

## Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.



# Navigating Changes to the California Consumer Privacy Act (CCPA): What You Need to Know

Kathleen McConnell  
Yana Komsitsky  
Vincent Smolczynski  
Danny Riley

April 23, 2026

**Seyfarth Shaw LLP**

"Seyfarth" refers to Seyfarth Shaw LLP (an Illinois limited liability partnership).

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

# Speakers

---



***Kathleen McConnell***  
***Partner***  
**San Francisco**



***Yana Komsitsky***  
***Senior Counsel***  
**Los Angeles**



***Vincent Smolczynski***  
***Counsel***  
**Charlotte**



***Danny Riley***  
***Associate***  
**Chicago**



## Agenda

- 1 | Compliance Timeline & General Updates
- 2 | Automated Decision-Making Technology ("ADMT")
- 3 | Risk Assessments
- 4 | Cybersecurity Audit Requirements
- 5 | CCPA and CIPA Consent Management Updates
- 6 | Preparing Your Business for the Future

# Compliance Timeline

## 2025

- **Preparation**

- Identify processing activities and tools that may trigger Risk Assessment or ADMT obligations.
- Begin drafting Pre-use Notices for ADMT if applicable.
- Map data flows and sensitive PI for risk assessment readiness.

## 2026

- **General Updates in Effect**
- **Risk Assessment (RA) Implementation**
  - Begin conducting RAs before starting new processing activities.
  - Implement processes for ongoing RA updates and documentation.
  - Begin internal planning for cybersecurity audit requirements.

## 2027

- **ADMT Enforcement**

- Comply with ADMT regulations: Pre-use Notices, opt-out rights, and access rights.
- Complete Risk Assessments for preexisting processing by **Dec 31, 2027**.
- Prepare for first cybersecurity audit if revenue > \$100M.

## 2028 and Beyond

- **Ongoing Compliance**

- Submit Risk Assessment summary to CPPA by **April 1, 2028**.
- Businesses > \$100M revenue: complete first cybersecurity audit by **April 1, 2028**.
- Continue annual certifications and audits per tiered schedule.

# General Updates



**General Updates:  
Effective 2026**

- **Privacy Policies**
  - *Disclosures to Service Providers & Contractors*
- **Access Requests**
  - *Date range for request*
- **Mobile Apps**
  - *Link to privacy policy required*
- **Financial Incentives**
  - *Symmetry required; may not default to opt in*
- **Connected Devices Opt-Out Timing**
  - *Same manner as collection; before or at collection*

