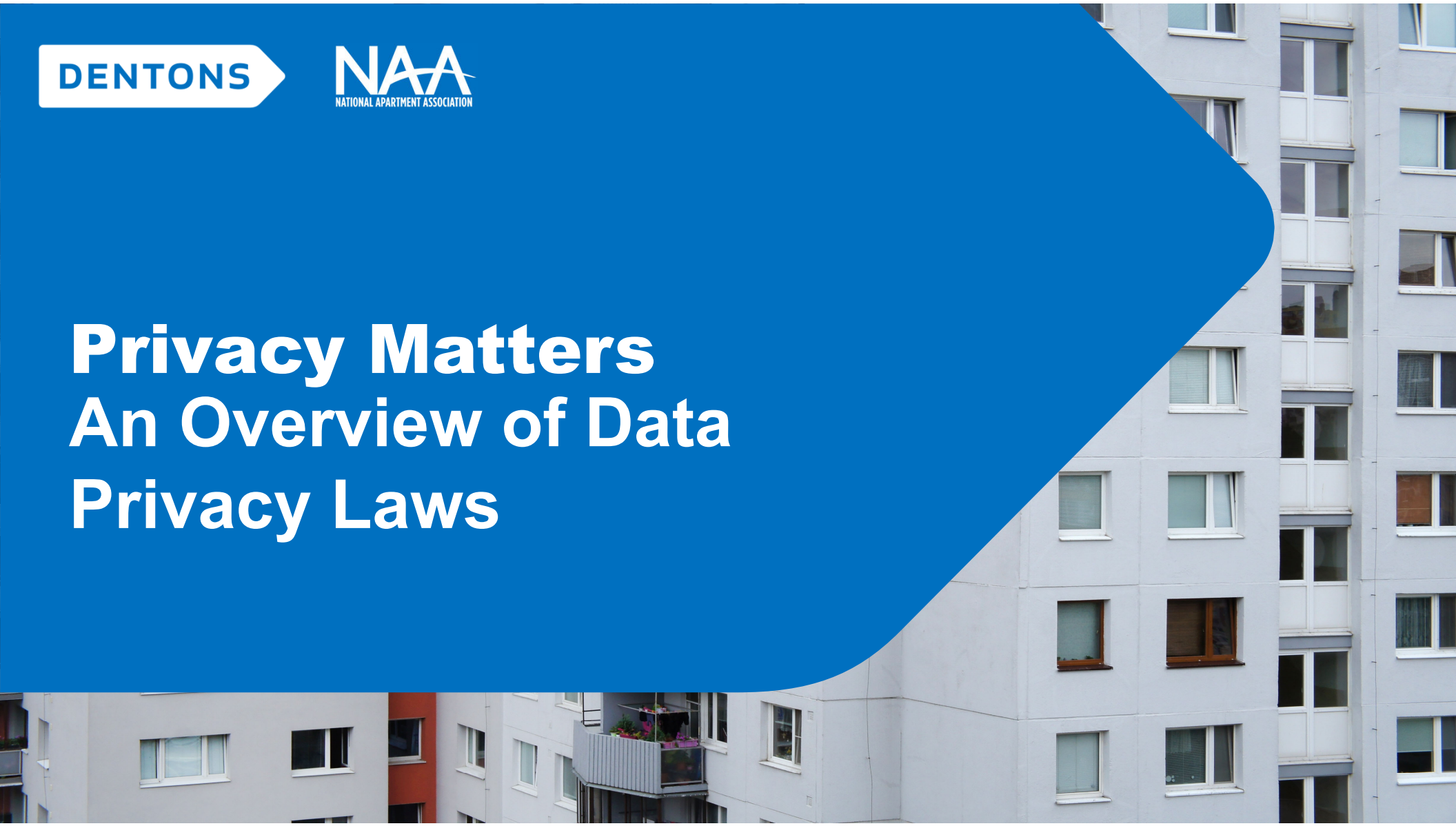
DENTONS

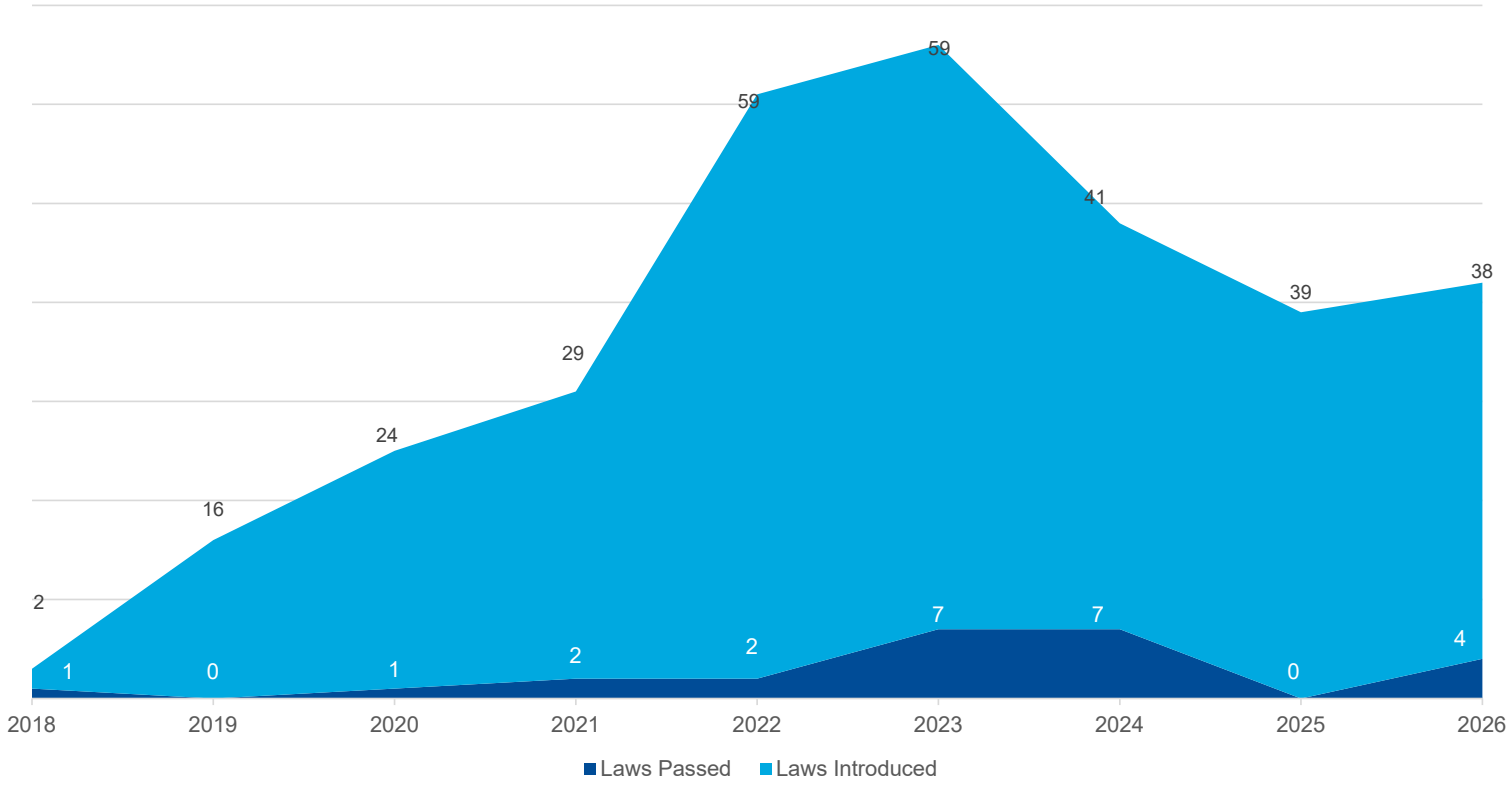
