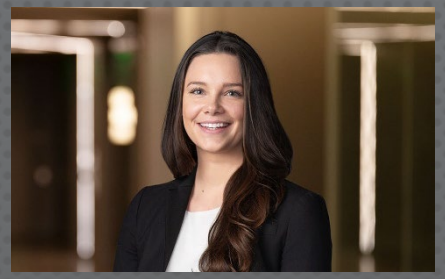
2024 Privacy Overview: How to Ensure Compliance and Reduce Business Risk

Scott C. Hall
Partner

Mari S. Clifford
Associate

Sabrina A. Larson
Partner



Emily Lentz
Associate

Amber Leong
Associate

Bina Patel
Associate

Coblentz Patch Duffy & Bass LLP

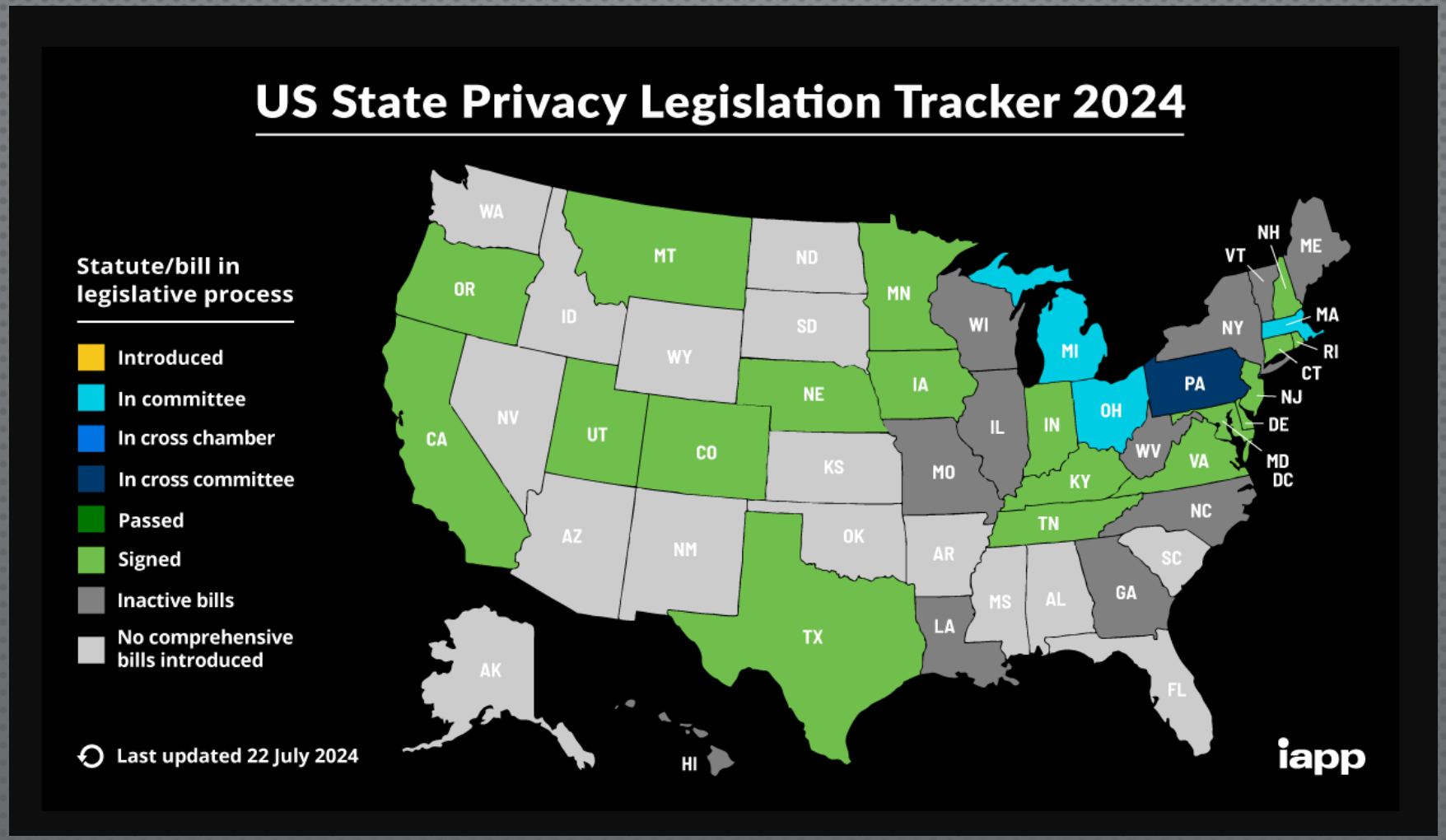
Agenda

- U.S. State Privacy Law Developments & Federal Privacy Law
- Privacy and Children's Data
- Health Privacy Trends
- Privacy Litigation Trends
- California Privacy Protection Agency's Priorities and Enforcement
- California's Draft Risk Assessment and Automated Decision-Making
- Artificial Intelligence and Privacy
- EU-U.S. Privacy Shield
- Takeaways

U.S. State Privacy Law Developments

- New State Privacy Laws Going into Effect in 2024 and Beyond
- What is similar and what is different in the new privacy laws being passed?
- What steps can businesses take to comply with the expanding patchwork of privacy laws?
- Status of a federal privacy law

Current Status of U.S. State Privacy Laws



Source: US State Privacy Legislation Tracker, IAPP.ORG

Coblentz Patch Duffy & Bass LLP

U.S. State Privacy Law Developments

2020	California
2023	Colorado, Connecticut, Utah, Virginia
2024	(Florida), Oregon, Texas, Montana
2025	Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland
2026	Indiana, Kentucky, Rhode Island

U.S. State Privacy Law Developments

- **Applicability Thresholds**
  - California – $25M Annual Revenue OR collection of PI of 100,000 residents
  - Other states – largely volume-based
    - Most states – Collection of PI from 100,000 residents
      - DE, MD, NH, RI (35k), MT (50k)
    - TX, NE – Doing business and offering goods/services to residents (no revenue or collection thresholds)
      - Small business exemption
    - FL – $1B Annual Revenue

U.S. State Privacy Law Developments

- **Consistent Principles**
  - Clear and conspicuous notice and transparency of use