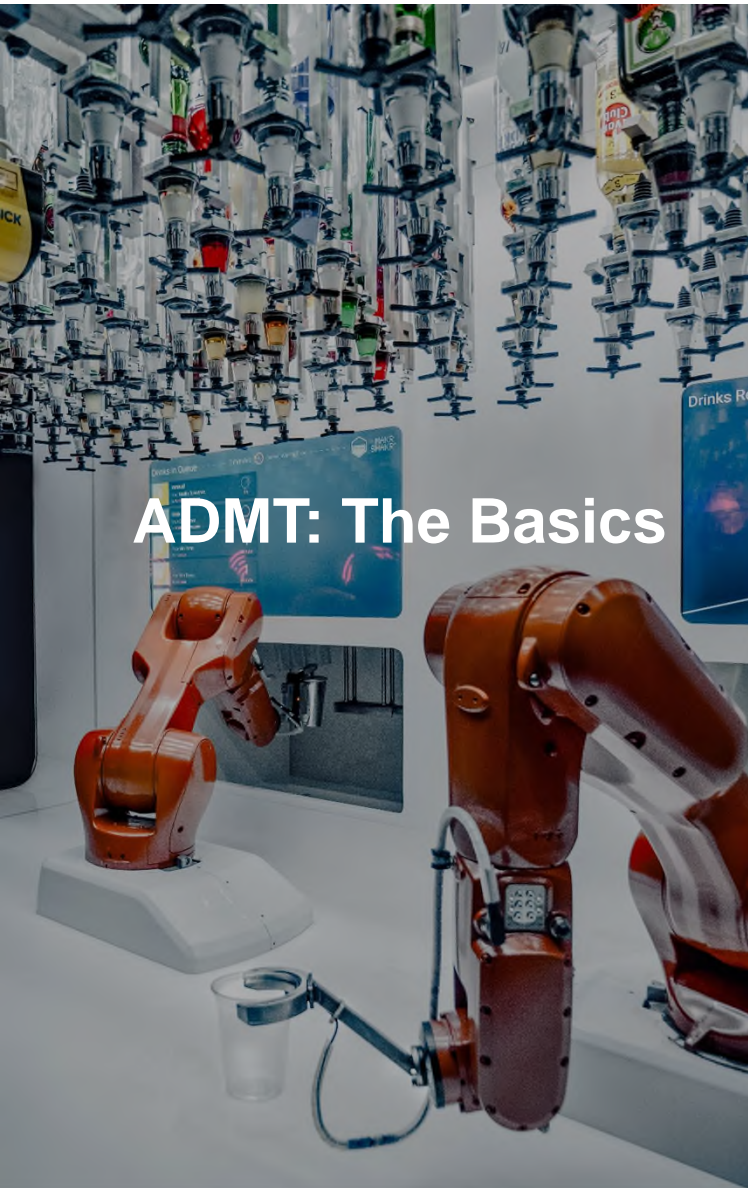


**General Updates:  
Effective 2026**

- **Sensitive Data Defined**
  - *Neural data; actual knowledge under 16; content of messages unless intended recipient*
- **Insurance Companies**
  - *Partial exemption limited to data governed by insurance code*
- **Opt-Out Confirmation; GPC Signals; Consent Management**
  - *Confirmation of opt-out; symmetry required; x-out not sufficient for consent (see Section 5, below)*



# Automated Decision-Making Technology (“ADMT”)



## What is ADMT?

ADMT refers to any technology that processes personal information (“PI”) and uses computation to substantially replace human decision-making.

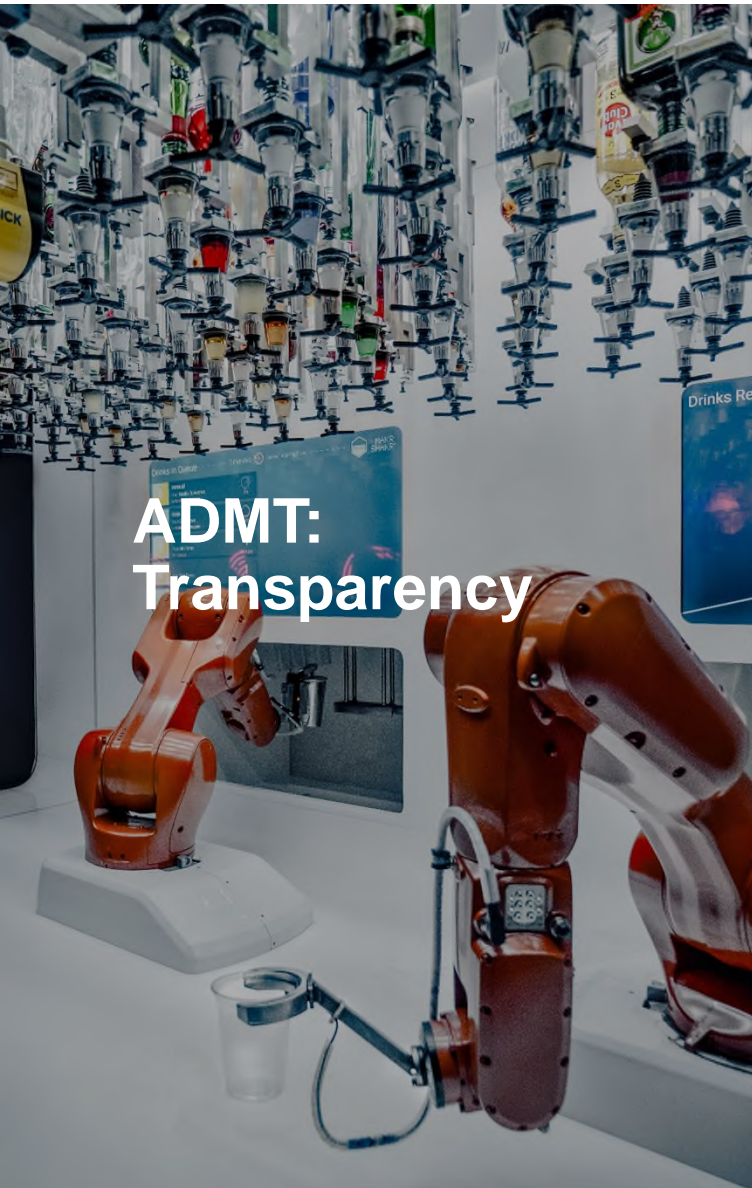
- To “substantially replace human decision-making” is to use a technological output to make a decision without human involvement.

## When is the Use of ADMT Covered by the Regulations?

When ADMT is used to make significant decisions concerning a consumer.

- A “significant decision” is a decision that results in the provision or denial of various services or opportunities including employment, insurance, housing, education, and financial services.

