

CCPA Workshop

Mike Hintze

Partner, Hintze Law PLLC

Joanne Charles

Associate General Counsel
Gilead Sciences

Courtney Manzel

Corporate Counsel, Privacy & Data
Governance, Volkswagen Group of America

Speakers



Mike Hintze

Partner
Hintze Law PLLC



Joanne Charles

Associate General Counsel
Privacy & Data Ethics
Gilead Sciences



Courtney Manzel

Corporate Counsel
Privacy & Data Governance
Volkswagen Group of America

- Background: Where Are We & How Did We Get Here?
- CCPA Overview (scope, applicability, general principles)
- Consumer Rights (rights of access, correction, and deletion)
- Sensitive Personal Information (right to limit)
- Data Selling and Sharing (right to opt-out)
- Implementing Rights and Choices (processes, “dark patterns,” GPC)
- Notice Obligations
- Risk Assessments
- Other Obligations on Businesses (data minimization, security)
- Service Provider, Contractor, and Third Party Agreements
- Employee (and B2B) Data
- Enforcement Update
- Looking Forward / What's Next

Background: Where Are We and How Did We Get Here?

2018 – 2024: A Moving Compliance Target



- **June 2018:** CA Legislature passed, and Governor signed, CCPA
- 2018 – 2019: Legislative amendments
 - **September 2018:** largely technical corrections
 - **October 2019:** five bills with substantive changes
- **October 2019:** Attorney General published initial proposed regulations
- January 2020: CCPA came into effect
- Modified versions of draft AG regulations published in **February & March 2020**
- **June 2020:** CCPA regulations finalized (the AG regulations)
 - Subsequently amended in **August, October, and December 2020.**
- July 2020: CCPA enforcement begins
- **November 2020:** CA voters pass the “California Privacy Rights Act” (CPRA) amendments to the CCPA
- **July 2022:** CPPA publishes proposed regulations under CPRA amendments
- **November 2022:** CPPA issues modified draft regulations
- January 2023: CPRA amendments come into effect
- **March 2023:** Final CPPA regulations issued
- **September 2023:** CPPA issued discussion draft of regulations on cybersecurity audits, risk assessments, & automated decision making
- **March 2024:** Revised drafts of proposed regulations released

CCPA Overview

- Broad application to any entity that “does business in California” and satisfies one or more of the following:
 - \$25,000,000 in annual gross revenue
 - Buys, sells, or shares data on 100,000 California residents or households annually
 - Derives 50% or more of revenue from selling or sharing personal information
- Applies to both online and offline data collection
- Broad definition of personal information: any information relating to an identifiable person, household [or device]
- Definition of “consumer” includes any California resident. Includes both consumers and B2B contacts.
- Exempts certain data or entities covered by other privacy laws
 - Protected health information covered by HIPAA (and the California equivalent)
 - Personal information covered by the Gramm-Leach-Bliley Act (and the California equivalent)
 - Certain information covered by the Fair Credit Reporting Act
 - Personal information covered by the Driver’s Privacy Protection Act

Key Principles and Requirements

Wide ranging consumer rights

- Access, portability, correction, deletion,
- Opt-out rights for sale/sharing and sensitive data [& automated decisionmaking]
- Detailed implementation requirements, including verification, use of agents, global privacy control, etc.

Contracting requirements for service providers, etc.