  - Data minimization in collection and use
  - Selling/Sharing/Targeted Advertising Opt-Outs
- **Consumer Rights**
    - Know/Access
    - Delete
    - Correct (not Utah/Iowa)
    - Appeal (not California/Utah)
- **No Private Right of Action**

U.S. State Privacy Law Developments

- **New Requirements to Be Aware Of:**
  - **Opt-In Regimes for Sensitive Data** (not CA/UT/IA)
    - Traditional "sensitive" categories (SSN, health/biometric, financial)
    - Data of children/minors
    - Precise geolocation data
  - **Data Protection Impact Assessments** (not UT/IA)
    - High risk activities (selling, targeted advertising, profiling, sensitive data processing)
  - **Profiling/Automated Decision-making Rights**

Federal Privacy Law

- **American Privacy Rights Act (APRA)**
  - Would apply to any entity collecting covered data and subject to jurisdiction of FTC
    - Small business exemption for businesses with less than $40M in annual revenue and collection of personal information from less than 200,000 individuals
  - Typical consumer rights provided in state laws
    - Transparent privacy notices, opt-outs for targeted advertising, security measures
  - Exemptions for federal privacy laws (GLBA, HIPAA, FCRA) but would preempt state privacy laws
  - Private right of action for breach of various provisions
  - Right to opt out of AI/covered algorithms
  - Bipartisan support; gained traction but ultimately stalled due to redrafts/markups; disputes over consumer rights, private right of action, and preemption of state laws
  - When, if ever, we will get a federal privacy laws remains unclear

The Expansion of Privacy Laws for Children

- Federal Law: Children's Online Privacy Protection Act ("COPPA")
- California Laws
  - California's Age-Appropriate Design Code Act ("CAADCA")
  - California's Children's Data Privacy Act
- Non-California State Laws

Children's Online Privacy Protection Act ("COPPA")