These regulations will be enforced beginning January 1, 2027.



## Pre-Use Notice Requirement

Businesses must give consumer a clear notice before using ADMT to make significant decisions about them.

A Pre-Use Notice must:

- Explain **why** the business is using ADMT.
- Describe **how** the ADMT will affect the consumer.
- Be easy to find, readable, and understandable.
- Be provided before the consumer interacts with the ADMT system.
- Inform the consumer of their right to opt-out.

Businesses may use a consolidated notice if multiple ADMT tools serve similar purposes.



## Consumer's Right to Access ADMT

Consumers have the right to understand how ADMT was used to make a decision about them.

- When a consumer submits an access request, businesses must provide:
  - The specific purpose for which ADMT was used.
  - How the ADMT processed the consumer's PI.
  - The ADMT's output and how it was used to make a significant decision regarding the consumer.
  - That the business is prohibited from retaliating against the consumer for exercising this right.



## Consumer's Right to Opt-Out of ADMT

Consumers may choose not to have ADMT used to make significant decisions about them.

Businesses must:

- Clearly inform consumers of this right in the Pre-Use Notice.
- Offer **two or more** easy-to-use opt-out methods.
- Make the opt-out process simple, accessible, and aligned with how the business interacts with consumers.
- Honor the opt-out quickly and notify any service providers who also use the ADMT system.



## Exceptions to the Opt-Out Consumer Right

In certain situations, businesses **do not** need to offer an opt-out:


- When consumers can appeal the ADMT decision to a qualified human reviewer.
- When ADMT is used for admission, acceptance, or hiring decisions.
- When ADMT is used to assign work or determine compensation.

Even when an opt-out isn't required, other ADMT obligations still apply, including Pre-Use Notices, access rights, anti-retaliation rules, and Risk Assessment requirements.



## How Should Businesses Prepare?

- **Identify ADMT Uses:** Map tools that automate or influence significant decisions.
- **Prepare ADMT Notices:** Draft Pre-Use Notices explaining each ADMT use and its impact.
- **Update DSAR Processes:** Incorporate ADMT access requests and response workflows.
- **Review Vendor Tools:** Confirm whether third-party AI tools function as ADMT and revise contracts accordingly.
- **Strengthen Governance:** Integrate ADMT obligations into existing AI and privacy programs.
- **Assess ADMT Risks:** Evaluate ADMT systems through Risk Assessments starting in **2026**.



**Risk Assessment  
Obligation: starts  
January 1, 2026\***



**Risk Assessments:**  
Required if  
processing  
presents  
*significant risk* to  
consumer privacy

## What processing presents a *Significant Risk*?

- **Selling or sharing** Personal Information (PI).
- Processing **Sensitive PI (SPI)**.
  - Except for pay, benefits, work authorization, accommodations, wage reporting.
- Using **ADMT** for a "**significant decision**."
- Using automated processing to **profile**, based on:
  - Systematic observation of an educational/job applicant, student, employee or independent contractor.
  - Presence in a sensitive location.
- Processing PI to **train an ADMT** for a significant decision on a consumer; or to train facial-recognition, emotion-recognition, or other technology that verifies identity or profiles.



## Risk Assessments: Examples

### Example Scenarios in the Regulations

Scenario	Why Assessment Required
A business will use emotion-recognition technology without human involvement to make hiring decisions.	This is ADMT for a significant decision concerning a consumer
A dating app will disclose precise geolocation, ethnicity, and medical info individuals provide in dating profiles to a third-party analytics service provider.	This is SPI processing
A budgeting app will display ads for payday loans on different websites based on evaluation of financial info consumers entered into the app.	This is sharing of PI
A tech company will train its facial recognition technology on consumer photos.	This is using PI to train ADMT



## Risk Assessments: A Balancing of Interests

## What are the Goals of a Risk Assessment?

The goal of a Risk Assessment is to **restrict or prohibit processing** if the *risks* to consumers' privacy outweigh the *benefits* of the processing to the consumer, the business, other stakeholders, and the public.





## Risk Assessments: Content Requirements

### What Must the Report Cover?

- Processing purpose – must not be generic.
  - ✘ : “security purposes” or “service improvement”
  - ✔ : “decreasing wait time when processing rights requests”
- Categories of PI/SPI to be processed.
- Operational requirements to be identified/documentated:
  - Planned method for processing and sources of PI.
  - How long PI will be retained or criteria to be used to determine retention period.
  - Method of interacting with consumers (e.g., websites, apps, offline) and purpose (e.g., to provide services).
  - Approximate number of consumers concerned.
  - What disclosures will be made and how.
  - Names or categories of service providers/third parties and the purposes of disclosure to them.