Detailed and extensive notice requirements

Data minimization (collection and retention)

Data security

Risk assessments and cybersecurity audits



Calif. & Other States: Consumer Rights

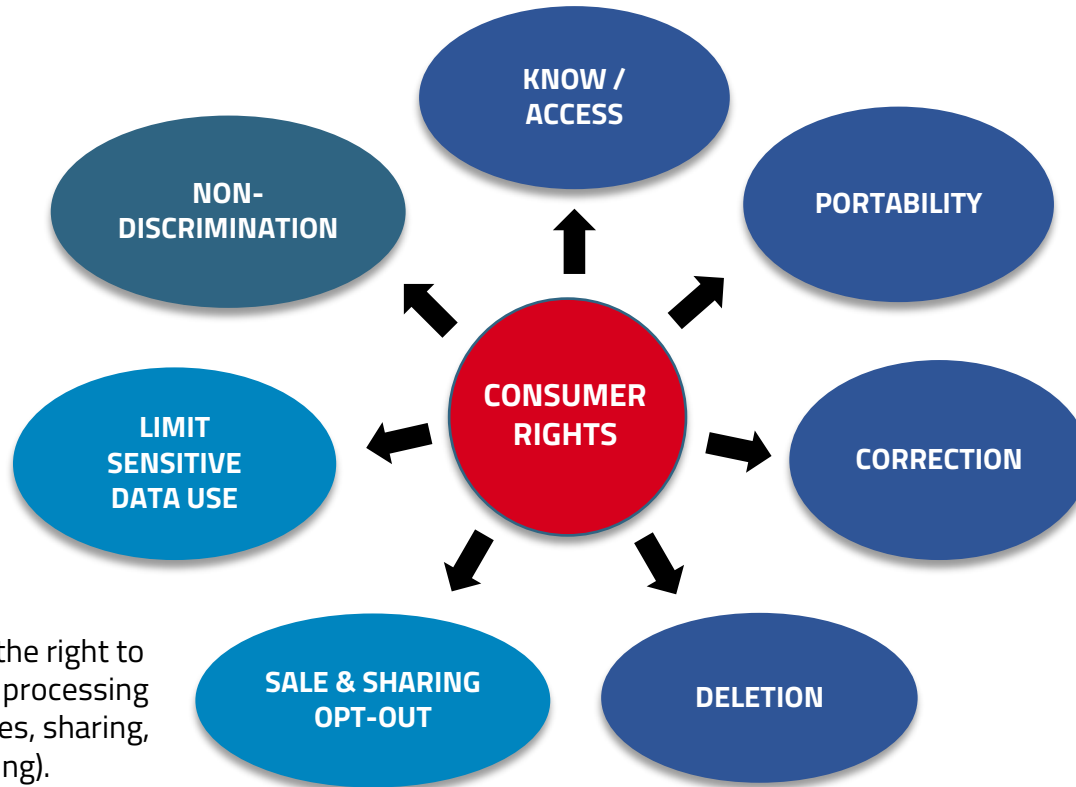
State	Rights of access & portability	Right of correction	Right of deletion	“Sale” opt-out	Targeted ads opt-out	Profiling w/ significant effect opt-out	Sensitive personal data	Secondary use consent
California	Yes	Yes	Yes	Broadly defined	Yes*	Yes (future rulemaking)	Opt-out for secondary use of sensitive personal info	
Virginia	Yes	Yes	Yes	Narrowly defined	Yes	Yes	Opt-in	Opt-in
Colorado	Yes	Yes	Yes	Broadly defined	Yes	Yes	Opt-in	Opt-in
Connecticut	Yes	Yes	Yes	Broadly defined	Yes	Yes	Opt-in	Opt-in
Utah	Yes	No	Yes	Narrowly defined	Yes	No	Opt-out	N/A

Calif. & Other States: Other Requirements

State	“Dark patterns” prohibited	Global Privacy Control	Collection limitation	Risk assessment	Employee & B2B data covered	Private right of action
California	Yes	Yes	Yes	Yes	Yes	Limited (security breach)
Virginia	No	No	Yes	Yes	No	No
Colorado	Yes	Yes	Yes	Yes	No	No
Connecticut	Yes	Yes	Yes	Yes	No	No
Utah	No	No	No	No	No	No

Consumer Rights

Overview of Consumer Rights



Special rules attach to sensitive PI: Opt-in in CO/VA/CT; limit use in CA; opt out in UT.

