2025 PRIVACY AND CYBER LAW UPDATE – WHAT'S OLD IS NEW AGAIN

9/24/2025

PRESENTER: NICK ADAMS (BMO)

CCPA V. 3.0: NEW REGULATIONS

- July 2025: the California Agency Board voted unanimously to **finalize** draft regulations on automated decision-making technology ("ADMT"), cybersecurity audits, and risk assessments after multiple years of drafts and public comments.
- The regulations moved to the Office of Administrative Law on August 8.

NEW REGULATIONS – KEY DATES

- ADMT regulations: require compliance **on or before January 1, 2027**.
- Privacy risk assessment: require Agency reporting for large entities by **April 1, 2028**
  - initial set of risk assessments must be complete by **December 31, 2027** and must cover activities going back to the effective date of the regulations.

NEW REGULATIONS – KEY DATES

- New requirement to display opt-out preference signal confirmation **on effective date** (previously optional)
- Cybersecurity audit report regulations: require a first report covering calendar year 2027 to be filed by **April 1, 2028** for entities with gross revenue over $100m,
  - deadline a year later for $50-100m, two years later for $25-$50m.

AUTOMATED DECISIONMAKING TECHNOLOGY (ADMT)

- Data level GLBA and FCRA exemptions apply to the ADMT regulations (chapter-wide).
- Consider systems that process California personal information in connection with business/commercial customers, prospects, employees and job applicants.

AUTOMATED DECISIONMAKING TECHNOLOGY (ADMT)

- Definition of ADMT**:** covers technology that that **processes personal information** and **substantially replaces human decision making.**
- Any human involvement that requires the human to understand and interpret the technology, review its output, and be capable of overriding or change the decision recommended by the technology removes the technology from the definition of ADMT.
- ADMT does *not* need to involve AI or machine learning technology, any excel spreadsheet can constitute ADMT if it is used to replace human decision making.

ADMT REGULATIONS

- Only apply to certain **significant decisions**, which are decisions that result in the provision or denial of **financial or lending services, housing, education, employment or contracting opportunities, work compensation, or healthcare services.**
  - The phrase “financial or lending services” includes not only extensions of credit or the provision of deposit or checking accounts, but also transmitting or exchanging funds, check cashing, and any installment payment plans.
  - “Employment or independent contracting opportunities or compensation” includes hiring, firing/suspension, promotion/demotion, allocation/assignment of work, compensation, benefits
  - Behavioral advertising, profiling and model training are no longer considered a “significant decision” subject to ADMT regs. Instead, they are subject to risk assessments.

ADMT REGULATIONS

- The ADMT regulations convey three key rights
  - Pre-Use Notice (warn individuals before using ADMT)
  - Opt-Out Right (ability to avoid or appeal ADMT),
  - Access Right (ability to ask for more information about the ADMT).
- All types of decisions subject to ADMT Opt-Out Rights (includes decisions for safety, security and anti-fraud purposes) may be satisfied with a human appeal option.
- No more opt-out/appeal exemption for security/fraud ADMT, but most HR use cases (hiring, allocation/assignment of work, compensation) are exempt from opt-out/appeal so long as solely used for this purpose and they do not unlawfully discriminate

ADMT PRE-USE NOTICE

- The ADMT Pre-Use Notice can be combined with the CCPA Notice at Collection, which means it can be centralized and included with the point of collection disclosures already presented, more detailed information may be hyperlinked or provided via layered notice separately
  - Consolidation of multiple ADMTs used for a single purpose or a single ADMT used for multiple purposes into a single Pre-Use Notice possible but may be limited by different opt-out/appeal paths
- The more detailed information required pursuant to an Access request may be limited to remove trade secrets and information that would compromise security and anti-fraud efforts

COLORADO AI ACT - JUNE 2026 EFFECTIVE DATE

- Key similarities and differences:
  - Both target algorithmic discrimination, transparency
  - Both define AI/ADMT broadly – no autonomy required
  - Both cover financial services and employment, but CO does not define “financial or lending service”
  - CO has no GLBA exemption – banking exception is narrow and convoluted, requires FI to be examined by banking regulator under guidance or regulations that apply to the use of high-risk AI systems, AND which imposes requirements substantially equivalent or more stringent than CO AI Act, including regular audit of AI systems for anti-discrimination law compliance

COLORADO AI ACT – KEY SIMILARITIES & DIFFERENCES CONT.