## Risk Assessments: Content Requirements

### Cont'd: What Must the Report Cover?

- Operational requirements (continued):
  - For **ADMT**: logic, including assumptions or limitations and output and how it will be used to make a significant decision
  - **Benefits** must not be generic, such as “improving service”
  - **Negative impacts to privacy** including sources and causes
    - e.g., unauthorized use, discrimination, impairing control, economic harms, creating opportunity for harm, reputational, psychological
  - Any **safeguards** to be used to address negative impacts
    - e.g., encryption, access controls, network monitoring, experts, training
  - **Decision** on processing – will you do it anyway?
  - Identify the **individuals** who provided the info, except legal counsel
  - Date of review and approval
  - Names/positions of **approvers**
    - Must include individual with authority over processing/the decision



## Risk Assessments: Additional requirements for businesses training ADMT

### If The Business is Training ADMT

- If making ADMT available to another business to make a significant decision concerning a consumer, you must provide to that recipient-business **all facts available** that are necessary for the recipient-business **to conduct its own risk assessment.**



A hand holding a white stylus is writing on a tablet. The tablet screen shows a checklist with several items, some of which are checked. The background is blurred, showing a desk with a keyboard and a plant.

## Risk Assessments: Timing and Frequency Requirements

### When and How Often?

- **Before** new activity with "significant risk."
- Any preexisting activity requires Risk Assessment by **December 31, 2027**.
- Review/update at least **once every 3 years** for accuracy.
- Update whenever there is a **material change** to the processing, as soon as feasibly possible, but no later than **45 calendar days** from the date of the material change.
- **Retention:** RAs must be retained for as long as the processing continues or for 5 years after the Assessment, whichever later.



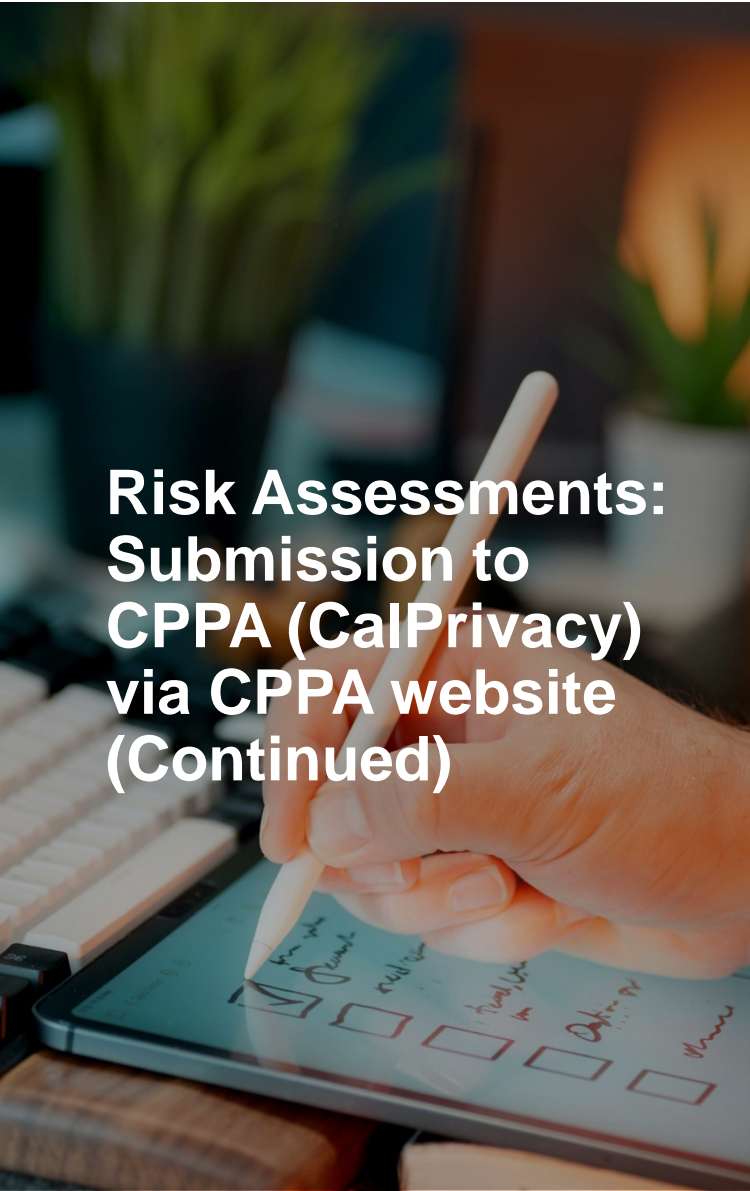
**Risk Assessments:  
Submission to  
CPPA (CalPrivacy)  
via CPPA website**

## Report Submission Requirements

- For Risk Assessments conducted in 2026 and 2027, submit no later than April 1, 2028.
- For Risk Assessments conducted after 2027, submit no later than April 1 in following year. (2028 assessments in 2029, etc.).