Consumers have a right to correct inaccurate or incomplete personal info

Consumers have the right to opt out of certain processing activities (e.g., sales, sharing, targeted advertising).

1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

- (1) The categories of personal information it has collected about that consumer.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting, selling, or sharing personal information.
- (4) The categories of third parties to whom the business discloses personal information.
- (5) The specific pieces of personal information it has collected about that consumer.



The right to know includes a consumer's right to receive individualized disclosure about the categories information a business collected, disclosed or sold about them (Categories Report), plus the right obtain to a copy of the actual information you collected about them (Specific Pieces Report; portability).

- **Verification of consumer**
- **Redactions of certain sensitive data (ex: SSN)**
- **Company-specific considerations**

Correction

- Consumers have a right to request that a business correct inaccurate personal information
- “Taking into account the nature of the personal information and the purposes of the processing of the personal information.”
- Business must use “commercially reasonable efforts” to correct inaccurate information upon request (and provide a Specific Pieces report, upon request)
- Same requirements as access and deletion requests for methods of submitting requests, verification, and response.
- Most exceptions that apply to access and deletion also apply to correction.
- Resolving questions re accuracy of data = “totality of the circumstances”
- Reasons for denial

Right to Deletion under CCPA

- Verification, timeframe for response
- Exceptions include exempt information, unable to verify consumer, information needed to complete transaction or provide service or for uses compatible with reasonable customer expectations, legal compliance...
- Must inform third parties of the consumer's delete request, require service providers to inform their subprocessors



California – only state that permits agent to make all DSRs

- Verification of agency
- Limits/requirements imposed directly on agents
- Operational challenges



Sensitive Personal Information

What is Sensitive Personal Information?



*Sensitive PI typically does **not** include:*
1) any information that is publicly available or
2) otherwise sensitive information collected
without inferring characteristics about the
consumer (if you say so in your policy).

- Social security, driver's license, state ID, or passport number;
- Consumer's account log-in, financial account, debit card, or credit card numbers;
- Precise geolocation;
- Racial or ethnic origin;
- Religious or philosophical beliefs, or union membership;
- Contents of mail, email and text messages (unless the business is the intended recipient of the message);
- Genetic or biometric information;
- Personal information collected and analyzed concerning a consumer's health; and
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

- Disclose categories of sensitive PI, purposes for which it is collected, and whether it is sold or shared
- Do not use sensitive PI for incompatible purposes or collect additional sensitive PI without notice
- Right **to limit use** of sensitive PI to that use which is necessary to perform services or provide goods “reasonably expected by an average consumer who requests such goods or services,” to perform certain business purposes, or authorized by regulation (can be bundled with other opt outs)
- *But, sensitive PI that is collected or processed “without the purpose of inferring characteristics about a consumer” is not subject to the opt out obligation*

Data Selling and Sharing

Selling and Sharing: What's the Difference?

Transferring, making available, or otherwise communicating, through any means, a consumer's personal information by the business to a third party...

SELL

for monetary or other valuable consideration

SHARE

for cross-context behavioral advertising, whether or not for monetary or other valuable consideration

“Share” was added by the CPRA amendments to make it clear that targeted advertising cannot escape the opt-out requirements through a “sale” loophole (real or perceived)

Businesses must:

- Disclose sharing and selling in privacy notices and in response to right to know requests
- Provide opt-out for sharing and selling



Is every “share” also a “sale”?

- And if so, what does that mean for your disclosures and opt outs?

What can a service provider do (and not do)?

What is (and what isn't) cross-context behavioral advertising for which companies can't be service providers?

