinois Supreme Court also wrote, in dicta, that to the extent the decision would result in "excessive damage awards," the Illinois legislature could amend the law.

The Illinois General Assembly took up the Supreme Court's offer in 2024, amending the damages section of BIPA to clarify that each person could recover for "one recovery" under subsections (b) and (d) so long as the company used "the same method of collection" for each.[2] The legislature also confirmed the discretionary nature of any damages award by noting that an individual is entitled to "at most," recovery based on a single violation.[3]

Retroactive Application of Amendment

After *Cothron*, the question remained as to whether the amendment would have retroactive effect. The Seventh Circuit recently held in the affirmative, that the damages cap would have retroactive effect.[4] The Seventh Circuit analyzed whether the amendment was substantive or procedural. Only procedural amendments could be retroactive under Illinois law.

The BIPA amendment was procedural because it involved the "rules that prescribe[d] the steps for having a right or duty judicially enforced."[5] The text of the amendment and the Illinois Supreme Court's discussion of Section 20 in *Cothron* indicated that it addressed the availability of damages, not proscribed conduct. Additionally, the amendment exclusively was contained in the damages section of BIPA, not in the liability section. Each of these points demonstrated that the amendment was remedial and therefore procedural, so it could have retroactive effect.

[1] *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 927 (Ill. 2023).

[2] 740 ILCS 14/20(b), (c).
[3] *Id.*
[4] *Clay v. Union Pacific Railroad Co.*, 2026 WL 891902 (7th Cir. Apr. 1, 2026).
[5] *Id.* at *3.

The appellees argued that the panel's interpretation would wipe away millions of dollars of liability, and also that whether someone has been injured once or a thousand times is a matter of substance,[6] but the Court was not persuaded and pointed to language in *Cothron* noting that damages were discretionary, so plaintiffs were not guaranteed any specific recovery in the first place.[7]

Key Takeaways

- Going forward, there will be upper limits on the amount of damages available to plaintiffs. Each plaintiff can seek up to $5,000 for violations of BIPA sections (b) or (d). No longer can a plaintiff seek damages for every BIPA violation over the course of multiple years, which may lower a company's exposure exponentially.
- Courts still have discretion over the amount of damages, up to the statutory maximum, or even whether to award damages at all.
- Businesses that collect biometric data should continue to maintain a privacy policy that discloses the specific data collected and collect data only from those consumers who expressly consent.
- The Texas biometric privacy law allows the Texas Attorney General to levy fines based on each individual violation, now putting that law at odds with BIPA. The Texas law does not have a private right of action.

---

[6] *Id.* at *4.
[7] *Id.* at *6.

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), and Phillip Wiese, a Certified Information Privacy Professional/United States (CIPP/US), 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

Leeza Arbatman

Associate
San Francisco

Contact
415.293.6449
larbatman@coblentzlaw.com

Katherine Gianelli

Associate
San Francisco

Contact
415.268.0594
kgianelli@coblentzlaw.com

Saachi S. Gorinstein

Associate
San Francisco

Contact
415.268.0515
sgorinstein@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com