- CO has no meaningful human involvement exception – any technology that "assists in making" a consequential decision or is "capable of altering" the outcome of a consequential decision is included
- CO differentiates obligations of developers vs. deployers
- CO appeal right limited to adverse decisions
- CO has a fraud/cyber exemption, but only if technology is not a substantial factor in a consequential decision
- CO utilizes the CO Privacy Act for its opt-out right, AI Act is chaptered separately
- Risk assessments required as part of CO AI Act, vs. as part of CA Privacy regulations

PRIVACY RISK ASSESSMENTS INCLUDES

- Sharing personal information for behavioral advertising (advertising based on activity or PI gathered at multiple businesses)
  - Selling personal information (BMO does not sell)
  - Processing sensitive personal information (“SPI”) including SSN, ID card, passport number, account number or login along with PIN/password sufficient for access, precise geolocation, racial/ethnic origin, citizenship/immigration status, contents of email/text messages where BMO not intended recipient, biometric info, health info, personal information of known minors under 16
    - Exception for processing SPI where strictly for administering HR benefits, pay, work authorizations (e.g. background checks, immigration status), providing worker accommodations

PRIVACY RISK ASSESSMENTS INCLUDES CONT.

- Using ADMT for a significant decision (can leverage ADMT workstream)
- Systematic observation of employees used to extrapolate performance at work, intelligence, aptitude, behavior, preferences, or interests (aka “profiling”)
- Training ADMT for a significant decision or training identity verification technology (with or without biometrics)

TIMELINE FOR COMPLETING PRIVACY RISK ASSESSMENTS

- Prior to any new processing activity that qualifies
- At least once every three years for previously-completed assessments
- Within 45 days of any material change in processing – “material” if creates new negative impacts or increases magnitude of previously-identified negative impacts (i.e. more data collected, new complaints, change in use)
- By December 31, 2027 for any qualifying processing as of effective data of regulations

REQUIREMENTS IN A RISK ASSESSMENT

- Description of purpose for processing
- Categories of PI to be processed, including sensitive personal information, and must include minimum PI necessary to achieve purpose
- Method for collection, use, disclosure, and/or retention of PI
- Retention period or criteria for retention period

REQUIREMENTS IN A RISK ASSESSMENT CONT.

- Method of interacting with consumers being processed (i.e. web/app, mail, phone, in person) and purpose of interaction (i.e. provide service)
- Approximate amount of consumers subject to processing
- List of existing disclosures about processing (i.e. CCPA notice at collection, ADMT pre-use notice, Digital Privacy Policy)
- Categories of service providers and third parties to whom data is disclosed and purpose for disclosure

REQUIREMENTS IN A RISK ASSESSMENT CONT.

- For ADMT, logic of ADMT including any assumptions or limitations of logic, and output of ADMT and how business will use output
- Benefits to business, consumer, other stakeholders, and public, and risks or negative privacy impacts (risk of unauthorized access/use, discrimination, lack of consumer control, coerced processing by conditioning service based on unnecessary disclosure, economic harm based on profiling, risk of physical or psychological harm, reputational harm)

REQUIREMENTS IN A RISK ASSESSMENT CONT.

- Safeguards business plans to implement (i.e. encryption, segmentation, access controls, change management, network monitoring and defenses, data quality/integrity monitoring, trusted execution environments, federated learning, homomorphic encryption, differential privacy, third party due diligence and reviews, threat intelligence and detection, policies/procedures/training, anti-discrimination analysis)

REQUIREMENTS IN A RISK ASSESSMENT CONT.