How to effectuate opt outs, including:

- Where does an opt out attach to a person vs. a device?
- How to do opt outs on mobile apps/intersection with device controls

How to handle automated opt outs/GPCs

Implementing Rights and Choices

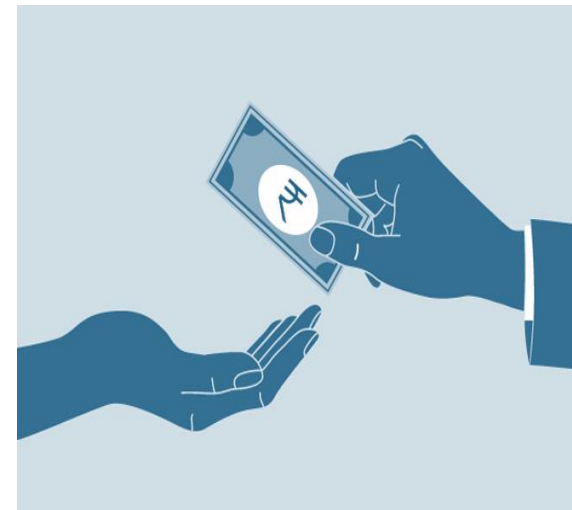
Businesses cannot discriminate against consumers who choose to exercise their rights under the law. When a consumer submits a request to know, correct, delete, opt-out, or limit sensitive info, the business cannot:

- ❑ Deny the consumer goods and/or services
- ❑ Charge the consumer a different price for the goods and/or services—including the use of discounts or through the use of penalties
- ❑ Provide for the consumer with a different level of quality of their goods and/or services

Except maybe they can ...

Loyalty & Financial Incentive Programs

- Generally, companies are allowed to offer a different price, rate, level, or quality of goods or services if price difference is ***reasonably related to the value of the personal information*** collected, used, or disclosed.
- Non-discrimination provisions do not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs.
- Specific obligations on “financial incentive” programs (mostly found in the regulations), including specific notice obligations.



Avoiding “Dark Patterns”

- Consent obtained through use of a “dark pattern” is not valid
- Defined as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation”
- Is this broader than, for example, FTC Act Section 5 “unfair” or “deceptive”?
- Does the prohibition apply only where “consent” is required (e.g., where a consumer has exercised an opt-out choice and subsequently opts back in) or more broadly?

Time limits

- Businesses must acknowledge receipt of the request to know/access within 10 days and have **45 days** to comply. This can be extended for an additional 45 days when reasonably necessary, provided the consumer is notified before the original 45-day period has lapsed.
- A business must respond to the consumer's request to opt out as soon as possible, but no later than **15 business days** from the date the request is received.

Verification

Under the CCPA, businesses must create effective processes to verify the identity of persons who submit consumer requests relating to rights to know/access or delete or a request to limit use of personal information. Businesses may require consumer authentication that is reasonable depending on the nature of the personal information requested, such as requiring consumers to submit requests through an existing account with the business if one already exists.

In April 2024, a CPPA Enforcement Advisory reminds businesses that the CCPA prohibits them from requiring consumers to verify their identity or collecting additional information to opt out of sale/sharing or to make a request to limit.

Authorized agents may submit requests on behalf of consumer. Businesses may require the following before complying with a request from an “authorized agent”

- the authorized agent to submit a written and signed permission with the request to know or delete;
- the consumer to directly verify their identify with the business; and
- the consumer to directly confirm with the business that they provided the authorized agent permission to submit the request. Without proof, the business may deny the request.

Other state comprehensive laws provide consumers with the right to appeal a denial of a consumer's request for access or deletion, however, there is **no comparable right to appeal in California.**

Universal Choice Mechanisms: What Are They?