Assessment Year	Submission Deadline
2026 - 2027	April 1, 2028
2028 onward	April 1 of the next year

- Time period covered by the Risk Assessment Report
- Number of assessments conducted/updated per activity.
- What categories of PI/SPI were processed by reference to the CCPA categories.



**Risk Assessments:  
Submission to  
CPPA (CalPrivacy)  
via CPPA website  
(Continued)**

## Cont'd: Submission Requirements

- Attestation under penalty of perjury: *“I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). Under penalty of perjury under the laws of the state of California, I hereby declare that the risk assessment information submitted is true and correct.”*
- Name and title of person submitting. This person must be:
  - Member of **executive management team**.
  - **Directly responsible** for risk assessment compliance.
  - Has **sufficient knowledge** to provide accurate information.
  - Has the authority to submit to the CPPA.
- The CPPA or the AG may require a Report at any time (which must then be submitted within 30 calendar days).

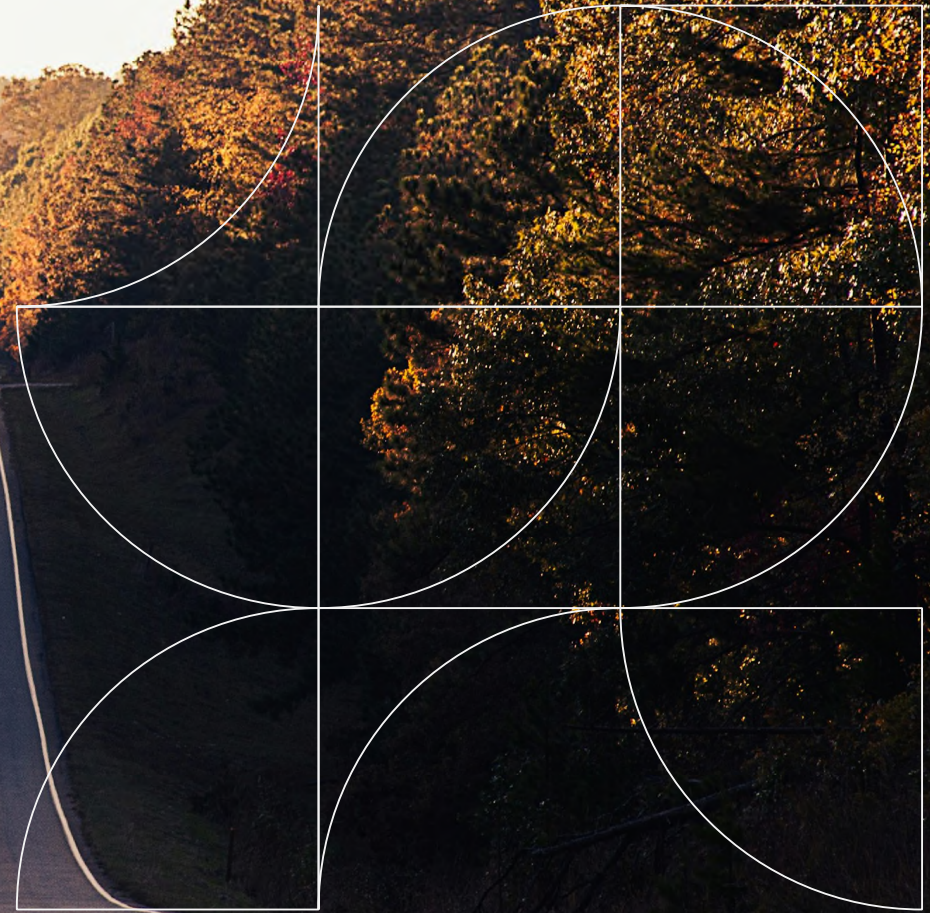


## Risk Assessments: OK to Combine with Comparable Requirements

### It is Possible to Combine Risk Assessments

- **Similar processing activities** that present **similar risks** to consumers' privacy may be addressed in a single Risk Assessment.
  - Ex.: Toy store will collect kids' names, addresses and birthdays, to mail a toy coupon, using the same vendor for several mailings across all stores. The toy store must conduct a RA, because it is processing SPI. It may use a single RA as it is collecting the same PI in the same way for the same purpose and there are similar risks to privacy.
- A Risk Assessment prepared for **another purpose** may be used, provided it meets the requirements.
  - Ex.: A business plans to sell PI and already conducts a Risk Assessment for another law. It can use that Assessment for these purposes, as long as all the CA requirements are met.