- Final decision on initiating processing, **list of individuals who provided information for assessment** other than counsel providing legal advice
- Date of approval, **name and position of assessment reviewers/approvers, which must include anyone with authority to participate in deciding whether business will initiate processing**

CYBERSECURITY AUDITS – WHO MUST COMPLY?

- Businesses which:
  - Derive 50% or more of their annual revenues from selling or sharing consumers' personal information; or
  - Have annual gross revenues exceeding $26,625,000 (adjusted periodically for inflation) and, in the preceding calendar year, processed the personal information of 250,000 or more consumers or households, or the sensitive personal information of 50,000 or more consumers.

CYBERSECURITY AUDITS – WHEN THEY NEED TO BE COMPLETED AND WHAT NEEDS TO BE INCLUDED IN THE AUDITS

- Audits must cover long list of topics “if applicable” and businesses must certify to Agency that audit was completed, certification must be signed by executive with direct responsibility for cybersecurity audit requirements
  - Some required coverage areas are fairly specific or veer into privacy topics – i.e. password strength enforcement, personal information mapping and classification, hardware inventories, DLP, training, record retention schedules

CYBERSECURITY AUDITS – WHEN THEY NEED TO BE COMPLETED AND WHAT NEEDS TO BE INCLUDED IN THE AUDITS

- Audits must be annual, qualified auditor may be internal or external, but if an internal auditor is used, the highest-ranking auditor must report directly to a member of executive management who does not have responsibility for the business's cybersecurity program

PRESENTER: NICK GINGER (CITY NATIONAL)

WEBSITE TRACKERS

Cookies	Pieces of data, usually text, that a website, or a server, **places on a user's device** and that store information, usually user preferences, login details. When people think of tracking technologies, they are often thinking of Cookies.
Pixels (aka Web Beacons)	Small piece of code **placed on a website** in the form of a single pixel to track a user's activity (usually in real time), such as clicks, pageviews, purchases. The Pixel is usually transparent and often difficult for the user to notice. **Conversion Pixels** allow companies to see how users are directed to their site. By knowing which site directed a user to the company's site, companies can gauge the effectiveness of **where** they advertise. **Retargeting Pixels** allow companies to collect information about a user's activity on their site, and then follow up with a targeted ad or email based on that information. The GoodRX complaint is a good overview of how Pixels work
Software Development Kits (SDKs)	Not a tracker by itself but provides the means by which most tracking through mobile apps occur. An SDK is essentially a package of tools (libraries, documentation, code samples, etc.) that helps an app function in a particular way, such as to track users.
Tag	Small piece of code **placed on a website that communicates with a 3rd party** analytics platform (Google Analytics, Adobe Analytics) and receives instructions on what data to collect.

WEBSITE TRACKERS

- Information collected through tracker technology is often sold to data brokers who use the information to build profiles on consumers.
- These profiles are then made available to advertisers interested in targeting their ads.

HOW IS THIS DATA HELPFUL TO COMPANIES?

- Allow personalization of sites.
  - Ex. Sites providing information on the weather or the news can be localized so you see information relevant to your location.
- Allow expected functionality.
  - Ex. When you buy products online, there is often a shopping cart function where you place the items you wish to purchase. This is all done through the magic of cookies.
- Save time.
  - Ex. Information about websites you visit often is stored, this allows the sites to load faster the next time you visit. That little “remember me” button on a login screen is made possible by these technologies.
- Advertising.
  - Ex. This one is a mixed bag, but it cannot be denied that these technologies help connect businesses with the customers they care most about.

