Cooley

PRIVACY TALKS

# CPRA and US State Privacy Laws: A Mid-Year Update on the Regulations and Compliance Approaches

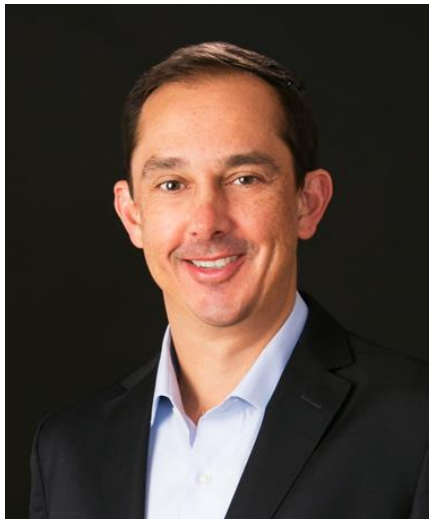
**Presented by:**

David Navetta, Partner

Christian Lee, Associate

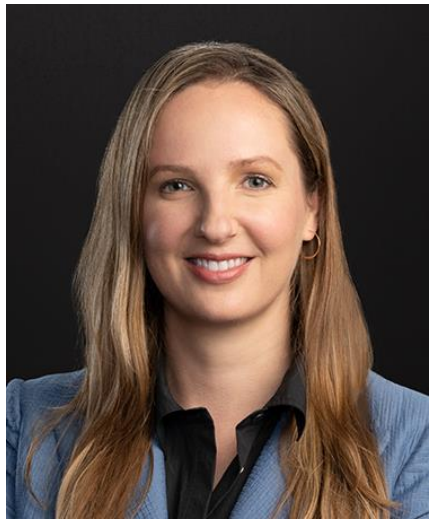
Claire (Blakey) Gibbs, Associate

# Presenters



**David Navetta**
**Partner**
**Denver, CO**
+1 720 566 4153
dnavetta@cooley.com

**Christian Lee**
**Associate**
**San Francisco, CA**
+1 415 693 2143
christian.lee@cooley.com



**Claire (Blakey) Gibbs**
**Associate**
**Washington, D.C.**
+1 202 776 2125
cmgibbs@cooley.com

# Agenda

- Overview of US State Privacy Law Environment
- Data Controller Obligations
- Consumer Rights
- Enforcement & Litigation
- Questions?