- FTC's proposed changes to COPPA:
  - Businesses can only collect personal information that is reasonably necessary for a child to participate in an activity
  - Separate opt-in parental consent for targeted advertising
  - Cannot condition a child's online activity on collecting their personal information
  - Businesses must operate a written security program that includes safeguards for protecting children's personal information
  - Personal information includes biometric identifiers

California's Age-Appropriate Design Code Act ("CAADCA")

- Applies to businesses that provide online services or products that are "likely to be accessed by children" who are under the age of 18
- Businesses must complete a Data Protection Impact Assessment (DPIA)
- Businesses must implement stricter default privacy settings and terms
- Businesses cannot use "dark patterns"
- Businesses cannot use a child's personal information in a way that is "materially detrimental" to their physical or mental health

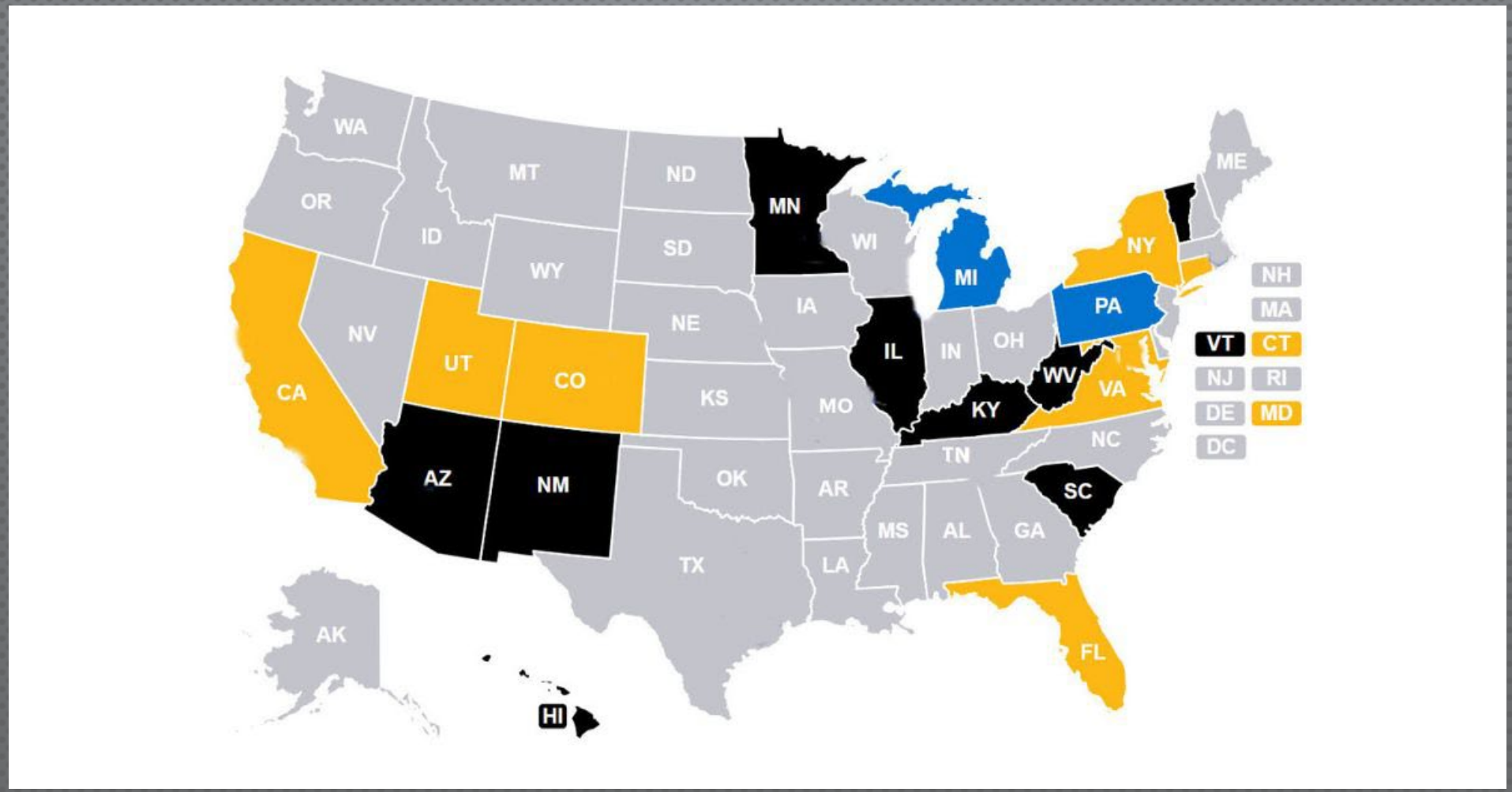
NetChoice LLC v. Bonta

- Dec. 2022 – NetChoice sues California to block CAADCA
- Sept. 2023 – U.S. District Court grants a preliminary injunction to halt enforcement of CAADCA
- Oct. 2023 – California AG appeals to the Ninth Circuit
- Aug. 2024 – Ninth Circuit issues opinion
  - Ninth Circuit upholds preliminary injunction on DPIA requirements
  - Remainder of the injunction is vacated

California's Children's Data Privacy Act (AB 1949)

- If passed, AB 1949 would amend the California Consumer Privacy Act (CCPA)
- Prohibits businesses from collecting, using, or disclosing personal data of minors under the age of 18
  - Exception: affirmative consent of the minor, or minor's parent/guardian (if minor is under the age of 13)
- Requires CA Privacy Protection Agency to issue regulations for age verification and opt-out preference signals

U.S. Child State Privacy Law Tracker



Source: https://www.huschblackwell.com/2024-state-childrens-privacy-law-tracker (last updated: June 2024)

Coblentz Patch Duffy & Bass LLP

Child State Privacy Laws: Common Trends

- “Child” includes children under the age of 18
- Websites meant for adults may be subject to children’s privacy laws if they are likely to be accessed by children
- “Personal information” includes broader categories of information (i.e., geolocation data and biometrics)
- Children’s consent is required before collecting, selling, or sharing their personal information