CALIFORNIA INVASION OF PRIVACY (CIPA)

- Enacted in 1967, Cal. Penal Code §§ 630–638.55
  - The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

CALIFORNIA INVASION OF PRIVACY (CIPA)

- Allows private private right of action
  - Many current Privacy laws have limited or no right to private action. This is one of the more contentious issues making it difficult to pass a Federal Privacy law.
- Prior consent required
- Applies broadly to wiretapping, eavesdropping, recording

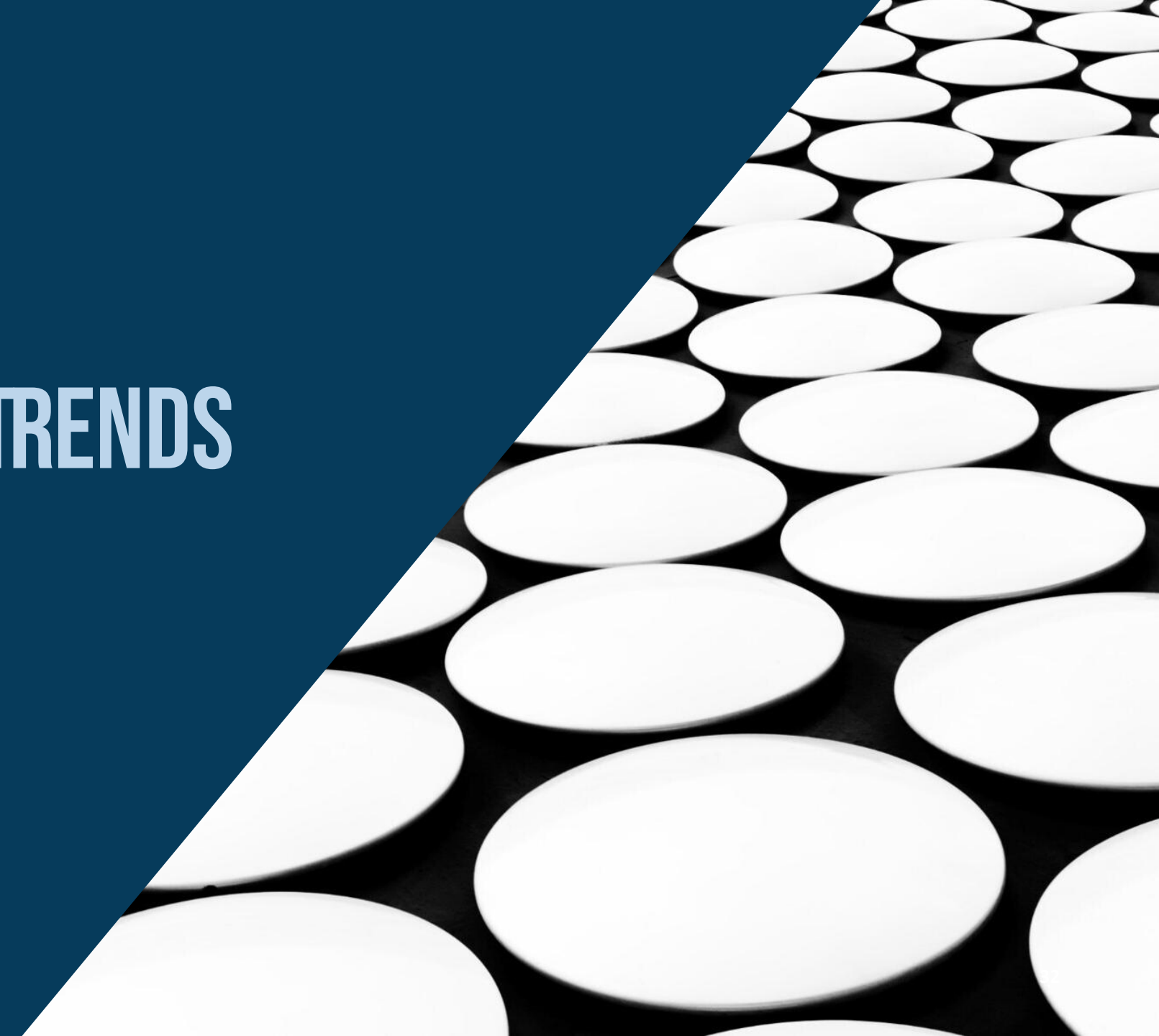
CALIFORNIA INVASION OF PRIVACY (CIPA)