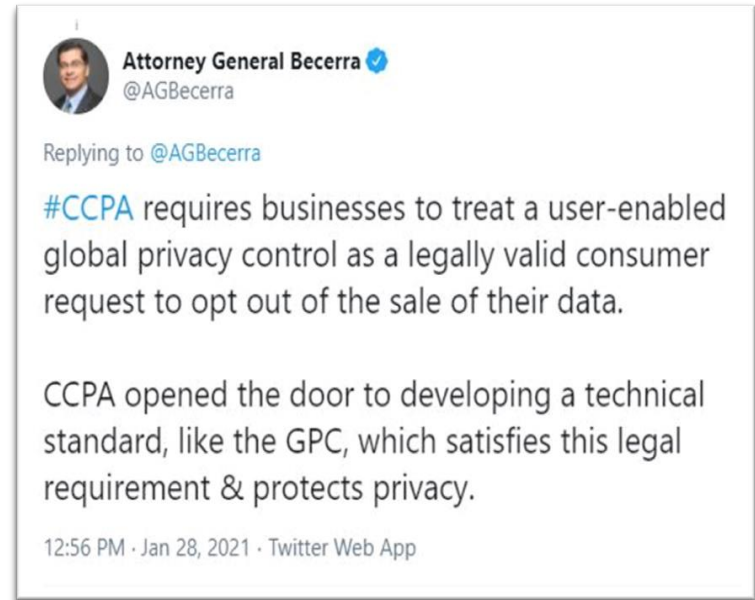
CCPA requires businesses to treat an “opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism” as a valid consumer request.

CCPA Regulations provide that a valid signal must:

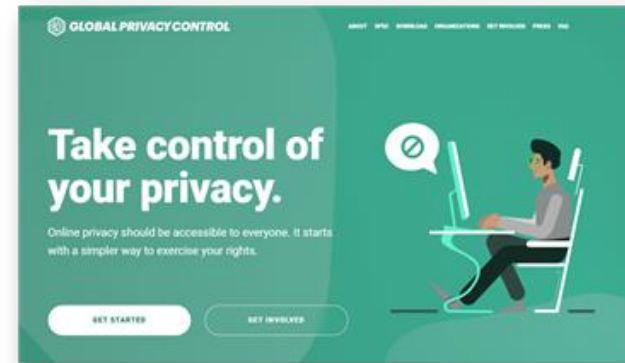
- Be in a commonly used and recognized format, such as an HTTP header field or JavaScript object.
- Make clear to the consumer, whether via configuration or disclosures to the public, that the signal is intended to opt the consumer out of the sale and sharing of personal information.

Is the “Global Privacy Control” the only valid signal today?

Other states (e.g. CO and CT) also require adherence to universal opt out mechanisms regarding sales, sharing, or targeted advertising. Like CA, the CO regulations include technical details.



- In California, businesses must honor GPC signals for sale/sharing
 - Signal can be overridden with consumer consent
 - For signed in users, must apply the opt-out preference at the account level
 - If implement OOPS in a “frictionless” manner (and meet certain other requirements), the homepage “do not sell/share” link becomes optional
- Does the signal apply to the right to the “limit the use of sensitive personal information” choice ?
- Other states:
 - CO: Starting July 2024, must honor signals as an opt out of data sales and targeted advertising. See Colorado rulemaking.
 - CT: Starting January 2025, must honor signals as an opt out of sales, targeted advertising, and profiling w/ legal or similarly significant effects.



Notice Obligations

CCPA includes several different notice obligations

- “Privacy Policy” – the general notice documents that includes a long list of required disclosures
- “Notice at Collection” – a (mostly) subset of the required disclosures that must be linked to from the point of collection
- “Notice of Financial Incentive” – specific disclosures of financial incentives or price/service differences connected to the exercise of consumer rights
- “Notice of Right to Opt-out of Sale/Sharing” – required disclosures at the time of exercising the opt-out right
- “Notice of Right to Limit” – required disclosures at the time of exercising the right to limit the use or disclosure of sensitive personal information

Privacy Policy must contain:



- The categories of personal information (including sensitive personal information) to be collected and/or have been collected.
- The categories of sources from which the personal information is collected.
- The purposes for which the categories of personal information are collected, used, and/or shared/sold.
- The categories of third parties with which the business discloses personal information.
- The categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months, or a statement that it has not disclosed personal information for a business purpose in the preceding 12 months.
- The categories of personal information it has shared/sold about consumers in the preceding 12 months, or a statement that it has not shared/sold personal information in the preceding 12 months.
- A description of a consumer's right to request certain specific information from the business and access the personal information collected
- A description of the consumer's right to request correction or deletion of personal information
- The right to opt-out from the sharing/sale of personal information, along with a link to a "Do Not Share or Sell My Personal Information" page where the consumer can exercise that right.
- Right to limit use and disclosure of sensitive personal information, along with the link...
- The designated method(s) for submitting requests, including opt-out preference signals
- A statement of a consumer's right to not be discriminated against for exercising the rights set out in the Act.
- Data retention (unless addressed in sperate Notice at Collection)

The CCPA doesn't stand alone: Like Shine the Light, it requires businesses to respond to requests to disclose with which third parties they are sharing personal information. And like CalOPPA, it requires businesses to provide consumers notice about the personal information they collect and share with third parties.

- Must provide a Notice at Collection at or before time of data collection
- Notice at Collection must disclose:
 - The categories of personal information and sensitive personal information to be collected,
 - The purposes for which each category is collected and used,
 - Whether each category is sold or shared
 - If yes, a link to the Notice of Right to Opt-out of Sale/Sharing
 - How long each category is retained.
 - A link to the business' Privacy Policy
- How to provide the Notice at Collection
 - Can be a separate notice, or
 - Can be included in the Privacy Policy if you can link directly to that content from the point of data collection.

Financial Incentive Notice must disclose:

- A succinct summary of the financial incentive or price or service difference offered
- A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
- How the consumer can opt-in to the financial incentive or price or service difference;
- A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- An explanation of how the price or service difference is reasonably related to the value of the consumer's data, including:
 - A good-faith estimate of the value of the consumer's data that forms the basis for offering the price or service difference; and
 - A description of the method(s) the business used to calculate the value of the consumer's data.

Risk Assessments

Periodic Risk Assessments

- Processing activities that present a “significant risk” to consumers’ privacy or security will require periodic risk assessments
- CPPA will have ability to conduct an audit to investigate if the collection or processing presents significant risk
- CO = likely standard for heightened risk assessments

Update: In March 2024, the CPPA Board shared draft proposed regulations on risk assessments and automated decision-making technology as well as draft updates to existing CCPA Regulations with updates and the formal rulemaking process expected to begin in July.

Other Obligations on Businesses

- **Collection minimization / purpose limitation**
 - “A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose...”
- **Retention minimization**
 - “[A] business shall not retain ... personal information ... for longer than is reasonably necessary for [each] disclosed purpose.”
- Regulations provide additional color
 - A business’s collection, use, retention, and/or sharing of a consumer’s personal information must be ***reasonably necessary and proportionate to achieve the purpose(s)*** for which the personal information was collected or processed or another disclosed purpose that is ***compatible with the context*** in which the personal information was collected
 - Regulations set forth a wide variety of factors for businesses to consider in this regard.

- **Affirmative obligation to implement data security protections**
 - Must “implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.”
 - 1798.81.5 is an existing CA data security law, but with a narrower definition of personal information
- **Private right of action where a breach resulted from a violation of the duty to implement and maintain reasonable security procedures and practices**
- **Annual cybersecurity audit requirement where processing presents a “significant” risk to consumer’s privacy or security**

Service Provider, Contractor, & Third Party Agreements

Who's Who Under the CCPA

Service Provider

A person that processes PI on behalf of a business and which receives PI from or on behalf of a business for a "business purpose" pursuant to a written contract that makes specific commitments.

Contractor

A person to whom the business makes available a consumer's PI for a "business purpose" pursuant to a written contract that makes specific commitments.

Third Party

A person who is NOT (1) the business with whom the consumer intentionally interacts and collects PI from the consumer as part of this interaction, (2) a service provider, or (3) a contractor.

CONTRACTS MUST PROHIBIT THE SERVICE PROVIDER OR CONTRACTOR FROM:

- Selling or sharing the PI
- Retaining, using or disclosing PI for any purpose other than for business purposes specified in the contract (*and the “limited and specified” business purpose must be set forth in the contract*);
- Retaining, using, or disclosing PI for any commercial purpose other than the business purpose specified in the contract
- Retaining, using, or disclosing PI outside of the direct business relationship between the service provider and the business - *for example, by combining or updating personal information received pursuant to the contract with personal information received from other sources or its own interactions with the consumer*

Also note: service providers and contractors cannot engage in cross-context behavioral advertising

Audit Rights

A business must have the right to take “reasonable and appropriate steps” to ensure that the service provider or contractor uses the personal information consistent with the business’s obligations, including “ongoing manual reviews and automated scans” and regular internal or third party assessments, audits, or other technical or operational testing at least once every year

Subprocessors

If the service provider or contractor engages another person to assist it in processing PI for the business, it must flow down the same contractual commitments via a binding written agreement

Comply with Law/Assist with Consumer Requests

Service providers and contractors must comply with law, may be required to cooperate with businesses in responding to verifiable consumer requests and to protect personal information, and notify the business if they cannot meet their obligations. Also must enable business to comply with consumer requests.

But What Are Business Purposes?

“OPERATIONAL” AND OTHER “NOTIFIED PURPOSES,” INCLUDING:

- Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance.
- Helping to ensure security and integrity to the extent the use of the consumer’s personal information is reasonably necessary and proportionate for these purposes.
- Debugging
- Short-term, transient use, including, but not limited to, **non-personalized advertising**
- Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
- Providing advertising and marketing services, **except for cross-context behavioral advertising**,
- Internal research for technological development and demonstration
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Due Diligence, Oversight, and Remediation



CCPA DEMANDS DUE DILIGENCE AND OVERSIGHT FOR SERVICE PROVIDERS AND CONTRACTORS:

- Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the law.
 - For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the law
- Contract must grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information.
 - For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

CONTRACT WITH THIRD PARTY MUST:

- Identify the “limited and specified” purposes for which PI is made available, not in generic terms
- Specify that the personal information is made available only for the “limited and specified purposes” set forth in the contract and the third party may use only for those purposes
- Require the third party to comply with applicable obligations under the CCPA, and may require the third party to comply with a forwarded opt out request or to protect the data
- Grant the business rights to take reasonable and appropriate steps to ensure the third party uses the PI in a manner that is consistent with the business’s obligations under the CCPA
- Grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of PI
- Require the third party to notify the business if it can no longer meet its obligations under the CCPA
- Grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of PI

Employee & Business Contact Data

Employee and B2B Data

CCPA Now Covers Employee and Business Contact Data

CCPA originally deferred extending rights of California consumers to California business contacts and employees (including job applicants and contractors)

Lobbying to extend that deferral beyond Jan. 2023 failed

All **obligations/rights** that attach to consumers in CA are extended to employees **and** business contacts, e.g.:

- Rights to access, delete, correct, etc.
- Service provider contracts
- Privacy notices

However, there can be significant differences in practical application




What it Means: You must extend your privacy program to Employee and B2B at least in California



- Rights to access, delete, correct, etc.
 - Requests and responses will need to align with HR systems and processes
 - Which exceptions might apply (or apply differently) in an employment context?
- Service provider contracts
 - Evaluate which providers are actually “service providers” vs. separate businesses
 - For those that are service providers, be sure necessary contract language is in place
 - For those that are not, could the transfer of employee data be a “sale”?
- Privacy notices
 - Apply just to CA (and EU) employees, or to all employees?
 - Present on internal site, employee handbook, onboarding for employees and contractors, as part of application process, etc.