- Businesses must complete Data Protection Impact Assessments (DPIAs)
- Businesses are prohibited from using “dark patterns” to encourage minors to provide their personal information

Health Privacy Trends

- Health data collected by companies
- Focus on this area by state regulators:
  - California AG Bonta's letters to eight major pharmacy chains and five health data companies reminding them of their obligations to comply with California's Confidentiality of Medical Information Act (CMIA) and new protections for reproductive health or gender-affirming care data
  - New York, Connecticut, and New Jersey's $4.5 million settlement with Enzo Biochem, Inc. for poor data security practices that led to a ransomware attack compromising health data
  - Regulators from states including Connecticut and Oregon expressed a focus on consumer health data at the 2024 International Association of Privacy Professionals' Global Privacy Summit

Health Privacy Trends (cont.)

- Courts have appeared receptive to health data-related claims at the motion to dismiss stage.
- *See, e.g., In re Meta Pixel Healthcare Litigation,* 647 F. Supp. 3d 778 (N.D. Cal. 2022)
  - The health-related communications "justif[ied] departing from the presumption" that internet communications do not give rise to an expectation of confidentiality under CIPA because (1) the patient-status and medical-related communications are protected by federal law, and (2) "health-related communications with a medical provider are almost uniquely personal."
- *Yockey v. Salesforce*, 2024 WL 3875785 (N.D. Cal. Aug. 16, 2024)

Privacy Litigation Trends: Data Breach Class Actions

- Data breach class actions increase every year
- Individual suits often consolidated
- Claims
  - Consumer fraud or consumer protection statutes
  - Negligence and negligence *per se*
  - Breach of contract or implied contract
  - Invasion of privacy
  - State privacy laws or data breach notification laws

Privacy Litigation Trends: Data Breach Class Actions

- *TransUnion LLC v. Ramirez, et al.*, 141 S.Ct. 2190 (2021)
  - Standing to bring claims:
    - Concrete injury
    - Traceability
  - Class certification
    - Issue of uninjured class members
- Data breach settlements

Privacy Litigation Trends: Website Features

- Chatbots, Session Replay, Mouse Clicks and Web Click Trackers
- Pixels (Google, Meta, TikTok) and use of Analytics

Privacy Litigation Trends: New Theories

Current:

- CIPA Wiretapping
- Video Privacy Protection Act

New Theories:

- Trap and Trace / Pen Register
- California Song-Beverly Act
- California Unruh Act

Privacy Litigation Trends: New Theories

Trap and Trace / Pen Register

- What *are* they: – Historically, laws to protect individuals from having devices that tracked incoming and outgoing phone calls without a court order
- Plaintiffs' Theory: – Collecting or accessing IP Addresses or other routing information is analogous to collecting telephone numbers without user consent

Privacy Litigation Trends: New Theories

- Song-Beverly Credit-Card Act: Prohibits companies from requiring consumers to provide non-credit card personal information and "recording" it (i.e., information that is not typically on a receipt)
- Plaintiffs' Theory: Collection of IP addresses is personal information in violation of Act

Privacy Litigation Trends: New Theories

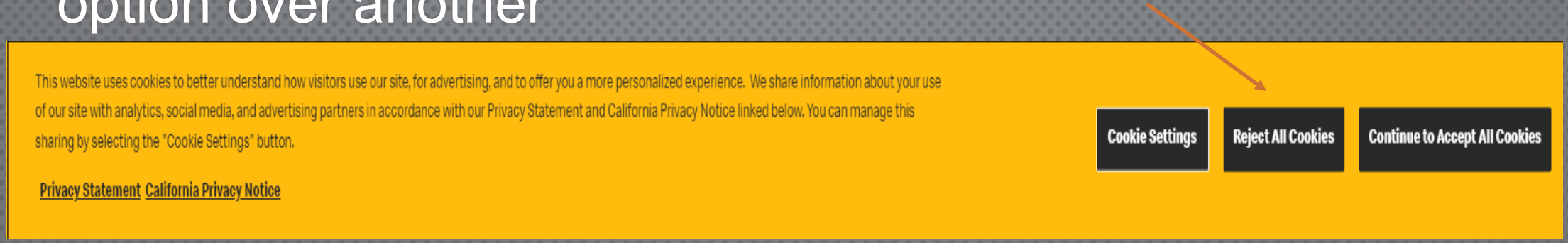
- California Civil Rights Unruh Act: The California civil rights statutes allow individuals to seek an enforcement of their rights against discrimination
- Plaintiffs' Theory: The use of analytics or targeted advertising is discrimination based on race, gender, or other protected traits

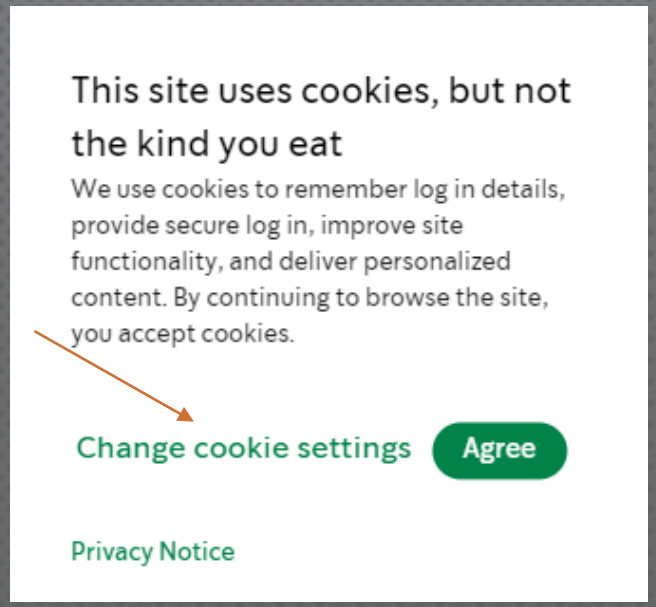
California Privacy Protection Agency (CPPA) Priorities

- Health Data – Post-*Dobbs*
- Sensitive Personal Information incl. Immigration Status
- Employee Data
- Smart Vehicles
- Dark Patterns
- Children Data
- Opt-Outs

CPPA Priorities (Cont'd)

- Dark Patterns: Designs to encourage or discourage one option over another





Coblentz Patch Duffy & Bass LLP

California's Focus on Enforcement and Priorities

Enforcement Decisions

- **Children's Data Privacy**
  - The CPPA recently fined an online gaming company $500,000 for violating COPPA and CCPA provisions related to children's data. The case highlights the importance of providing neutral and effective age screens and obtaining verifiable parental consent before collecting personal information from minors.
- **Failure to Honor Opt-Outs**
  - High-profile cases such as those against Sephora and DoorDash have underscored the importance of respecting consumer opt-out preferences, including the failure to honor global opt-out signals. These cases illustrate the CPPA's commitment to enforcing opt-out rights under California's privacy laws.