NAA
NATIONAL APARTMENT ASSOCIATION

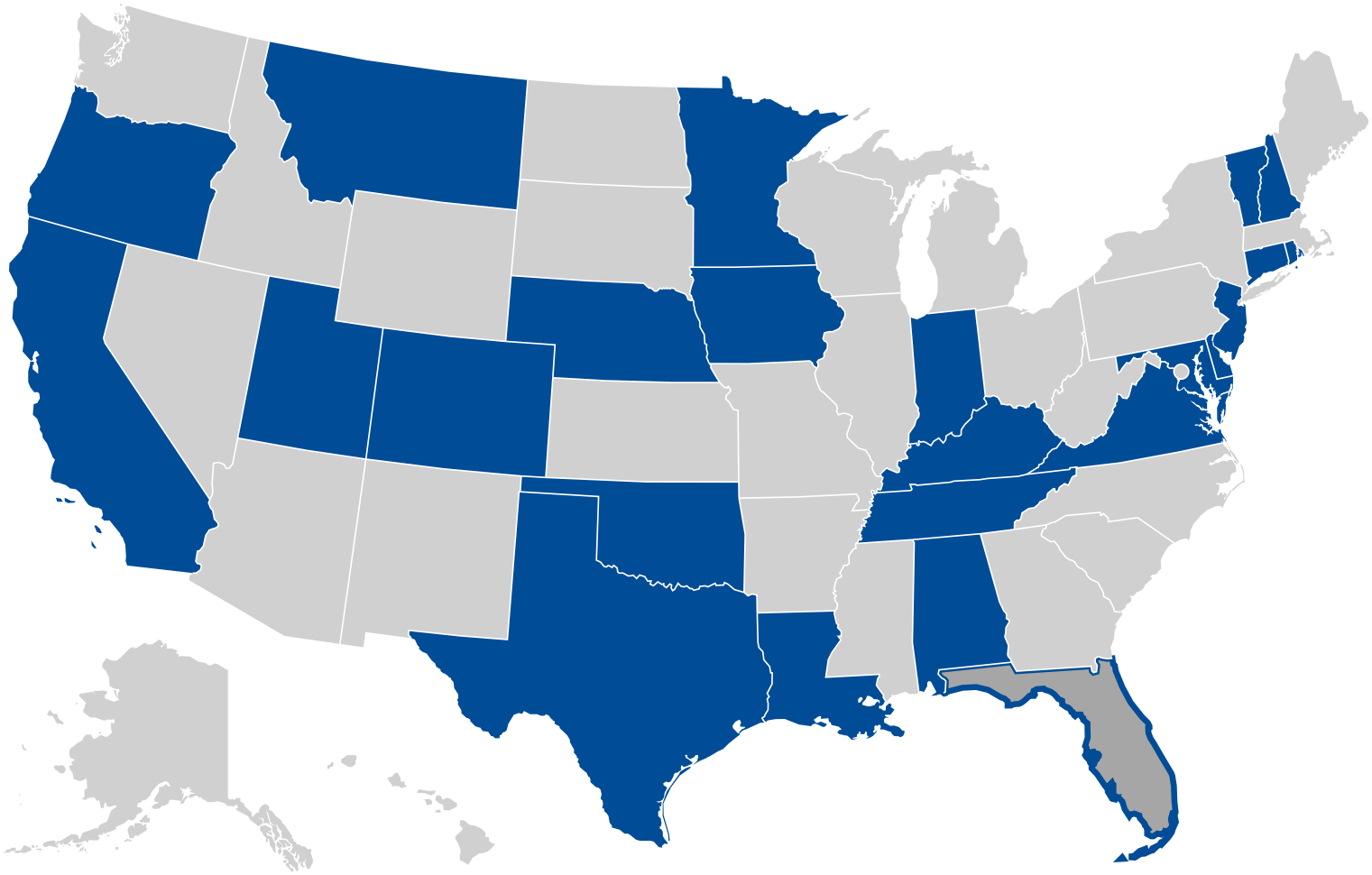
Privacy Matters
An Overview of Data Privacy Laws



Privacy Legislation

Growth of US State Comprehensive Consumer Privacy Laws



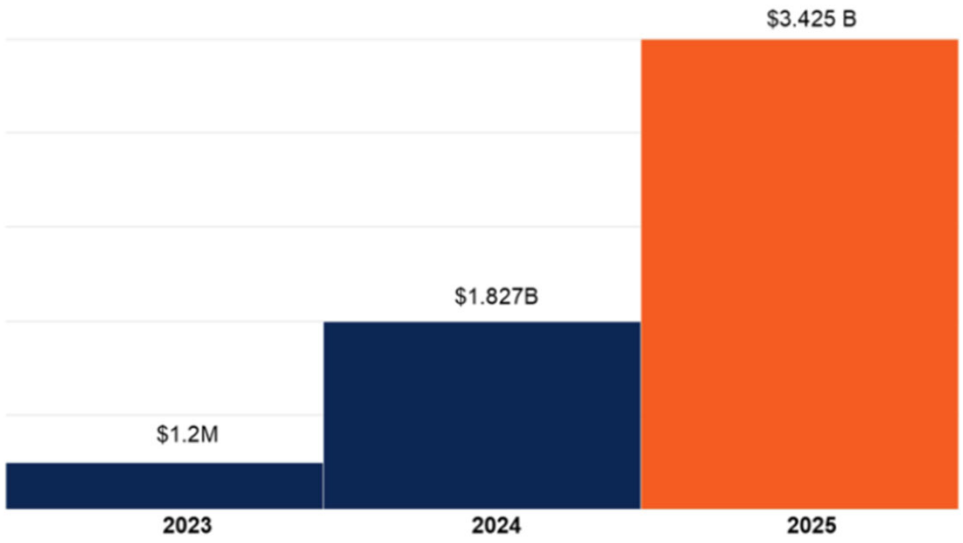


Gartner Estimates U.S. States' Privacy Fines Totaled $3.425 Billion in 2025; Trend Expected to Accelerate Through 2028

STAMFORD, Conn., April 28, 2026

In the U.S., More Fines Have Been Levied Due to Violations of Privacy Laws in 2025 Than the Five Years Prior Combined

Figure 1: U.S. State Privacy Fines — Annual Fines Cumulative

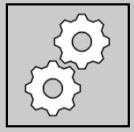


Source: Gartner (April 2026)

Thresholds

Jurisdiction	Data Subject Volume	Sales % Revenue + Volume
NE & TX	Any	Any % + Any
DE	≥ 10,000	> 20% + ≥ 5,000
CT	≥ 35,000	Any % + Any
VT	≥ 35,000	Any % + 3,000
CA	≥ 100,000	> 50% + Any
MD, & RI	≥ 35,000	> 20% + ≥ 10,000
NH	≥ 35,000	> 25% + ≥ 10,000
MT	≥ 25,000	> 25% + ≥ 15,000
AL	≥ 25,000	> 25% + Any
LA	≥ 75,000	> 50% + Any
CO & NJ	≥ 100,000	Any % + ≥ 25,000
MN & OR	≥ 100,000	> 25% + ≥ 25,000
IN, IA, KY, OK, UT, & VA	≥ 100,000	> 50% + ≥ 25,000
TN	≥ 175,000	> 50% + ≥ 25,000

Key Definitions



"**Processing**" is any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.



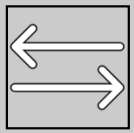
A "**Consumer**" is a natural person who is a resident of the state acting in an individual, personal, or household context. (Except California)

Key Definitions

Sensitive Data Categories

- Racial, National, or ethnic origin
- Religious or Philosophical beliefs
- Mental or physical health information
- Information on Sex Life
- Citizenship or immigration status
- Biometric identifiers
- Personal data of known child
- Precise geolocation
- Status as victim of crime
- Government-issued identification #
- Financial Information
- Union membership
- Contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication
- Genetic or Biological data (including neural data)

Key Definitions



“Sale” of personal data is “the exchange of personal data for monetary or other valuable consideration by a controller to a third party.”



“Third Parties” are a “natural or legal person … other than the consumer, controller, processor, or an affiliate of the processor or the controller.”

Definitions of Sale

Only Monetary Consideration	Monetary "or other valuable consideration"	
• Indiana • Iowa • Kentucky • Oklahoma • Tennessee • Utah • Virginia	• Alabama • California • Colorado • Connecticut • Delaware • Maryland • Minnesota • Montana	• Nebraska • New Jersey • New Hampshire • Oregon • Rhode Island • Tennessee • Texas • Vermont

California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations

by Practical Law Data Privacy & Cybersecurity

Published on 26 Aug 2022 • California

Related Content

The California Attorney General has settled an investigation arising from allegations that Sephora USA, Inc. violated the California Consumer Protection Act's (CCPA) notice and opt-out requirements for personal information sales in connection with using third-party tracking technology that enabled online behavioral advertising (OBA) and other third-party analytics.

Key Responsibilities

- Establish a **privacy governance** program with policies and procedures overseen by an officer;
- Abide by certain **conditions and prohibitions** when processing personal data;
- **Conduct risk assessments** with specific elements of analysis prior to particular personal data processing activities;
- Provide **public disclosures** containing statutorily required information;
- Execute complaint **contracts** with “Processors” containing statutorily required terms;
- Effectuate **Data Subject Right requests**.

Key Responsibilities

Privacy Governance

- **Universal:** establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect personal data.

- **Jurisdiction Specific Enhancements**
  - Montana, Colorado, California, Oregon: record retention schedules
  - California: Training for individuals handling Data Subject Right Requests.
  - Delaware: Third Party due diligence
  - Minnesota: description of policies (where applicable) for Privacy by Design, Data Subject rights, security controls, data minimization, purpose limitation, and violation remediation must have a named officer.

Key Responsibilities

Processing Conditions and Prohibitions (Processing Principles)

- Data Minimization: A Controller must limit the collection, use, disclosure, and retention of Personal Data to the minimum amount that is adequate, relevant, proportionate, and reasonably necessary for the specific purpose(s) for which the Personal Data is processed, as disclosed to the Consumer.
- Purpose Limitation: A Controller must not collect, use, retain, or disclose personal data in a manner that is not reasonably necessary for, proportionate to, and compatible with both (i) the processing purpose(s) originally specified to the Data Subject and (ii) the processing context, each as they existed at the time of collection, without the Data Subject's consent.
- Non-Retaliation: A Controller must not retaliate Consumer for exercising any of the Data Subject Rights afforded to the Consumer by Applicable Data Protection Law, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer (subject to some exceptions).

Key Responsibilities

Processing Conditions and Prohibitions (Processing Requirements)

- A Controller must have consent to collect, use, or disclose “sensitive” personal data.
- A Controller must have consent to process the personal data of a “minor” for targeted advertising, profiling for significant decisions, or “sale” without consent (age range for “minor” is between 13 and 18, depending on jurisdiction.
- A Controller must not “sell” “sensitive” personal data (MD & NJ, other jurisdictions only ban the sale of certain types of personal data, or require consent).

Key Responsibilities

Data Protection Impact Assessments: Triggering Conditions

- A data protection impact assessment must be conducted before processing “sensitive” data, or prior to processing personal data where the purpose is for targeted advertising, is a “sale,” uses ADMT, or presents a reasonably foreseeable risk of harm.
- This assessment must:
  - Characterize the context of the processing, such as the relationship between the controller and the consumer.
  - Identify benefits that may flow from the processing to the business, consumer, other stakeholders and public.
  - Identify potential risks to the rights of the consumer.
  - Identify safeguards that can be employed by the controller to reduce the risk (such as de-identified data).
  - Weigh the benefit against the mitigated risk and consumer expectations.

Automated decision-making Tech (ADMT)

California, Colorado, Connecticut (Employment), NYC (Employment)

Generally:

- ADMT broadly is a technology that processes personal data and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores, or other information that is used to make, guide, or assist a decision, judgment, or determination concerning an individual.

- ADMTs “materially influence” or “substantially replace”, depending on the state, human decision-making in a situation with potentially legally significant consequences.

ADMT

California, Colorado, Connecticut (Employment), NYC (Employment)

Generally:

- **Notice**
  - Public Posting
  - Point of Interaction Notice
  - Post-Adverse Outcome Disclosures
- **Consumer Rights**
  - Appeal Process
  - Opportunity for meaningful human review
  - Opportunity to request and correct data

Key Responsibilities

Privacy Notice: Sample Multi-Jurisdiction Structure

- Preamble: who is delivering the notice, and what are the scope restrictions (if any)
- Collection: what personal data is collected and how
- Use
  - General Use: how the categories of data collected are used.
  - Whether the Controller engages in Profiling for Significant Decisions
- Disclosure
  - Disclosures to Service Providers
  - Disclosures to “Third-Parties”
  - Disclosures that are “Sales”
- Retention (if applicable)
- “Your Privacy Choices”
  - Email, SMS, push notifications, etc.
  - Do Not Track
  - Information for California Residents (CCPA rights, “Shine the Light” Law disclosures if applicable, “Eraser Button” disclosure if applicable, etc.)
  - Data Subject Rights in Other Jurisdictions
  - Available Data Subject Right Mechanisms, Authentication, Responding to the Global Privacy Control (“GPC”), Authorized Agents
- Contact Information

Lessons Learned

Privacy Notices Must Be Accurate And Specific



- Connecticut AG penalized ticket marketplace for not having Connecticut-specific disclosures.
  - Statements like “you may have these rights, depending on where you live” are inadequate.
- CalPrivacy penalized vehicle manufacturer for vague and high-level disclosures.
  - Statements like “we may collect personal data from you about how you use our services” are inadequate.

Key Responsibilities

Data Subject Rights: Data Subject Request Mechanism

- Must have at least two “secure and reliable” Data Subject request mechanisms. Many jurisdictions require a Controller to accept opt-out of sale and targeted advertising requests via an Opt-Out Preference Signal (“OOPS”).

- The mechanism must consider:
  - The ways that consumers normally interact with the controller;
  - The need for secure and reliable communication;
  - The ability of the controller to authenticate the identity of the consumer making the request

Key Responsibilities

Data Subject Rights: Data Subject Requests



Access



Correction



Opt-Outs



Third Parties Receiving Personal Data



Deletion



Portability



Appeal



Limit Processing of Sensitive Data

Key Responsibilities

Data Subject Rights: Data Subject Requests



Profiling for Significant Decisions



Targeted Advertising



Sale of Data

Lessons Learned

Opt-Outs Must Be Honored Across All Systems



- Recent enforcement action from California penalizes media company for not honoring opt-outs across all platforms and technologies when an opt-out is received from an authenticated user.
- Nearly all enforcement actions include examples of misconfigured consent and opt-out mechanisms.

Enforcement
On The Rise

- **CPPA Enforcement Activity:** As of early 2026, the CalPrivacy has brought numerous enforcement actions. Key non-data-broker CCPA actions include:
  - Vehicle Manufacturer: $632,500 settlement (March 2025) for excessive identity verification requirements for consumer rights requests
  - Retail Brand: $345,178 fine (May 2025) for multiple CCPA violations including failure to honor opt-out requests
  - Retail Brand: $1.35 million settlement (September 2025) for ineffective opt-out mechanisms, failure to honor OOPS, inadequate disclosures, and deficient service provider contracts
  - Vehicle Manufacturer: $375,703 settlement (March 2026) for imposing unnecessary identity verification on opt-out requests

- **AG Enforcement Activity:** $2.75 million settlement with Family Entertainment Company (February 2026) for failing to honor consumer opt-out requests across streaming services and devices. Prior AG settlements include a retail cosmetics company ($1.2M, 2022), food delivery app, ($375K, 2024), and consumer health news organization ($1.55M, July 2025).
- **Joint Investigative Sweep:** In September 2025, CalPrivacy, California AG, and AGs of Colorado and Connecticut announced a coordinated investigative sweep focused on businesses' noncompliance with opt-out preference signals such as Global Privacy Control (GPC).
- **Investigative Priorities:** Opt-out mechanism functionality, GPC compliance, privacy policy accuracy and annual updates, service provider contract adequacy, and employee/applicant privacy notices.



DENTONS

NAA
NATIONAL APARTMENT ASSOCIATION

Thank you!

kyle.miller@dentons.com

dalton.cline@dentons.com