DENTONS

Navigating California’s Privacy and Tech Landscape

Peter Stockburger
Dentons

Rebecca Hanovice
Mattel

Discussion

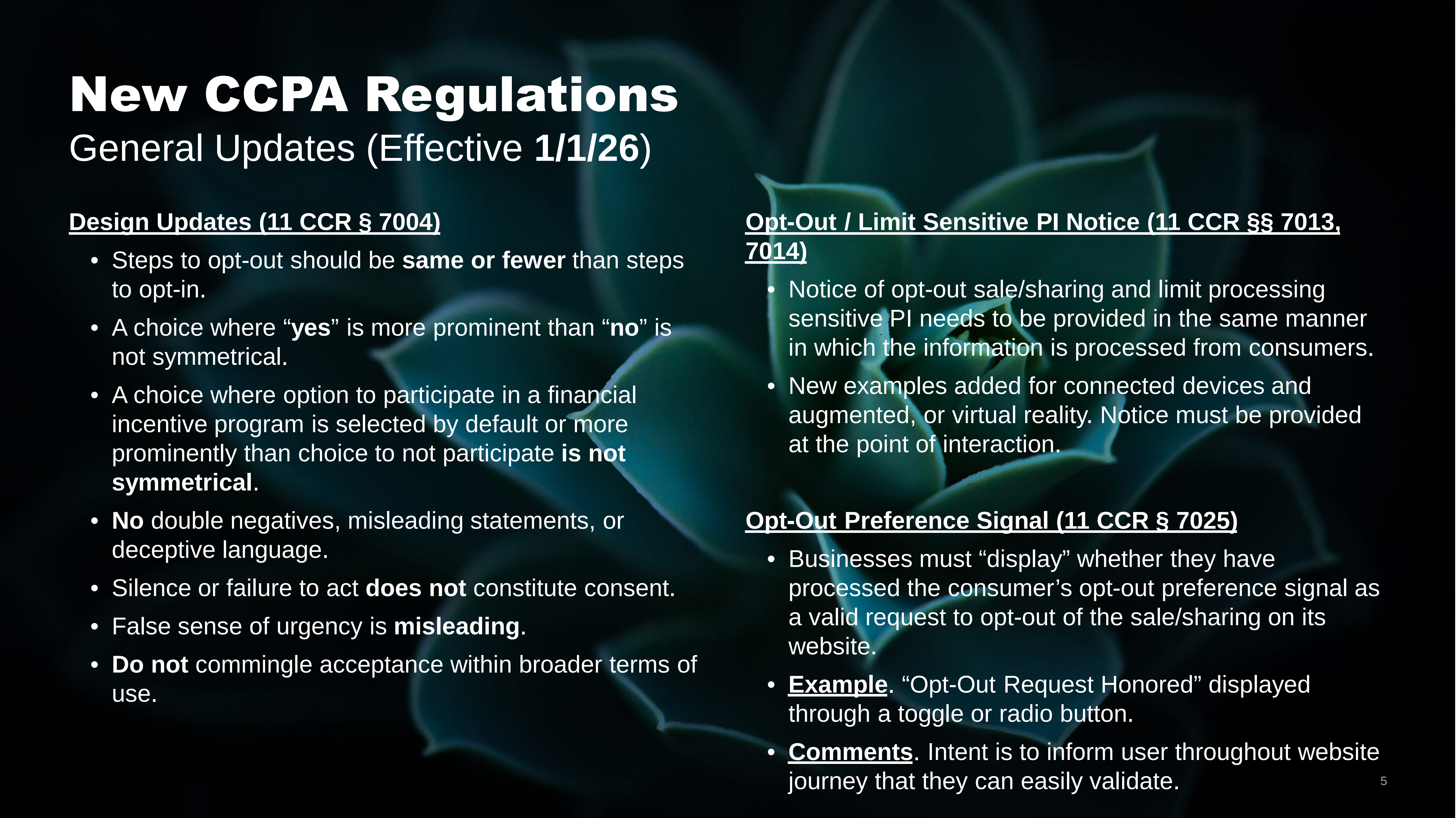
- New CCPA Regulations
- New California Privacy Laws
- Privacy Enforcement Trends
- Privacy Litigation Trends
- AI Regulation & Litigation
- Minor Data Trends Outside of CA
- Key Takeaways