Enforcement Update

- AG and CPPA have concurrent enforcement authority
 - AG: Judicial Proceeding before state court judge
 - CPPA: Administrative proceeding before administrative law judge
- Both have announced / signaled enforcement priorities:

Attorney General	CPPA
<p><u>Announced investigative sweeps:</u></p> <ol style="list-style-type: none"> 1. Streaming apps & devices (01/24) 2. Employee & job applicant privacy (07/23) 3. Mobile apps & sales (retail, travel, food service) (01/23) 4. Loyalty programs / financial incentives (01/22) <p><u>Enforcement case examples:</u></p> <ol style="list-style-type: none"> 5. Opt-out of sales, including via GPC; do not sell links 6. Privacy policies and notice at collection 7. Service provider contract terms 8. Individual rights request / authorized agent processes 9. Minor personal data disclosures and protections 	<ol style="list-style-type: none"> 1. Privacy notices and policies 2. Right to delete 3. Consumer request implementation 4. Connected vehicles & related tech 5. Opt-outs of sales and sharing 6. Dark patterns 7. Marginalized/vulnerable populations 8. Data minimization in consumer requests <div style="display: flex; align-items: center; margin-left: 20px;"> <div style="margin-right: 10px;">    </div> <div> <p>07/23 CCPA Board Meeting</p> <p>07/23 Press Release</p> <p>04/24 IAPP Global Privacy Summit</p> <p>04/24 Enforcement Advisory</p> </div> </div>

Sephora Enforcement Action

State of California Department of Justice

 **ROB BONTA**
Attorney General

Search

[Translate Website](#) | [Traducir Sitio Web](#)

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS APPOINTMENTS CONTACT

Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act

Press Release / [Attorney General Bonta Announces Settlement with Sephora as ...](#)



Wednesday, August 24, 2022

Contact: (916) 210-6000, agpressoffice@doj.ca.gov

Marks strong second year of CCPA enforcement with update on enforcement efforts and new investigative sweep of businesses failing to process opt-out request via a user-enabled global privacy control

OAKLAND – California Attorney General Rob Bonta today announced a settlement with Sephora, Inc. (Sephora), resolving allegations that the company violated the California Consumer Privacy Act (CCPA), California's first-in-the-nation landmark privacy law. After conducting an enforcement sweep of online retailers, the Attorney General alleged that Sephora failed to disclose to consumers that it was selling their personal information, that it failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA,





The Attorney General sees **all disclosures that are not to service providers as sales**, particularly in the advertising and analytics space.



The AG **isn't kidding** about the Global Privacy Control (GPC).



Enforcement is here: **"No more excuses."**



- Settlement announced February 2024
- Alleged violations of CCPA & CalOPPA
- Alleged CCPA violations focused on “do not sell” rights and related disclosures
 - Personal information including names & addresses shared in a marketing co-op
 - Participants in co-op cross promoted brands with direct mail
 - A consumer got an unwanted direct mail from another brand
 - Practice not disclosed as a sale
 - DoorDash did not have sale opt-out processes for the practice
 - Practice ended January 2020, first month CCPA was in effect



What's Next

Ongoing Rulemaking by the California Privacy Protection Agency (CPPA)

- CPRA shifted rulemaking authority from the Attorney General to the CPPA
- First round of CPPA rulemaking finalized in March 2023
- Second round underway, addressing cybersecurity audits, risk assessments, & automated decisionmaking
- Additional rounds expected

Rulemaking authority is both specific and open-ended

- Directed to engage in rulemaking on certain enumerated topics,
- But also broad authority to adopt rules “to further the purposes of this title”

Industry positions continuing to evolve. Things to watch for include:

- Selling/Sharing:
- Can you share without selling? Will “we do not sell” companies shift their positions?
 - Ad industry standards – NAI Guidelines, IAB MSPA (way to transmit signals) etc.
- Shifting positions from service provider to third party
 - E.g., “custom audience” terms offered by social media companies and others
- Decisions on uses of sensitive PI (e.g., add the opt out or stop the practice?)
- Aligning with new and evolving requirements in other states / jurisdictions