California's Draft Risk Assessment and Automated Decision-Making (ADMT) Regulations

- **Development Stage:** Still in progress
- **Court Ruling:** CPPA can enforce rules immediately upon finalization
- **Potential Changes:** Regulations may change before official adoption but certain core elements unlikely to shift

Definition of ADMT by CPPA

- **Definition:** Software or programs that process personal data to execute, replace, or facilitate human decision-making
- **Includes:** Machine learning, statistics, other data-processing techniques, and artificial intelligence
- **Exclusions:** Spam filters, spreadsheets, firewalls (unless used to circumvent regulations)

Covered Uses of ADMT

- **Making Significant Decisions**
  - **Impact:** Decisions affecting rights or access to critical goods, services, and opportunities (e.g., jobs, education, healthcare, loans)
- **Training ADMT**
  - **Scope:** Use of consumer personal data to train ADMT tools
  - **Applications:** Significant decisions, identification, deepfakes, physical or biological identification, and profiling
- **Extensive Profiling**
  - **Definition:** Automated processing to evaluate or predict traits and characteristics
    - **Examples**
      - Profiling in work or school (e.g., keystroke logging)
      - Profiling in public places (e.g., facial recognition)
      - Behavioral advertising

Draft CCPA Rules on AI and Automated Decision-Making (ADMT) Technology

- **Key Requirements**
  1. **Pre-Use Notices**
     - Organizations must issue notices to consumers before using covered ADMT
  2. **Opt-Out Options**
     - Consumers must be offered ways to opt out of ADMT
  3. **Impact Explanation**
     - Businesses must explain how their use of ADMT affects consumers

Exemptions to Opt-Outs for ADMT

1. **Safety, Security and Fraud Prevention**
   - No opt-out needed for ADMT used to detect/respond to security incidents, prevent/prosecute fraud, and ensure physical safety
2. **Human Appeal Exception**
   - No opt-out if consumers can appeal automated decisions to a qualified human reviewer
3. **Work and School Contexts**
   - **Performance Evaluation**: Admissions, hiring, task allocation, compensation
   - **Profiling**: Assessing performance as a student or employee

States with Enacted AI Legislation (Part 1)

- **California: Bolstering Online Transparency Act (BOT)**
  - Requires disclosure when a bot is used to communicate online for sales or influencing votes
- **Alabama: SB 78**
  - Establishes the Alabama Council on Advanced Technology and AI
  - Advises on the use and development of advanced technology and AI
- **Illinois: AI Video Interview Act**
  - Requires employers to notify applicants and obtain consent before using AI to analyze video interviews
  - Mandates sharing of AI evaluation results with applicants upon request

States with Enacted AI Legislation (Part 2)

- **New York: NYC Local Law 144**
  - Regulates the use of automated employment decision tools
  - Requires bias audits and disclosure to candidates
- **Massachusetts: AI Task Force**
  - Established to study and provide recommendations on AI use and regulation
  - Focuses on ethical and equitable AI deployment
- **Tennessee AI Legislation: Ensuring Likeness, Voice, and Image Security (ELVIS) Act**
  - **Effective Date: July 1, 2024**
  - **Disclosure Obligations**
    - Disclose the use of AI-generated voices and fake recordings (deepfakes)
  - **Right of Publicity**
    - Expands the right of publicity law
    - Provides individuals with property rights over their name, photograph, likeness, or voice
  - **Consumer Protection**
    - Aims to combat the rise of AI-generated deepfakes