New CCPA Regulations

New CCPA Regulations

What You Need To Know

- **General CCPA Updates**. New updates to the CCPA regulations clarifying symmetry of choice, opt-out links, and GPC signal recognition.
- **Risk Assessment Regulations**. “High risk” processing requires detailed risk assessments beginning 1/1/26 with reporting beginning 4/1/28.
- **ADMT Regulations**. Effective 1/1/27, impacts automated decision-making technologies in making decisions around finance, lending, employment, housing, education, or healthcare. Robust pre-use notice and opt-out rights included.
- **Cybersecurity Regulations**. Requires auditing against 18 controls for “high risk” processing. Rolling compliance depending on size of business starting 4/1/28.



New CCPA Regulations

General Updates (Effective **1/1/26**)

Design Updates (11 CCR § 7004)

- Steps to opt-out should be **same or fewer** than steps to opt-in.
- A choice where “**yes**” is more prominent than “**no**” is not symmetrical.
- A choice where option to participate in a financial incentive program is selected by default or more prominently than choice to not participate **is not symmetrical**.
- **No** double negatives, misleading statements, or deceptive language.
- Silence or failure to act **does not** constitute consent.
- False sense of urgency is **misleading**.
- **Do not** commingle acceptance within broader terms of use.

Opt-Out / Limit Sensitive PI Notice (11 CCR §§ 7013, 7014)

- Notice of opt-out sale/sharing and limit processing sensitive PI needs to be provided in the same manner in which the information is processed from consumers.
- New examples added for connected devices and augmented, or virtual reality. Notice must be provided at the point of interaction.

Opt-Out Preference Signal (11 CCR § 7025)

- Businesses must “display” whether they have processed the consumer’s opt-out preference signal as a valid request to opt-out of the sale/sharing on its website.
- **Example**. “Opt-Out Request Honored” displayed through a toggle or radio button.
- **Comments**. Intent is to inform user throughout website journey that they can easily validate.

New CCPA Regulations

Risk Assessments

- **Effective**. 1/1/26 to begin conducting risk assessments. 4/1/28 to begin submitting attestation to CalPrivacy that assessments were completed and a summary.
- **Triggers (11 CCR § 7150)**. Processing presents a "**significant risk**" to privacy. "**Significant risk**" includes:
  - Selling or sharing PI.
  - Processing sensitive PI (excluding employment processing).
  - Using an ADMT.
  - Using automated processing to infer features or characteristics about an individual in relation to applying for education, employment, or based on a sensitive location.
  - Processing PI to train an ADMT or train a facial-recognition or emotion-recognition system.

New CCPA Regulations

Risk Assessments

Requirements (11 CCR § 7152)

- Purpose for processing, categories of PI, processing methods, retention length, methods of interacting with consumers, approximate number of consumers impacted, and disclosures made.
- Names or categories of third parties / service providers, and purpose of disclosure to those parties.
- The logic of the ADMT, assumptions or limitations of the logic, the output, and how the business will use the output to make a significant decision involving the consumer.
- Benefits to the business, consumer, or other stakeholders, and the public from the processing.
- Negative impacts to consumer's privacy (unauthorized access, discrimination, impaired control, coercion, economic harm, physical harm, reputational harm, and psychological harm).
- Identify safeguards (PET, encryption, policies, etc.).
- Whether processing will move forward, the individuals who provided information for the risk assessment, and the date of approval and review.

New CCPA Regulations

Risk Assessments

Stakeholder Involvement (11 CCR § 7151)

- An employee who processes PI must be included in the risk assessment. May include external parties, including service providers, experts, or other stakeholders.

Timing, Retention, Reporting

- May conduct a single risk assessment for a comparable set of processing activities. Must complete before processing begins. Must be conducted on processing that begins before 1/1/26 but carries over.
- Must be reviewed and updated ever three years or within 45 days of a material change. Retain risk assessments for so long as the processing continues or 5 years after completion of risk assessment, whichever is later.
- Risk assessments completed in 2026 and 2027 must be submitted to CalPrivacy no later than 4/1/28. April 1 thereafter.
- Submit information to CalPrivacy about scope, and attest to summaries.

California ADMT Regulations (Jan. 1, 2027)

"**Automated decision making**" technology processes personal information and uses computation to replace human decision making, or substantially replace human decision making. New rules apply to ADMT used to make a "**significant decision**" (i.e., high-risk area of life such as employment).

Pre-use Notice

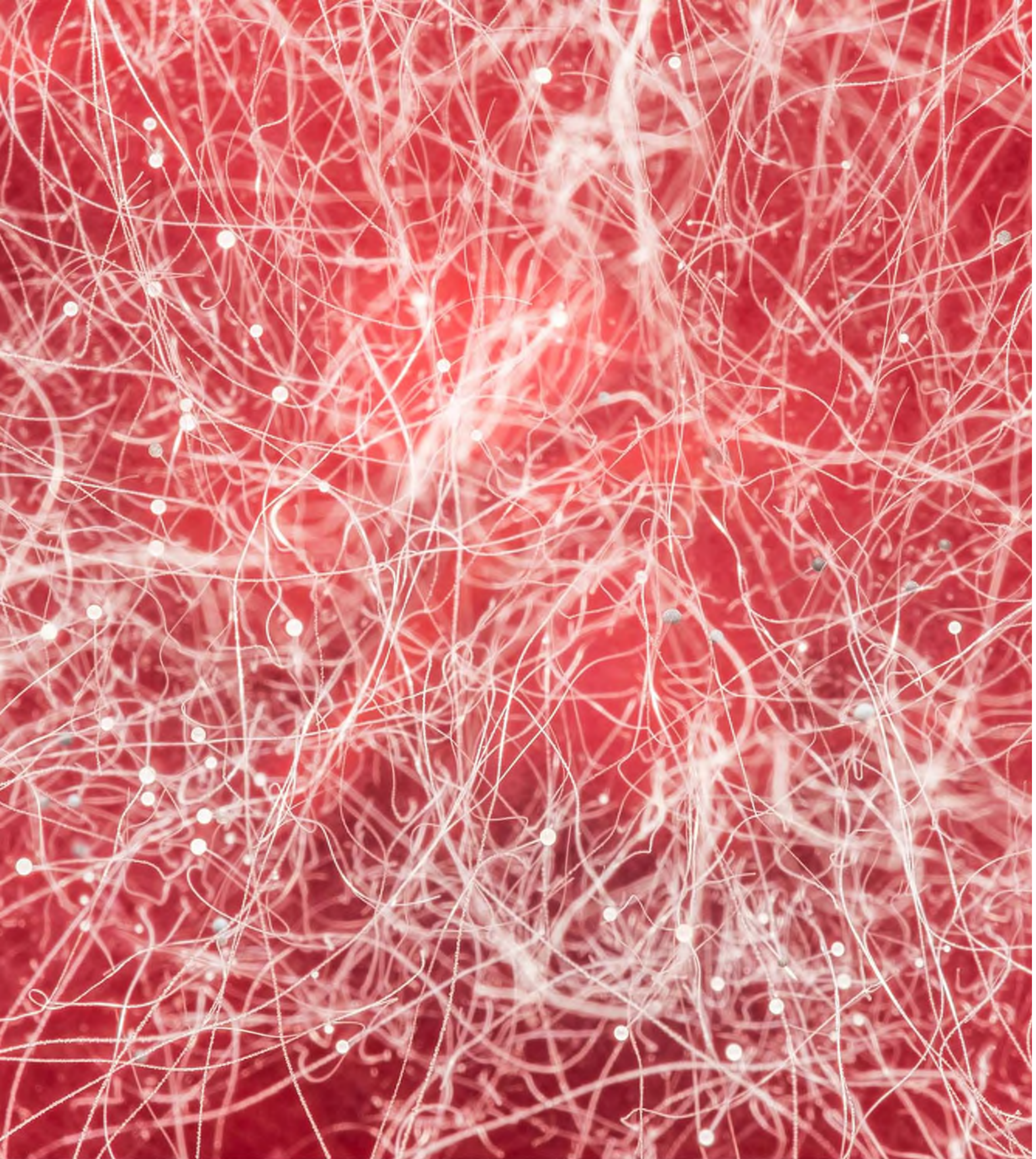
Inform consumers about the use of the ADMT, the right to opt-out, and right to access the ADMT.

Consumer Rights

Consumers have the right to opt-out of ADMT use and access information about the logic and outcome.

Risk Assessments

Evaluate training data and testing processes to identify and mitigate potential bias.



New CCPA Regulations

Cybersecurity Audits

- **Effective Date**. 4/1/28 over $100m annual gross revenue. 4/1/29 for $50m-$100m. 4/1/30 if less than $50m.
- **Triggers**. Any business that derives 50% or more revenue from selling or sharing, or $25m annual gross revenue + processing the PI of 250k or more consumers in preceding calendar year, or 50k or more consumers in preceding calendar year.
- **Auditor Requirements**. Must be independent with knowledge of cybersecurity. Can be internal or external if sufficiently independent.
- **Scope**. Must review 18 separate controls, including around access, encryption, inventory, configuration, training, and awareness.
- **Certification**. Must certify completion of the audit no later than 4/1 of following year by member of executive management team with cyber knowledge.

New California Privacy Laws

New CA Privacy Laws

Privacy Related

Opt-Out Preference Signals

Requires all web browsers to include a setting that enables consumers to send an opt-out preference signal by **January 1, 2027**.

The law also grants browser companies immunity from liability for website operators who fail to recognize the signal.

This may impact the rate of opt-outs coming from browsers such as Chrome and Edge.

Age Verification Signals

The Digital Age Assurance Act will require operating system providers to implement an age verification interface by **January 1, 2027**.

The operating system provider will be required to send age bracket signals to mobile applications in covered app stores.

This may impact a company's position re: "knowledge" of minor data.

Data Broker Law Expansion

Effective **January 1, 2026**, data brokers must provide additional disclosures at registration, such as whether the broker collects sensitive data such as children's data, precise geolocation, biometric data, and government IDs. Watch for DROP Act regulations (automatic deletion mechanism)

Note, broader data broker definitions took effect earlier this year. Potential impact on enhancement data.

Privacy Enforcement Trends

CalPrivacy / California AG

Enforcement Actions (2025)

Sling TV

- California AG / Announced **10/30/25**.
- Resulted from AG sweep of streamlining services.
- **$530,000** in penalties with data disgorgement relief (settlement).
- Inadequate opt-out flow, no recognition of opt-out signal.
- Selling minor data on dedicated channels without protections.

Tractor Supply Company

- Cal/Privacy / Announced **9/30/25**.
- **$1,350,000** in penalties (settlement).
- Inadequate privacy policy.
- Inadequate privacy notice to job applicants.
- Inadequate opt-out flow or recognition of opt-out signal.
- Inadequate contracts with third parties.

Healthline Media

- California AG / Announced **7/1/25**.
- **$1,550,000** in penalties (settlement).
- Failed to allow consumers to opt-out of targeted advertising with third parties without protections, including data suggesting serious health conditions.
- Inadequate contracts.

Honda

- CalPrivacy / Announced **3/12/25**.
- **$632,500** in penalties (settlement).
- Over collection of data for verification and opt-out.
- Dark patterns (non-symmetry of choice).
- Inadequate contracts.