- Potential mitigants
  - Modifying cookie banners

Mitigants	Risk of Mitigation
Remove all tracking technologies from your website	Large impact on user experience. Eliminates the good with the bad. Everybody loses.
Repurpose cookie banner with CIPA specific language, making it clear that tracking technologies are being used and information received is shared with 3rd parties.	Impedes user experience. This approach increases the size and intrusiveness of the pop-up cookie banner. Likely far more wordy than the average user would appreciate. Might create undue apprehension.
Adopt an opt-in model for all applicable tracking technologies.	Users often choose the path of least resistance. Having to opt in will place businesses reliant on this information at a disadvantage.
SB 690 summary: This bill would also exempt communication intercepts for a commercial business purpose from [CIPA]. The bill would define a commercial business purpose to mean the processing of personal information either performed to further a business purpose or subject to a consumer's opt-out rights. This bill contains other related provisions and other existing laws. (Based on text date 5/29/2025)	Failed legislative deadline, no action in 2025. Potential action in 2026 session.
Wait for a determinative court decision.	May parties find it cheaper to settle. In the meantime, you could be next.

PRESENTER: ALI BAIARDO, MCGUIREWOODS LLP

CIPA LITIGATION TRENDS



OVERVIEW OF CIPA LITIGATION

- In the past few years, Plaintiffs' firms have brought thousands of lawsuits and demand letters against companies that utilize online tracking devices.
- Plaintiffs allege liability based on CIPA's prohibitions against unauthorized wiretapping, eavesdropping, and use of pen register and trap and-trace devices.

OVERVIEW OF CIPA LITIGATION

- Technologies targeted by plaintiffs in CIPA suits include:
  - Tracking pixels
  - Session replay software
  - Cookies
  - Chatbots
  - Email tracking software
  - Cloud contact centers
- Significant statutory damages available: $5,000 per violation

VARIED RESULTS IN TRIAL COURTS

- *Ramos v. The Gap, Inc., No. 23-CV-04715-HSG, 2025 WL 2144837 (N.D. Cal. July 29, 2025)*
- *Shah v. Capital One Fin. Corp., 768 F. Supp. 3d 1033 (N.D. Cal. 2025)*
- *Mirmalek v. Los Angeles Times Communications LLC, No. 3:24-cv-01797-CRB, 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024)*
- *Lakes v. Ubisoft, Inc., No. 24-cv-06943-TLT, 2025 WL 1036639 (N.D. Cal. Apr. 2, 2025) (currently on appeal)*
- *Thomas v. Papa John's Int'l, Inc., No. 24-3557, 2025 WL 1704437 (9th Cir. June 18, 2025)*
- *Mikulsky v. Bloomingdale's, LLC, No. 24-3564, 2025 WL 1718225 (9th Cir. June 20, 2025)*
- *Gutierrez v. Converse Inc., No. 24-4797, 2025 WL 1895315 (9th Cir. July 9, 2025)*

PRACTICE POINTERS TO ENSURE COMPLIANCE

- Conduct a data map to identify all third-party tracking tools and any personal information collected/shared
- Document practices to show that systems and vendors do not access or use contents of user communications without consent
- Provide complete and accurate disclosure of use of tracking technologies in privacy policies.
  - Disclose what data will be collected by these tools, what parties have access to the data, and provide mechanism for users to opt out

PRACTICE POINTERS - CONSENT

- Utilize cookie banners to disclose tracking software and obtain affirmative consent
  - Two critical points here
    - (1) Obtain consent *before* the cookies and other tracking technologies are triggered
    - (2) Make sure the consent option complies with laws regarding internet agreements
  - Scrollwraps are best
    - At a minimum, have a clickwrap with a clear statement as to what the user is agreement

PRACTICE POINTERS

- Vendor management
  - Review contracts with third-party vendors to ensure compliance with privacy laws. Consider including indemnification clauses to mitigate risk
  - Implement routine audits of vendor practices
- Keep a record of the foregoing, especially as it relates to consumer consent

QUESTIONS OR COMMENTS?