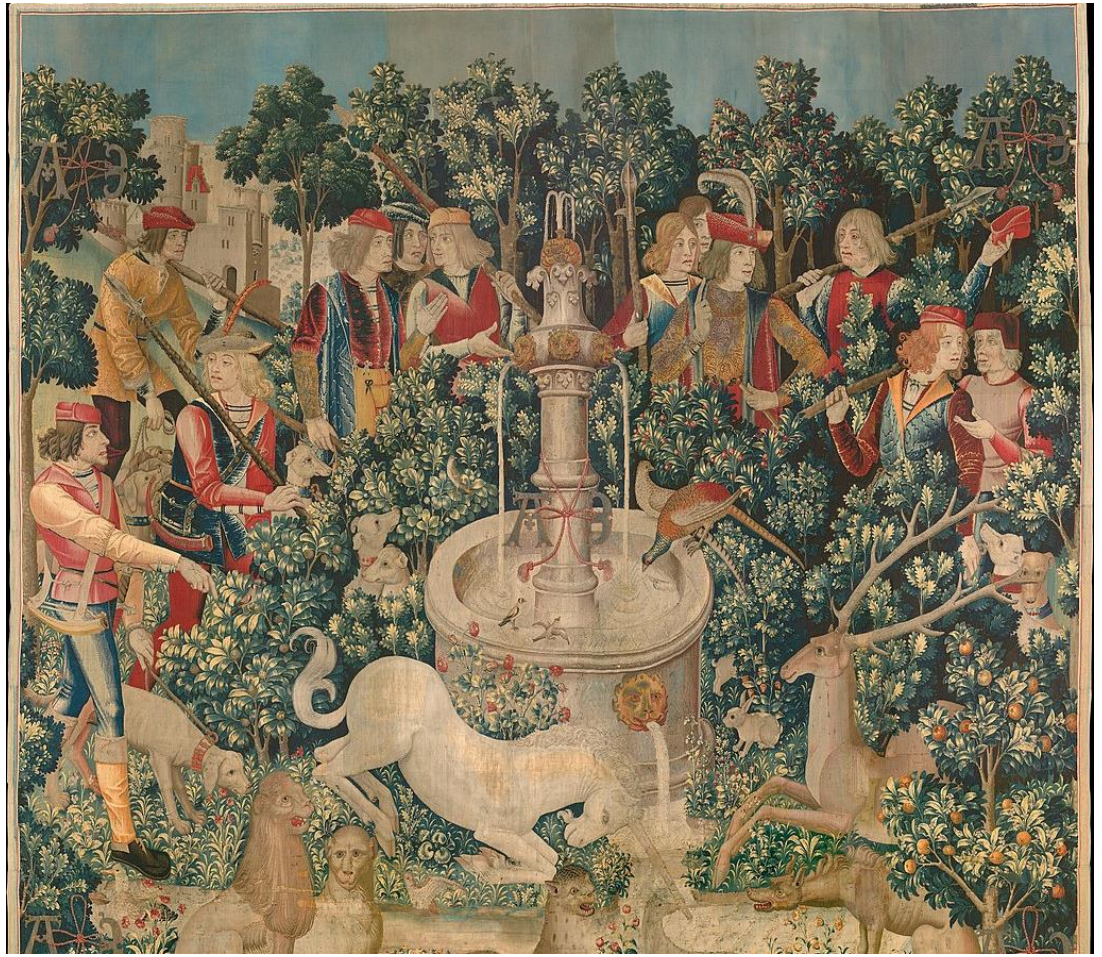
# Overview of U.S. State Privacy Law Environment