Privacy Litigation Trends

Privacy Litigation

A Continuing Battleground

- **Eavesdropping / Wiretapping / Pen Register / Trap & Trace Device**. These cases continue to progress across California, with new players involved daily. Expanding claims to federal law to avoid coming California restrictions.
- **Check-Out Targets**. Increased litigation around collection of personal information to process a credit card, offer discounts, and use of payment providers such as Stripe, etc.
- **AI Litigation On The Rise**. AI + privacy is a growing field.
  - **Ambriz, et al. v. Google LLC (N.D. Cal)**. Google AI call center on behalf of multiple clients, including Home Depot. Allegation is that Google violated CIPA directly.
  - **Galanter v. Cresta Intelligence (N.D. Cal)**. Conversation intelligence SaaS used by United Airlines. Ingests live conversations and prompts agents with real-time suggestions. Allegation is United Airlines aided and abetted Cresta to violate CIPA without consent.
  - **Brewer v. Otter.ai (N.D. Cal)**. Allegation of violation of CIPA through use of AI recording software.

AI Regulations & Litigation

FEHA Regulations

Preventing Algorithmic Discrimination

- **Effective**. October 1, 2025.
- **Regulates Automated-Decision Systems (ADS)**. A computational process that makes or assists in making decisions regarding employment benefits, such as hiring, promotion, selection for training programs, and similar activities. Not limited to AI. Excludes common tools.
- **Prohibited Action**. It is unlawful for an employer to use an ADS to discriminate against an applicant or employee on a protected basis. Evidence or lack of evidence of anti-bias testing or “similar proactive efforts to avoid unlawful discrimination” will be considered.
- **Recordkeeping**. Existing recordkeeping obligations can expand to ADS related data.

AI Employment Litigation

An Emerging Battleground

- **EEOC v. iTutorGroup (E.D. NY) (2023)**. EEOC alleged the company hired tutors based in the US to provide online tutoring from their homes or other remote locations. Allegation is that application software was programmed to automatically reject female applicants aged 55 or older and male applicants aged 60 or older. Fine of $365,000.

- **Mobley v. Workday (N.D. Cal. 2023)**. A black, over-40, disabled job applicant alleged Workday’s AI-powered hiring tools caused discrimination by screening out applicants based on race, age, disability in violation of Title VII, ADA, and ADEA. Agency theory is being permitted to proceed. June 2025, conditional certification occurred for certain claims.

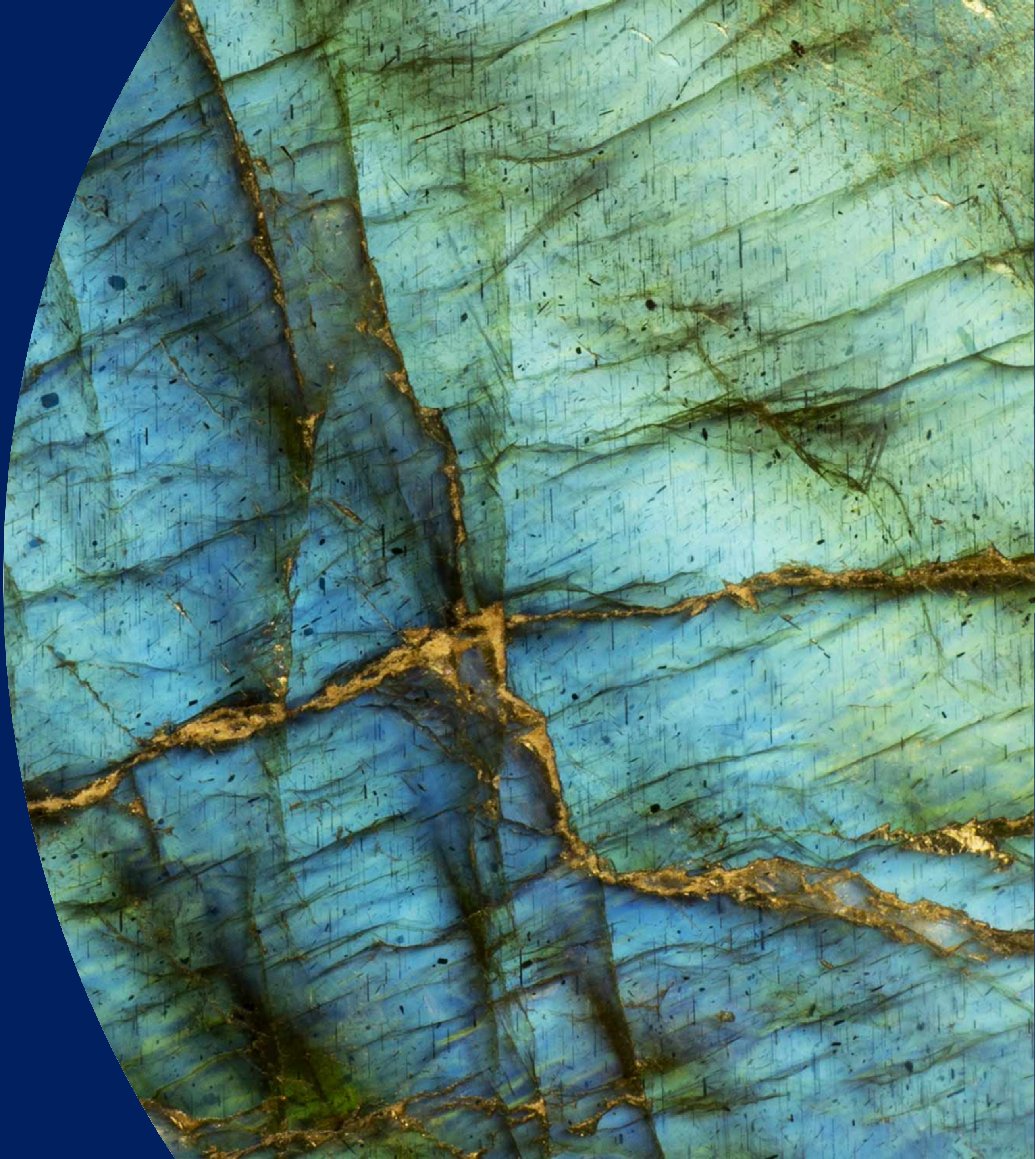
- **Harper v. Sirius XM Radio (E.D. MI) (August 2025)**. Job applicant alleges that Sirus XM relied on an AI-powered hiring system (iCIMS Applicant Tracking System) that embedded historical bias, resulting in his rejection from 150 positions.

Minor Data Trends Outside CA

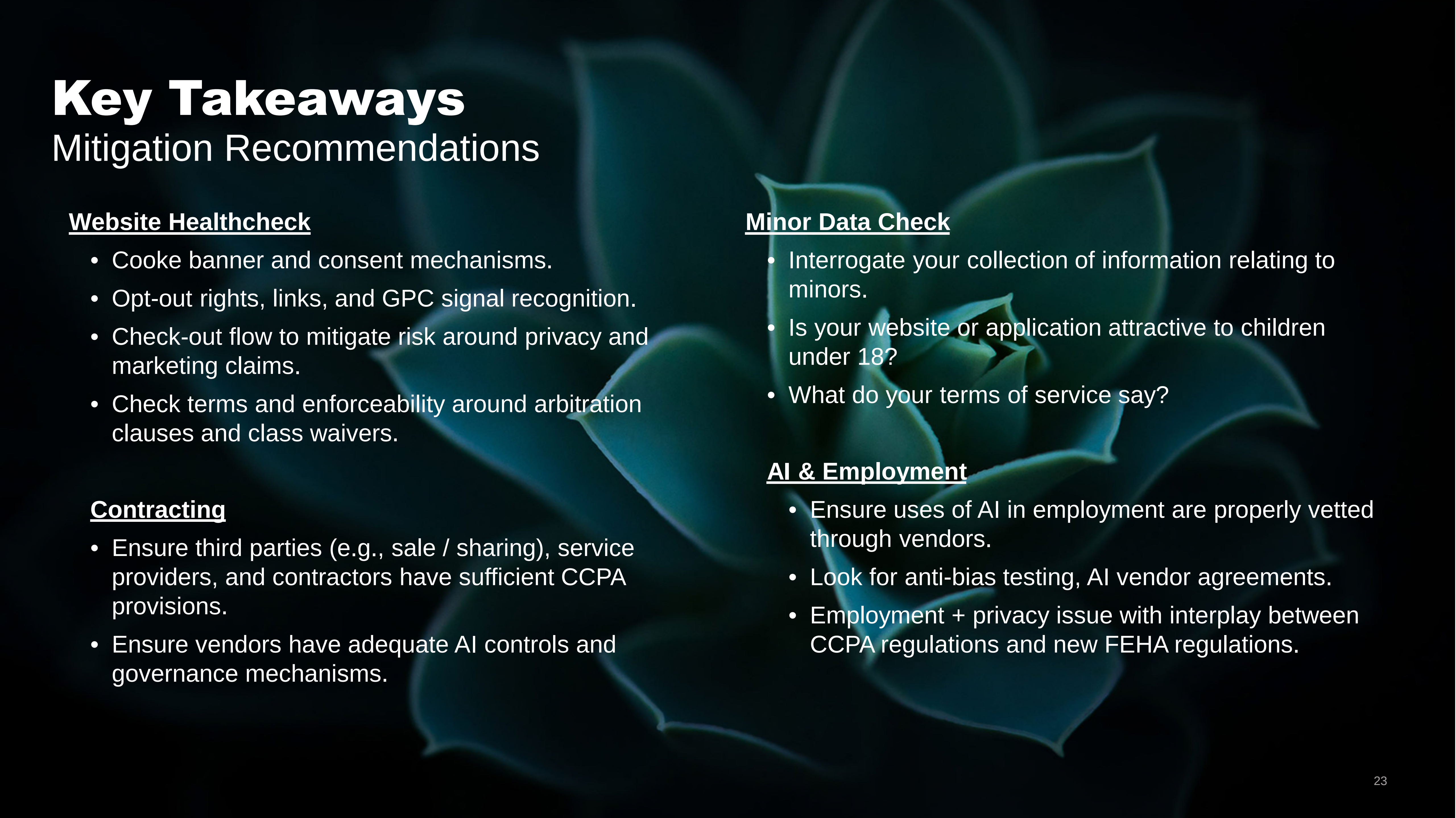
Minor Data Trends

New Laws & Restrictions

- **App Store Laws**. New trend in 2025 is legislation requiring app store providers to provide information to app store developers on age of users. Utah, Texas, and Louisiana all enacted laws that take effect in 2026.
- **Age-Appropriate Design Code Style Laws**. Several states enacted age-appropriate design code style laws following Maryland and California. These states include Arkansas, Connecticut, Montana, Nebraska, and Vermont. These laws require default settings for minors, geolocation data restrictions, impact assessments, restriction on targeted advertising and sale of data, and prohibition on dark patterns.
- **Pending Federal Bills**. Several bills are pending in Congress that may impact the collection and use of data of children under 18.



Key Takeaways



Key Takeaways

Mitigation Recommendations

Website Healthcheck

- Cooke banner and consent mechanisms.
- Opt-out rights, links, and GPC signal recognition.
- Check-out flow to mitigate risk around privacy and marketing claims.
- Check terms and enforceability around arbitration clauses and class waivers.

Contracting

- Ensure third parties (e.g., sale / sharing), service providers, and contractors have sufficient CCPA provisions.
- Ensure vendors have adequate AI controls and governance mechanisms.

Minor Data Check

- Interrogate your collection of information relating to minors.
- Is your website or application attractive to children under 18?
- What do your terms of service say?

AI & Employment

- Ensure uses of AI in employment are properly vetted through vendors.
- Look for anti-bias testing, AI vendor agreements.
- Employment + privacy issue with interplay between CCPA regulations and new FEHA regulations.

Questions

DENTONS

Speakers

Rebecca Hanovice
Mattel, Inc.
Head Privacy Counsel

Peter Stockburger
Dentons
619.876.1971
peter.Stockburger@dentons.com