# Cybersecurity Audit Requirement





## Cybersecurity Audit: Who

### **Who Needs to Complete a Cybersecurity Audit?**

Every business whose processing of consumer's PI presents a **significant risk** to consumer security.

- A **significant risk** exists when:
  - 50% or more of a business's annual revenue is derived from selling or sharing consumer's PI, or
  - The business's annual gross revenue exceeds \$25 million and
    - The business processed the PI of 250,000 or more consumers, or
    - The business processed the sensitive PI of 50,000 or more consumers.



## Cybersecurity Audit: When

### ***When Does the Audit Need to be Completed?***

The determination of when businesses are required to complete a cybersecurity audit is dependent on revenue and being implemented in a tiered system.

- Businesses with an annual gross revenue for 2026 of more than **\$100 million**, must complete their first cybersecurity audit by **April 1, 2028**.
- Businesses with an annual gross revenue for 2027 **between \$50 million and \$100 million**, must complete their first cybersecurity audit by **April 1, 2029**.
- Businesses with an annual gross revenue for 2028 **less than \$50 million**, must complete their first cybersecurity audit by **April 1, 2030**.

Following April 1, 2030, if a business meets the criteria requiring it to complete an audit (previous slide), the business must complete an audit covering the next 12 months by April 1 of the following year.



## Cybersecurity Audit: What

### ***What Needs to be Included in the Audit?***

- Details of the business's cybersecurity program.
- An assessment of the business's establishment, implementation, maintenance, and enforcement of its cybersecurity program.
- An assessment of any applicable components as listed in the regulations.
  - Regulations provide eighteen components, most of which have various subsections, and allows the auditor to include additional components if applicable.
    - Example components: authentication; antivirus and antimalware protections; cybersecurity education and training
- Other required reports
  - Regulations provide ten areas the audit must address.
    - Example areas: applicable components assessed; corrections or amendments to prior audits; auditor's information



## Cybersecurity Audit: Auditor Required

### Interactions with Auditor and Auditor Requirements

Every business required to complete an audit must use a qualified, objective, independent professional who uses accepted procedures and standards.

- May be an internal or external auditor, but internal auditors must follow additional regulations.
- The business must:
  - Provide all information within its possession, custody, or control that is requested by the auditor as relevant to the audit; and
  - Act in good-faith to disclose all relevant facts and not misrepresent relevant facts.
- Auditor must rely primarily upon specific, appropriate evidence rather than assertions or attestations by management.
- Audit report must be provided to an applicable employee of the business.
- Business and auditor must retain all documents relevant to audit for a minimum of five years.



## Cybersecurity Audit

### **Certification of Completion**

Each year that a business is required to complete a cybersecurity audit, it must submit a written certification of completion to the Agency no later than April 1.

- Certification must be submitted by an applicable employee of the business who is directly responsible for audit compliance, has sufficient knowledge of the audit, and has authority to submit the certification.
- Certification must be submitted through the Agency's website and include the following:
  - Business's name and point of contact.
  - Statement that the business has completed the audit.
  - The time period covered by the audit.
  - Electronically signed attestation of the form statement.
  - The name and business title of the person submitting the certification, and the date of the certification.




# CCPA and CIPA Consent Management Updates



## Background: CIPA

- Massive increase in lawsuits under the California Invasion of Privacy Act.
  - Any company with a website can be a target.
  - Claims target the operations of cookies, pixels, chatbots, pen registers and tracking software.
  - Liability up to \$5,000 per violation.
- Approximately 3000+ CIPA related cases filed
- Uptick in other similar lawsuits
  - Florida
  - Washington
  - Federal Wiretap Act
  - Electronic Communications Privacy Act
  - Video Privacy Protection Act.



**CCPA Consent  
Management  
Regulation  
Amendments &  
Related / Do Not  
Sell Enforcement  
Activity**

**Opt-Out  
Confirmation  
Display**

- The California Privacy Protection Agency (tasked with enforcing the CCPA along with the California AG's office) has issued only two enforcement advisories to date, one of which addresses consent / cookie management in connection with "dark patterns" (CCPA Enforcement Advisory No. 2024-02).
- 2026 Regulation Amendments are consistent with the enforcement advisory.
- State enforcement agencies are increasingly active.
- September 2025: California, Colorado and Connecticut enforcement authorities announced a joint investigative privacy sweep relating to Do Not Sell / Global Privacy Opt-Out / Consent Management matters.
- 2026 Regs require a means for consumers to confirm opt-out has been processed (including for GPC signals) – *e.g.*, by display on a website of "Opt-Out Request Honored."



## CCPA and Other State Level Data Privacy Laws

- Numerous states with state level privacy laws, including California, Colorado, Connecticut, Delaware, Iowa, Indiana, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia.
- No private right of action under the CCPA/CPRA
  - Enforcement actions may be brought by the California Attorney General or the California Privacy Protection Agency.
  - This may be changing in N.D. Cal.
    - Allison v. PHH Mortgage (N.D. Cal.)
    - Shah v. Capital One Financial Corp. (N.D. Cal.)
    - M.G. v. Therapymatch, Inc. (N.D. Cal.)
- Multiple enforcement actions ranging up to \$1.5 million



## Consent Under the CCPA

- "Dark Patterns" – means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.
- Consent – freely given, specific, informed, and unambiguous.
  - Consent obtained through dark patterns is not "consent."
- How to Avoid:
  - Easy to understand
  - Straightforward
  - No technical or legal jargon
  - Symmetrical Choices for user to say "yes" or "no"
    - Both in difficulty and in time required



## Dark Patterns Guidance

### Examples of Prohibited Dark Patterns

The updated CCPA regulations provide examples of several practices that may constitute prohibited dark patterns, including:

- Requiring more steps to opt-out of the sale or sharing of personal information than to opt-in;
- Making a “yes” button more prominent than a “no” button (e.g., through sizing or color selection);
- Treating the act of closing or navigating away from a pop-up as a valid form of consumer consent without the consumer first affirmatively selecting “I accept” or an equivalent;
- Selecting by default, or featuring more prominently, the option to participate in a financial incentive program than the option not to; and
- Creating a false sense of urgency that pressures consumers into quickly making a decision about the scope of their consent.



## Decisions Regarding Website Tracking Technologies

Courts are becoming savvier... *but there's still confusion...*

- *Popa v. Microsoft Corporation (9<sup>th</sup> Cir)* - pen register – no standing for collection of device and browser-type information
  - “no embarrassing, invasive or otherwise private information”
  - *Khamooshi v. Politicio, LLC (N.D. Cal.)* – follows *Popa* holding
  - *In re USA Today Co. (N.D. Cal.)* - same

*Compare D'Antonio v. CNN, Inc. (S.D.N.Y.)* – IP address, device data sufficiently private data to survive Motion to Dismiss
- *Heiting v. HP, Inc. (Cal. Sup. Ct. 2024)*
  - Dismissed "trap and trace" complaint without leave to amend.
  - Judges aren't buying plaintiffs' attempts to apply CIPA statutory scheme to these technologies.
- *Ramos v. The Gap, Inc. (N.D. Cal 2025)* - dismiss w/o leave
  - Dismissed Sec. 631(a) complaint re: marketing email tracking; Sec. 631(a) does not apply to internet comms. or cover data such as URLs and device information.
- Tester Plaintiffs –professional plaintiffs may lack standing to bring CIPA claim –*i.e.*, lack an expectation of privacy.



## CIPA & Potential Legislative Action

### California Senate Bill 690

- Increasing pressure on the legislature to address the uncertainty and potential exposure relating to CIPA led to the introduction of a bill this past legislative session.
  - “commercial business purposes” exception
  - SB 690 has since stalled out in the California Assembly
- Renewed call for legislative action:
  - *Doe v. Eating Recovery Center*, N.D. Cal (Oct. 17, 2025) – legislature should go back to the drawing board
  - *Palacios v. Fandom, Inc.* (Cal. Sup. Ct. 2025) - district courts would "benefit from appellate guidance."
- Reform CIPA Coalition – California businesses, non-profits, organizations pushing for legislative reform
  - Seeking to avoid the deluge of lawsuits and inconsistency within the Courts



## Practical Considerations

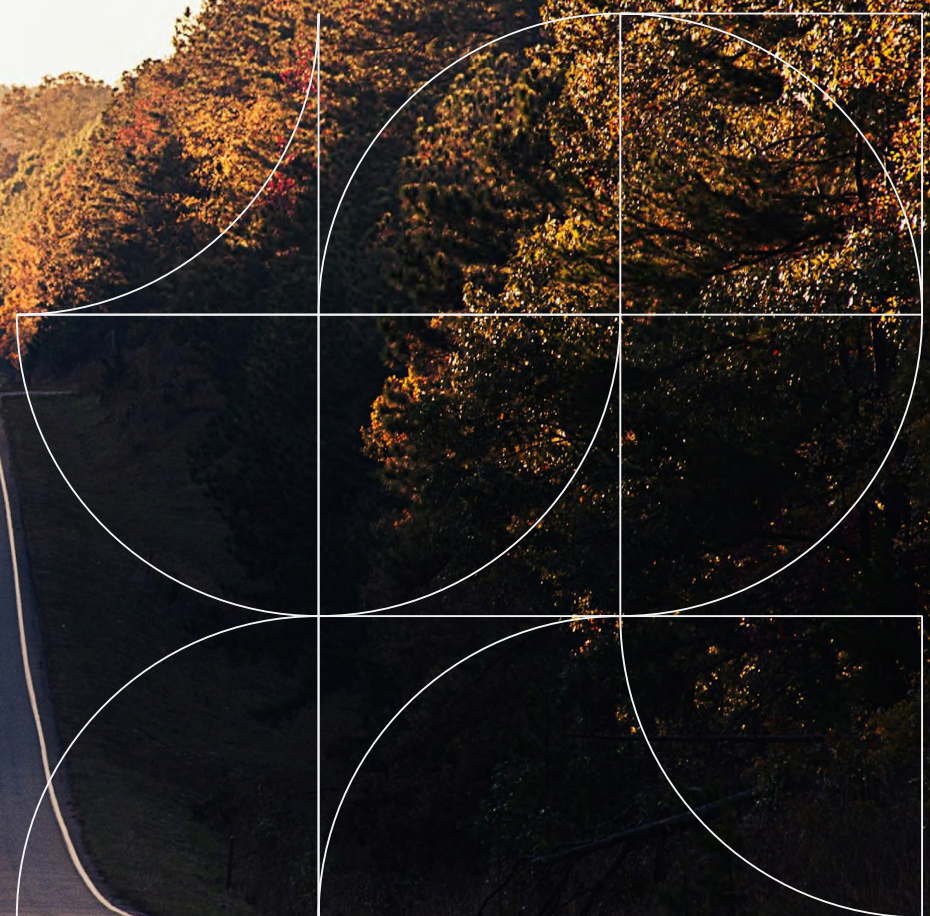
- **Cookie Banner Considerations:**

1. Audit Tracking Technologies – What are you using, what tools do you need, and when does that tool begin collecting data?
2. Evaluate Your Consent Mechanisms
  - a. Do you have one in place?
  - b. Opt-in v. Opt-out – CIPA v. CCPA – largely dependent on your risk tolerance and business objectives
  - c. Avoid “Dark Patterns”
  - d. Fully Functional – ensure cookie management tool is effectuating users’ selections
3. Revise your Privacy Notices – ensure what you disclose accurately describes what you are doing
  - a. Policies are not a one-size-fits-all endeavor

- **Opt-Out Considerations - CCPA**

- Tested; functioning; global (GPC)?

# Preparing Your Business for the Future





## Action Items & Considerations

### **Priority Actions for 2025–2026**

#### **✓ Build a Unified AI & Data Inventory**

- Map all AI, ADMT, profiling, cookies/trackers, and high-risk processing across the organization.

#### **✓ Implement a Global Risk & Governance Framework**

- Stand up processes for AI tool/ADMT reviews, privacy risk assessments, cybersecurity controls, cookie/consent compliance, and shadow-AI management.

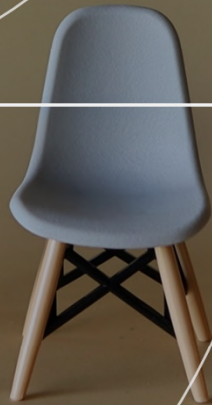
#### **✓ Modernize Notices, Consent & DSAR Workflows**

- Update global privacy notices, cookie banners, ADMT/AI transparency, opt-out rights, and human-review appeal pathways.

#### **✓ Ensure Policies Match Actual System Behavior**

- Validate that AI tools, website cookies/trackers, and DSAR workflows operate exactly as described in notices, banners, and internal policies.

*Questions?*



# *thank you*

**Kathleen McConnell**

Email: [kmccconnell@seyfarth.com](mailto:kmccconnell@seyfarth.com)

Phone: (415) 544-1062

**Yana Komsitsky**

Email: [ykomsitsky@seyfarth.com](mailto:ykomsitsky@seyfarth.com)

Phone: (310) 201-5242

**Vincent Smolczynski**

Email: [vsmolczynski@seyfarth.com](mailto:vsmolczynski@seyfarth.com)

Phone: (704) 925-6043

**Danny Riley**

Email: [driley@seyfarth.com](mailto:driley@seyfarth.com)

Phone: (312) 460-5310