Cooley

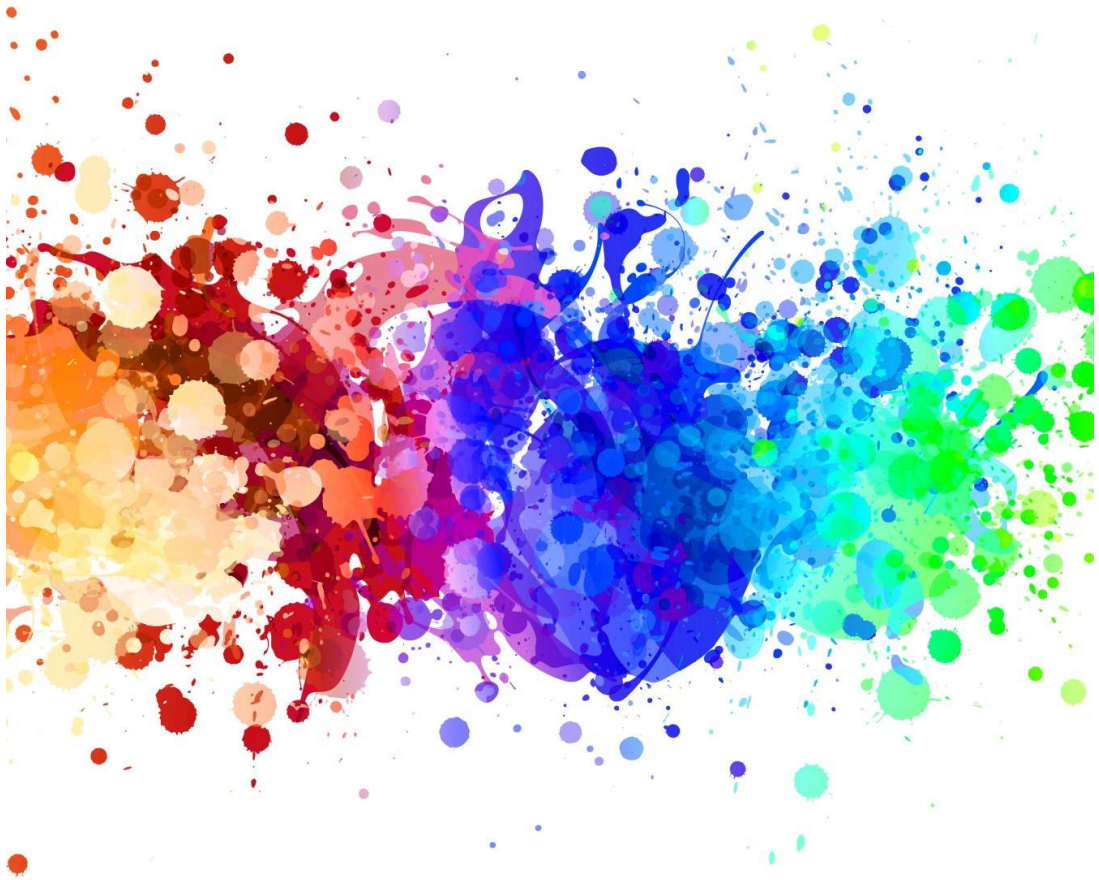
# Complex Tapestry of Privacy Laws

- More laws on national and global level
- More enforcement
- More class actions
- More advanced processing techniques (AI/ML)
- More crucial to success of business
- More valuable data and insights

**SPOILER ALERT**: It's much harder for companies to process PI and privacy laws are cutting to the core of some business models



# U.S. State Privacy Law Scoreboard



- **CCPA / California Privacy Rights Act –** effective Jan 1. 2023
  - Enforcement to begin July 1, 2023
  - Sole law that applies to HR and B2B data
- **Virginia Consumer Data Protection Act ("VCDPA") -** effective Jan. 1, 2023
- **Colorado Privacy Act ("CPA") -** effective July 1, 2023
  - Regulations finalized, also effective July 1
- **Connecticut Data Privacy Act ("CTDPA") -** effective July 1, 2023
- **Utah Consumer Privacy Act ("UCPA") -** effective Dec. 31, 2023

**Other enacted laws on horizon**: **Tennessee** (July 1, 2024); **Montana** (Oct. 1, 2024); **Iowa** (Jan. 1, 2025); **Indiana** (Jan. 1, 2026); **Florida** (July 1, 2023; July 1, 2024)

**Laws likely to be enacted**: **Texas** (3 new privacy laws, general, children's social media, and data broker bill)

# Regulatory Updates

## California's CCPA regulations

- Effective March 29, 2023; enforced July 1, 2023
- Explains what constitutes "disproportionate effort", an exemption for several data subject rights
- Provides different ways to comply with "sales"/"sharing" opt-out right (e.g., alternative opt-out link)
- Provides details on what constitutes an opt-out preference signal (e.g., GPC)
- Details what it means to process PI in a manner that is "reasonably necessary and proportionate" and consistent with "reasonable expectations" of consumers
- Matrixed disclosures for privacy policies
- *Rulemaking ongoing for cybersecurity audits; risk assessments; automated decision making*

## Colorado's CPA regulations

- Effective July 1, 2023
- Provides details on what constitutes a "universal opt-out mechanism"
- Establishes GDPR-style requirements for consent
- Establishes recordkeeping requirements for data subject requests
- Establishes standards and procedures for processing data subject requests (e.g., form of data provided, systems to search for data, responses to requester)

# More Sectoral / Topical Privacy Laws

- **Health / medical data privacy laws**
  - WA's My Health, My Data Act
  - CA's Confidentiality of Medical Information Act
  - NV SB-370 (passed legislature)
- **Financial privacy laws**
  - CA, VT, ND
- **Children's privacy laws**
  - CA's Online Eraser law
  - CA's Age-Appropriate Design Code Act
  - FL's Digital Bill of Rights
  - TX's HB 18, "Relating to the protection of minors…" (proposed)
  - MT's law banning TikTok
- **Biometrics laws**
  - IL BIPA; TX CUBI; WA HB 1493
- **Data broker laws**
  - CA & VT
- **Artificial intelligence and machine learning**
  - IL AI Video Interview Act; NYC Local Law 144 re use of AI in hiring
  - Upcoming: generative AI laws?

# Washington My Health/My Data

- Very broad healthcare data law that applies to non-traditional health-related entities and entities that have little to do with healthcare at all.
- Effective date:  partial July 23, 2023;  regulated entities March 31, 2024;  small businesses June 30, 2024
- Covers entities conducting business in WA or products products/services targeted to consumers in WA); no other thresholds
- HR and B2B exemption
- "**Consumer health data**" means PI that "identifies the consumer's **past, present, or future physical or mental health status**."

# Washington My Health/My Data Obligations

1. Maintain a consumer health data privacy policy (while not crystal clear, it appears that this privacy policy must stand on its own and be separated at some level from a regulated entity's other privacy policies).
2. Obtain opt-in "consent" for certain consumer health data collection and sharing activities.
3. Comply with data subject rights.
4. Maintain reasonable data security measures including a least-access privilege access restriction.
5. Enter into data processing agreements with processors.
6. Refrain from selling consumer health data without a "valid authorization."
7. Not implement a "geofence" around an entity that provides in-person health care services under certain conditions.
8. Private right of action – no statutory damages (must prove harm)

# California Age-Appropriate Design Code Act

## Scope

- Covers online services likely to be accessed by children
- "Child" means anyone under 18 years of age
- Covers information collected **about** children, not just from children (unlike COPPA)

## Compliance obligations

- Default privacy settings to a "high level of privacy"
- Consider the "best interests of children" over commercial interests
- List of prohibited activities, including
  - Using child's PI in a way that materially detrimental to the health or well-being of a child
  - Profiling by default
  - Collecting, sharing, or selling PI except as necessary
  - Collecting, sharing, or selling precise geolocation data by default
- Data Protection Impact Assessments and plans to mitigate/eliminate risks to children

# Data Controller Obligations

Cooley

# Controller or Processor …

- Depends on what you want to do with PI
  - Controllers determine the purpose(s) and means of the processing, while processors are generally limited to processing PI on behalf of a controller / pursuant to a controller's instructions
  - "Fact-based determination"
- **CA**: SPs must process for a "business purpose" pursuant to a written contract—cannot provide cross-context behavioral advertising services
- Note general exemptions (e.g., compliance with law)
  - **CCPA Regs** also specifically allow SPs to process PI to "build or improve the quality of the services" & "to prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity"

# Or Third Party?

- If you can't be a processor vis a vis a particular controller (or if you don't have a written contract as required by CCPA), then you are a "third party"
  - Exception: affiliates of a controller under **VA/CO/CT/UT** – not third parties

# Applicability Thresholds for “Controllers”

- **CA:** only law that can apply based only on $25M annual revenue
- **UT:** $25M revenue requirement in addition to data thresholds
- Data thresholds:
  - Process PI of **100K** residents during a calendar year; **OR**
  - ***CA:*** *Buy, “sell,” or “share” PI (not just “process”)*
  - Process PI of at least **25K** residents and derive:
  - **VA, UT:** more than **50%** of gross revenue from “sale” of PI
  - **CT:** more than **25%** of gross revenue from the “sale” of PI
  - **CO:** revenue or receive a discount on the price of goods/services from the “sale” of PI
  - ***CA:*** *50% of annual revenue from “selling” or “sharing” PI (no 25K requirement)*

# What is PI?

- **Definitions very similar** – any information that is linked or reasonably linkable to an identified or identifiable consumer
  - **CA:** gives examples; also includes households
- **New category of "sensitive" PI**
- "Consumer" under **VA/CO/CT/UT** excludes individuals acting in a commercial or employment context
- Don't forget general data exemptions (e.g., health data, NPI)
  - *Also*: entity-level exemptions & activities the laws do not apply to or restrict

# Privacy Policies / Notice(s)

- **CA** & **CO** have more detailed requirements and require "matrix" / "matching"
  → CA/CO-specific section? Or for all PI?
- **CA** also requires a "Notice at Collection"
  - At or before point of collection
  - Fewer content requirements than PP – but adds retention period/criteria (not explicitly required in PP)
  - Separate link required (in website footer/app settings menu) – market practice?
  - Not required if don't collect PI directly from consumers **and**: 1. don't sell PI; or 2. sell PI and register as a data broker
- **CA** & **CO** require Notice of Financial Incentives, if applicable (covered later)

# Data Minimization & Purpose Limitation

- **Data Minimization:**
  - **VA/CO/CT:** Collection of PI must be **adequate, relevant**, and limited to what is **reasonably necessary** in relation to the disclosed purposes for which the PI is processed
  - **CA:** Collection, use, retention, and disclosure of PI must be **reasonably necessary and proportionate** to achieve the purposes for which the PI was collected or processed **&** purposes must be consistent with the **reasonable expectations of the consumer**, unless obtain consent
- **Purpose Limitation** (aka duty to avoid secondary use):
  - **VA/CO/CT:** Cannot process PI for purposes that are **not reasonably necessary to or compatible with** the disclosed purposes, unless obtain consent
  - **CA**: Can only process PI for another disclosed purpose (other than the purpose for which the PI was collected/processed) if **1. reasonably necessary and proportionate** to achieve that purpose; and **2.** that purpose is **compatible with the context in which the PI was collected**, unless obtain consent

# Data Protection Impact Assessments (DPIAs)

- **CA:** Regulations pending re: "risk assessments" for processing that presents a "significant risk to consumers' privacy or security" – must be submitted to CPPA
- **VA/CO/CT (UT has no requirement):**
  - **Requirement:** Conduct and document a data protection assessment for processing activities that present heightened risk of harm
  - **Triggers include: 1. Sales** of PI; **2. Targeted advertising**; **3. Profiling** that could lead to reasonably foreseeable risk of certain harms to consumers; processing of sensitive PI; **4. Sensitive data**
  - **Content:** Only **CO** contains specific content requirements (in regs)
  - **Not retroactive:** Only applies to processing activities carried out on/after laws' effective dates

# Contractual Requirements

- **Controller/processor contracts** – all statutes require certain provisions
  - **CA:** technically, can't be a "service provider" without these provisions
- **Market approach** – cover VA/CO/CT/UT in body of data processing addendum
  - Add certain CA-specific terms in CCPA Appendix
- **Certain direct processor obligations** – controllers may want to add these
- **CA only** – also requires certain provisions in contracts with third parties

# Security Requirements

- **“Reasonable”** administrative, technical and physical data security measures to protect PI
  - Appropriate to volume/nature of PI
- **CA:**
  - Ties reasonable security to the “CIS Top 20” controls
  - Regs pending re: **annual cybersecurity audits** for processing that presents significant security risk (factors: size/complexity of business and nature/scope of processing activities)

# Consumer Rights

Cooley

# Right to Know & Access / Portability

- **Right to Know**
  - **CA:** Right to request disclosure of the categories of PI a business has collected about that consumer, the categories of sources from which the PI is collected, the business or commercial purpose for collecting, selling, or sharing PI, and the categories of third parties to whom the business discloses PI
  - **VA/CO/CT/UT:** Right to confirm whether a controller is processing the consumer's PI
- **Right to Access/Portability**
  - **CA**: Right to request disclosure of the specific pieces of PI in a readily useable and transmittable format
  - **VA/CO/CT/UT:** Right to copy of the consumer's PI in a portable and, to the extent technically feasible, readily useable and transmittable format

# Right to Correct & Delete

- **Right to correct**
  - All laws **except UT** give residents the right to correct inaccuracies in the consumer's PI (taking into account the nature of the PI and the purposes of the processing)
- **Right to delete**
  - All laws give residents the right to request the deletion of their PI
  - **CA, UT**: limited to PI collected from/provided by the consumer
  - Subject to a number of exceptions (**CA, CO**)

# Implementation & Exemptions

- Implementation
  - Disclose rights in privacy policy
  - How broadly to honor requests?
- Exemptions
  - Not all exemptions apply to all requests (**CA** most prescriptive)
  - General v. specific exemptions

- Examples of exemptions
  - Verification of identity
  - Frequency/excessive requests
  - Sensitive PI
  - Unstructured information
  - “Disproportionate effort”
  - Legal/contractual need to retain personal information
  - Internal use
  - Crime/fraud
  - Research

# Right to Opt Out of Sale / Sharing / Targeted Advertising

- All laws give residents the right to opt-out of "sales" and "sharing" (**CA**) / the processing of PI for "targeted advertising" purposes (**VA/CO/CT/UT**)
- Exception – children. Opt-in to sales and sharing / targeted advertising for children under 16 (**CA**) or 13-16 (**CT**)
- Also note general opt-in for processing PI of known child (under 13) in **VA/CO/CT**
  - **UT:** opt-in for processing *sensitive PI* concerning a known child (under 13)

# What Is a "Sale?

- **CA:** "Selling, renting, releasing, **disclosing** disseminating, making available, transferring … a consumer's **PI** by the **business** to a **third party** for monetary or other valuable consideration."
- **VA/CO/CT/UT:** "Exchange of **PI** for monetary [**CO, CT**: or other valuable] consideration by a **controller** to a **third party**."

Does not include:

1. Directed disclosures (i.e., consent) [**CA, CT, UT**] / To fulfill consumer request [**VA/CO/CT/UT**] / Consistent with consumer's reasonable expectations [**UT**]
2. M&A context [**all**]
3. Disclosures to affiliates [**VA/CO/CT/UT**]
4. Where consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience [**VA, CT, UT**]
5. Disclosures necessary to implement opt-outs [**CA**]

# “Sharing” vs. Processing PI for “Targeted Advertising”

- **Sharing**: Disclosure of PI by business to 3P for **CCBA**
- **Cross-context behavioral advertising**: Targeting of advertising to a consumer based on the consumer’s PI obtained from the consumer’s activity across businesses, distinctly branded websites, apps, or services *other than* the business, distinctly branded website, app, or service with which the consumer intentionally interacts.

**CA**

- Targeted advertising: Displaying advertisements to a consumer where the advertisement is selected based on PI obtained from that consumer’s activities over time and across nonaffiliated websites or online apps to predict such consumer’s preferences or interests.

**VA/CO/CT/UT**

# Implementation of Opt-Out Right

- **Notice of Right to Opt-Out**
  - Description of right to opt-out of sale/sharing
  - Instructions on how to submit an opt-out request (& interactive form by which consumer can submit request online)
- **"Do Not Sell or Share my Personal Information" link [CA]**
  - Conspicuous link on website homepage (footer)
  - Must immediately effectuate right to opt out or direct consumer to Notice to learn about and make choice
  - Alternative link [**CA**]**:** single opt-out link allowing users to opt-out of 1) sale/sharing and 2) certain uses/disclosures of sensitive PI (if applicable) – "Your Privacy Choices" (or "Your California Privacy Choices")
- **CO:** link examples: "Your Opt-Out Rights," "Your Privacy Choices," etc.

# Universal Opt-Out Mechanism

- **Opt-out preference signals** – allow consumers to opt-out with all businesses they interact with online without having to make separate requests
  - Mandatory for **CA** (**CO** starting July 1, 2024; **CT** starting Jan. 1, 2025)
- **Privacy Policy** – should explain that you recognize opt-out signals (and any limitations)
- **"Global Privacy Control" (GPC)** – https://globalprivacycontrol.org/
- **CO:** To release a list of approved opt-out mechanisms by Jan. 1, 2024
  - Controllers have 6 months to recognize a mechanism added to the list

# Right to Opt Out of Profiling

- **What Is "Profiling"?** Any form of automated processing of PI to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, performance at work [**CA only**], health, personal preferences, interests, reliability, behavior, location, or movements.
- **VA, CO, and CT** currently provide their residents the **right to opt out of "profiling"** in furtherance of [**CT**: solely automated] decisions that produce legal or similarly significant effects concerning the consumer.
- **CA:** preliminary rulemaking has begun for regulations governing access and opt-out rights.
- **UT** does not provide this right.

# Rights Regarding Sensitive Personal Information (SPI definition)

- Racial or ethnic origin, religious [or philosophical] beliefs, mental or physical health diagnosis [or: history/condition/treatment], sexual orientation [or sex life], or citizenship or immigration status
- Genetic or biometric data
- Precise geolocation data (specific distance reference – 1,750/1,850 ft)
- PI collected from a known child under 13 [**VA, CO, CT only**]
- **CA only**: 1) social security, driver's license, state identification card, or passport number; 2) account log-in, financial account, debit card, or credit card number; 3) union membership; 4) contents of mail, email, and text messages (unless the business is the intended recipient)

# Rights Regarding Sensitive Personal Information

- **CA:** Right to limit certain uses/disclosures of SPI
  - To that which is necessary to provide goods/services reasonably expected by an average consumer who requests such goods/services, or for: service delivery and operations, compliance and protection, research and development, or service improvement and analytics purposes
  - Exception: if SPI not collected/processed to infer characteristics about a consumer
- **UT:** Generally, right to opt-out of processing SPI
- **VA, CO, CT:** Must obtain consent before processing SPI
  - **CO**: Exception for adult SPI where 4 criteria are met

# Right to Non-Discrimination (& Financial Incentives)

- Cannot discriminate against a consumer because the consumer exercised any of their rights, including by:
  - Denying goods or services;
  - Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; or
  - Providing a different level or quality of goods or services to the consumer.
- **Except if:**
  - **VA/CO/CT/UT:** related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program **or** (except CO) if consumer has exercised opt-out right
  - **CA:** "reasonably related to the value of the consumer's data"
  - **CA/CO** also require Notice of Financial Incentive (and for **CA**, must obtain consent)

# Enforcement & Litigation

Cooley

# Sephora

- Only CA AG enforcement action on CCPA
- Failed to 1) disclose to consumers that it was selling their PI and 2) process user requests to opt-out of sale via Global Privacy Control (GPC)
- Did not cure these violations within the 30-day period (now expired)
- Required to pay $1.2 million in penalties

# CA AG Enforcement Sweeps

- Online retailers (incl. Sephora) that allegedly failed to comply with, or do not provide a mechanism for, requests to opt out of sales
- Businesses operating loyalty programs that offered financial incentives such as discounts, free items, or other rewards, in exchange for PI without providing consumers with a notice of financial incentive
- Businesses with mobile apps in the retail, travel, and food service industries that allegedly failed to comply with, or do not provide a mechanism for, requests to opt out of sales and authorized agent requests
- July 1, 2023 is the official start of enforcement

# Class Action Litigation Boom

**Literally hundreds of privacy class actions involving:** BIPA (biometric data), VPPA (Meta pixel), Wiretapping laws (session replay and chatbots), and TCPA (text messaging)

- Companies are often being sued based on their vendor or partner's processing activities (e.g., VPPA and session replay)
- **Common thread: statutory damages**
- Privacy class action settlements in 2022: **$896.7 million, a jump of 40.5%***

**Data breach class actions**

- Hundreds of class actions filed each year (a lawsuit a day per trackers)
- *Hajny v. Volkswagen Grp. of Am. Inc.*: Settlement of over $4.5M in connection with claims that Volkswagen violated, among other laws, the CCPA when it failed to protect customer data, leading to a data breach of driver's license numbers, Social Security numbers, payment card data, and other sensitive data categories.
- *Mehta v. Robinhood Financial LLC*: Settlement of $20M for violations of CA law, including CCPA, in connection with data breach affecting 40k users of the Robinhood trading platform.
- Data breach class actions settlements in 2022: **$719.21 million, a 46% increase***

# Questions?

Cooley