Colorado AI Act

- **Effective Date**: February 1, 2026
- **Requirements**
  - **Risk Management**: Establish and implement risk management policies
  - **Impact Assessments**: Conduct thorough impact assessments before deployment
  - **Consumer Notices**: Provide specific notices to consumers about AI use
  - **Algorithmic Discrimination**: Prevent and disclose any known or foreseeable risks of algorithmic discrimination
  - **Annual Reviews**: Annually review AI systems to ensure they do not cause discrimination

EU AI Act

- **Categorizes AI systems by risk levels**
  - Prohibited, High-risk, Limited-risk, Minimal-risk
- **High-risk AI systems**
  - Subject to strict regulations (data governance, compliance documentation)
- **General-purpose AI systems**
  - Must meet specific rules and transparency on training data
- **Systemic-risk AI models**
  - Providers must assess, mitigate risks, and ensure cybersecurity
- Act establishes **timelines** for compliance, monitoring, and implementation

EU-U.S. Data Privacy Framework

- **Overview**
  - **Effective Date**: July 10, 2023
  - **Purpose**: Facilitates data transfer between the EU and U.S. while ensuring data protection
  - **Replaces**: EU-U.S. Privacy Shield (invalidated by Schrems II decision in 2020)
- **Compliance and Impact**
- **Data Transfer**
  - Smooth flow of personal data without additional contractual arrangements
- **Consumer Protections**
  - EU citizens can address and challenge privacy concerns
- **Business Implications**
  - Affects companies handling EU personal data
  - Encourages adherence to high data protection standards

EU-U.S. Data Privacy Framework

- **Requirements for Self Certification**
  - Clearly outline data collection, use, and protection practices
  - Provide free and accessible dispute resolution mechanisms
  - Designate an independent recourse mechanism for handling complaints
  - Inform individuals of their rights to access their personal data
  - Establish procedures for data access requests
  - Address and resolve complaints within 45 days

Conclusion and Key Takeaways (Part 1)

- **Summary of Key Points:**
  - The 2024 privacy landscape is shaped by a combination of new state laws, ongoing federal discussions, and heightened regulatory enforcement.
  - Businesses must navigate these changes by implementing comprehensive privacy strategies that account for both state-specific and federal requirements.
  - Ongoing trends in privacy litigation and enforcement underscore the need for proactive compliance measures, particularly in areas like AI, automated decision-making, and children's privacy.
  - Ensure your business is not engaging in prohibited activities (i.e., using “dark patterns,” processing child’s personal data, including geolocation data)

Conclusion and Key Takeaways (Part 2)

- **Action Items for Legal Compliance:**
  - **Review and Update:** Regularly review and update your privacy policies and practices to ensure they align with the latest legal developments.
  - **Cookie Banners:** Not required, but suggested, and ensure adequate disclosures and neutral options
- **Monitor Legal Landscape:** Stay informed about emerging privacy laws and enforcement trends.
- **Engage in Continuous Training:** Ensure that your legal and compliance teams are up-to-date on best practices and legal obligations.

Conclusion and Key Takeaways (Part 3)

- **Be Extra Mindful and Cognizant of Collection Practices Pertaining to:**
  - **Children's/Minors' Data**
  - **Employee Data**
  - **Health Data**
  - **Sensitive Personal Information**
  - **Honoring Opt-Outs and Requests**

Questions and Discussion

- Open Floor for Questions

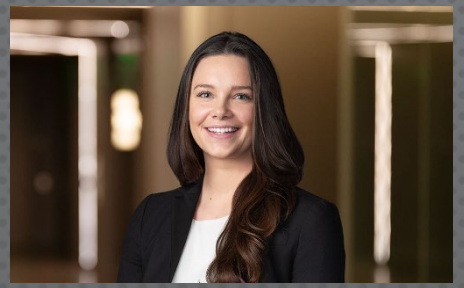
Thank You for Attending

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

Scott C. Hall
Partner
shall@coblentzlaw.com

Mari S. Clifford
Associate
mclifford@coblentzlaw.com

Sabrina A. Larson
Partner
slarson@coblentzlaw.com



Emily Lentz
Associate
elentz@coblentzlaw.com

Amber Leong
Associate
aleong@coblentzlaw.com

Bina Patel
Associate
bpatel@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP