

2026 SUMMER PRIVACY WEBINAR

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



Scott C. Hall
Partner



Phillip Wiese
Special Counsel



Leeza Arbatman
Associate



Kat Gianelli
Associate



Saachi Gorinstein
Associate

Agenda

01

Regulatory Enforcement Actions

02

Navigating the Shifting AI Landscape

03

Risk Assessments

04

California Data Broker Requirements in
2026

05

California Age-Appropriate Design Code Act

06

Wiretap Litigation Update

07

Beyond CIPA: CDAFA Litigation

08

Illinois Biometric Privacy Act (BIPA)

09

Q&A

Regulatory Enforcement Actions

Regulatory Enforcement Actions

Date	Company	Agency	Fine/Payment	Key Issues
5/8/2026	General Motors	Cal. AG	\$12.76M	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	CalPrivacy	\$375,000	Friction in Opt-Out Requests
2/11/2026	Disney	Cal. AG	\$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	Cal. AG	\$1.4M	Methods of Opt-Out Requests Protection of Children's Data
10/30/2025	Sling TV / Dish	Cal. AG	\$530,000	Honoring Opt-Out Requests Protection of Children's Data

Regulatory Enforcement Actions

General Motors

- Joint action between AG, local District Attorneys, and CalPrivacy
- Personal and sensitive personal information collected through OnStar and sold to data brokers

Key Issues ⚠️

- Failure to minimize data
- Purpose limitation
- Sale to data brokers



- **California Attorney General**
- **May 2026**
- **Penalty: \$12.75M**
- **Largest CCPA penalty to date**

Regulatory Enforcement Actions

PlayOn Sports

- Media company sold digital tickets to high school events—concerts, dances, sporting events
- Students were required to agree to tracking technology to access tickets

Key Issues ⚠️

- Ability to opt out of data collection
- Protection of student data



- **CalPrivacy**
- **February 2026**
- **Penalty: \$1.1M**

Regulatory Enforcement Actions

Disney

- Disney had opt-out controls for users, but controls did not work across all devices and all streaming services associated with customer accounts

Key Issues ⚠️

- Honoring opt-out requests across platforms



- **California Attorney General**
- **February 2026**
- **Penalty: \$2.75M**

Regulatory Enforcement Actions

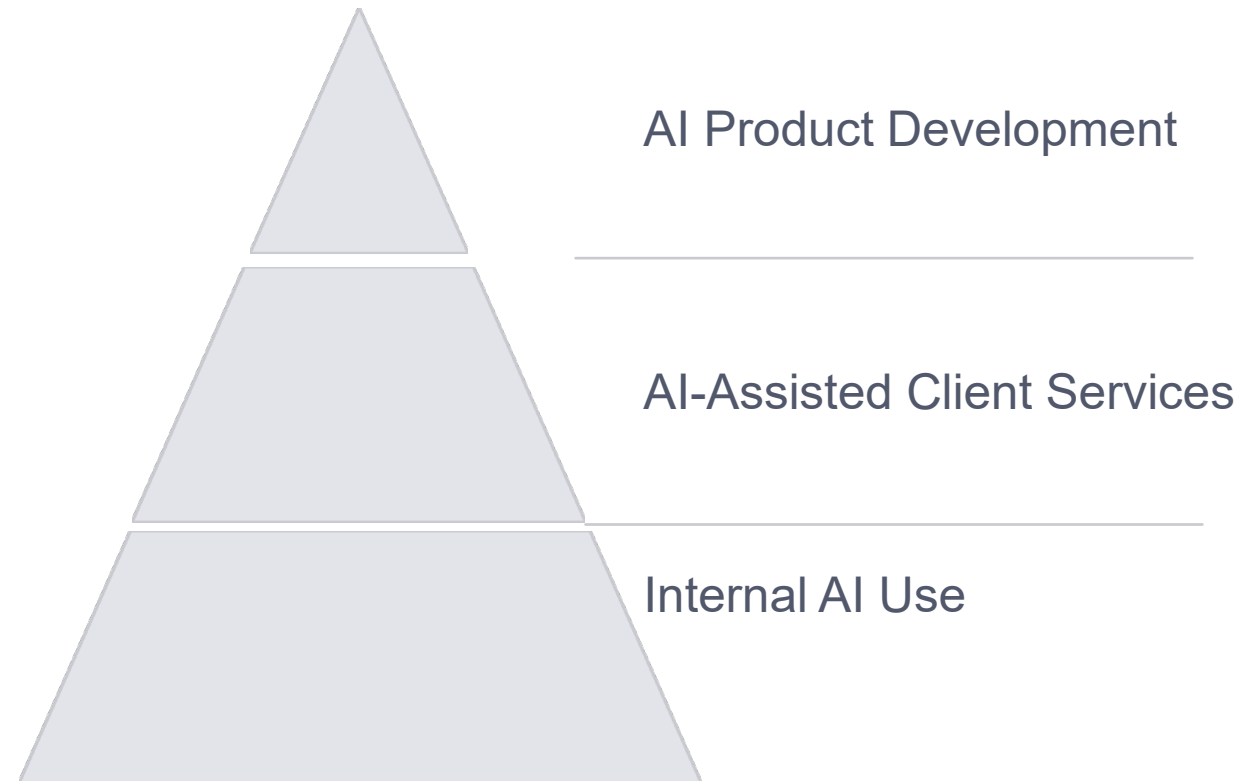
Date	Company	Agency	Fine/Payment	Key Issues
5/8/2026	General Motors	Cal. AG	\$12.76M	Data Minimization Sale of Information to Data Brokers
2/27/2026	PlayOn Sports	CalPrivacy	\$1.1M	Ability to Opt-Out of Data Collection Protection of Children's /Students' Data
2/27/2026	Ford	CalPrivacy	\$375,000	Friction in Opt-Out Requests
2/11/2026	Disney	Cal. AG	\$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	Cal. AG	\$1.4M	Methods of Opt-Out Requests Protection of Children's Data
10/30/2025	Sling TV / Dish	Cal. AG	\$530,000	Honoring Opt-Out Requests Protection of Children's Data

Navigating the Shifting AI Landscape

Navigating the Shifting AI Landscape

- Federal Uncertainty
- California Privacy + ADMT Rules
- Business Risk Tiers
 - Internal Use
 - AI-Assisted Client Services
 - AI Product Development
- State AI Patchwork

Business Risk Tiers



Navigating the Shifting AI Landscape

Compliance Steps for Businesses

Inventory AI uses and vendors

Add human review for high-impact uses

Classify by risk: internal, deliverables, product

Update required notices/disclosures, contracts, and internal policies

Assess privacy, bias, IP, and security risks

Monitor state-law developments

Risk Assessments

Background

- Under the GDPR, businesses needed to conduct Data Privacy Impact Assessments
- CA is moving toward a similar practice under the CCPA regulations from 2025
- Shift from a best practice to a formal, enforceable requirement

What is it?

High Risk Processing

Documentation to assess any "high risk processing"

Weighing the Benefits

Weigh the benefits of the processing (businesses and consumers) against foreseeable risk to individual privacy

High Risk Processing



Selling/sharing data



Collecting sensitive personal information



Automated Decision-Making Technology



Systematic profiling



Large-scale processing

What Should the Assessment Include?

- Purpose of processing
- Categories of personal information involved
- Safeguards
- Operational details of processing

Who Should Conduct the Assessment?



Internal Team

Business Employees

Business employees whose job duties include participating in the processing of personal information subject to a risk assessment

Timeline

Jan 1, 2026

Assessments begin;
prepare by end of 2027,
reports filed starting
April 1, 2028

Before New Processing

A risk assessment must
be completed before any
new processing that
presents a significant risk

Within 45 Days

Must be updated within
45 days if there is a
material change to
processing

Every 3 Years

At a minimum, updated
every 3 years

Impact

- Legal and privacy teams need to develop standardized frameworks and documentation processes
- Business, engineering, and data teams will need to integrate risk analysis into development lifecycles

California Data Broker Requirements in 2026

California Data Broker Requirements in 2026

Threshold status questions for businesses that compile, license, or monetize data

Data Broker Definition

- Collects and sells personal information
- About consumers
- No direct relationship with those consumers
- Publicly available data requires a fact-specific review

Important Nuance

Public-record sourcing is not a blanket exemption.

- Aggregation, enhancement, and licensing practices can change the analysis
- "Direct relationship" requires intentional interaction with the business's own products or services

Data Broker Compliance Timeline

DROP creates a new operational compliance layer

Key Dates

Date	Requirement
January 31	Annual registration with CalPrivacy
January 1	DROP account requirement begins
August 1	Access DROP at least every 45 days and process verified deletion requests
July 1	Publish consumer request metrics in privacy policy
January 1, 2028	Independent third-party audits begin every three years

DROP changes the request process, not the scope of what must be deleted under the CCPA.

Data Broker Enforcement Risk and Takeaways

Active enforcement makes early assessment important

2026 shifts the regime from registration-focused to operational compliance.

\$200/day

Per registration failure or unfulfilled deletion request

Enforcement Risk

- \$200 per day for registration failures
- \$200 per day per unfulfilled deletion request
- Unpaid fees and enforcement costs may apply
- Additional civil penalties may be available

Practical Takeaways

- Assess public vs. non-public data
- Evaluate direct relationships
- Prepare DROP workflows
- Update privacy disclosures and metrics processes

California Age-Appropriate Design Code Act

California Age-Appropriate Design Code Act

Portions of CAADCA are now in effect

Scope

- Applies to online services, products, or features likely to be accessed by children
- "Child" means under 18
- Litigation remains ongoing

Currently Effective Obligations

- Estimate age or apply high privacy protections to all users
- Highest privacy settings by default for children
- Age-appropriate privacy language
- Parental monitoring signals where applicable
- Tools to exercise privacy rights
- Limit use of age-estimation data
- Restrict default precise geolocation processing

Children's Privacy Comparison: CAADCA, CCPA, and COPPA

Overlap exists, but the compliance models are different

Issue	CAADCA	CCPA	COPPA
Covered age	Under 18	Under 13 and under 16 for certain obligations	Under 13
Main focus	Child-centered product design and privacy defaults	Consumer privacy rights and sale/share limits	Parental consent for children's online data
Trigger	Online services likely to be accessed by children	Businesses subject to CCPA thresholds	Online services directed to children or knowingly collecting from children
Key obligations	High privacy settings, age-appropriate notices, age estimation, geolocation limits	Notice, access, deletion, correction, opt-out, limits on sale/share of children's data	Notice to parents, verifiable parental consent, data minimization, parental access/deletion rights
Practical impact	Design and default-setting review	Broader privacy compliance framework	Child-specific federal consent framework

Wiretap Litigation Update

Privacy Litigation Landscape in 2026



Statutes

CIPA
VPPA
ECPA



Technologies

Pixels
Session Replay
Cookies
Embedded analytics



Sectors

Healthcare
Financial services

Supreme Court Grants Cert in VPPA Case

Salazar v. Paramount Global

- SCOTUS to resolve circuit split over the definition of "consumer"
- Sixth Circuit: If not subscriber to audiovisual content, not a consumer
- Second Circuit: Newsletter subscription sufficient for subscriber status
- If Sixth Circuit definition adopted, could curtail VPPA litigation

Popa v. Microsoft – A developing split

Popa v. Microsoft (9th Cir. 2025)

Bare statutory violation of wiretap statute does not automatically confer standing; concrete injury required

District courts split on how to apply *Popa*

- Broad application – dismissed claims involving routine data collection
- Narrow application – standing where sensitive information collected or "cradle to grave" collection

Pen Register Developments

Growing divide over what constitutes a pen register

Federal courts

- Interpreting statute broadly to encompass evolving privacy threats
- Statute contains no explicit limitation to telephonic comms

State courts

- Relying on statutory language and legislative history
- Limiting application to telephonic comms

Beyond CIPA: CDAFA Litigation

Computer Data Access and Fraud Act (CDAFA)

- CA analogue to federal Computer Fraud and Abuse Act (CFAA)
- New wave of litigation based on the use of third-party tracking tech

Important differences between state and fed statutes

CFAA

- Unauthorized access to data
- \$5K loss threshold

CDAFA

- Unauthorized taking or use of data
- No minimum loss threshold (easier to bring suit)

CDAFA: Key Defenses



Consent

Explicit notification vs. broader permissions



Ownership

Third party collection/storage – potentially no ownership interest



Damages

- Theories based on loss of control/diminished value generally rejected
- Must mean harm to underlying computer system or data

Illinois Biometric Privacy Act (BIPA)

Illinois Biometric Privacy Act (BIPA)

Clay v. Union Pacific Railroad, 2026 WL 891902 (7th Cir. Apr. 1, 2026)

Question

Whether the 2024 BIPA amendment limiting damages to one recovery per violation applies retroactively.

Holding

Yes. The amendment was procedural because it did not prohibit any activity, it only limited the recovery for already prohibited activity.

Court's Reasoning

The court was not persuaded by the plaintiff's claims that he could not recover millions of dollars in damages.

Illinois Biometric Privacy Act (BIPA)

4

Key Takeaways

Damages Cap

Upper limits on available damages.

Judicial Discretion

Courts retain discretion over the amount of damages.

Texas vs. BIPA

BIPA is at odds with Texas biometric privacy law.

Consent & Disclosure

Continue to disclose specific biometric data collected and obtain express consent.

Q&A

Questions and Discussion

Open Floor for Questions

Thank you for Attending

Please direct any questions to Scott Hall and our privacy team.



Scott C. Hall

Partner

shall@coblenzlaw.com



Phillip Wiese

Special Counsel

pwiese@coblenzlaw.com



Leeza Arbatman

Associate

larbatman@coblenzlaw.com



Kat Gianelli

Associate

kgianelli@coblenzlaw.com



Saachi Gorinstein

Associate

sgorinstein@coblenzlaw.com