

# Digital Content Next

Legal and Legislative Committee  
October 15, 2019

## Agenda

---

### Review of CCPA Regulations Issued by CA AG

## CCPA Regulations

---

10/11 - CA AG Xavier Becerra issued draft CCPA regulations

<https://www.oag.ca.gov/privacy/ccpa/>

12/2, 3, 4, and 5 – CA AG to host public hearings

12/6 – Comments due

## CCPA Regulations

---

Notices of Collection, Opt-Out, Financial Incentive

Requirements for Privacy Policy

Business Practices for Handling Consumer Requests

- Methods for Submitting Requests to Know and Delete
- Responses to Requests to Know and Delete

Service Providers

Requests to Opt-Out/Opt-in

Training/Record Keeping

Verification

Minors

Non Discrimination

### Regs require notice at/before collection

Can be a link on homepage OR on app download page OR on all pages

- Unclear if same/separate from “Do Not Sell My Info” link
- Can be a link to relevant section of privacy policy

Must be easy to read, draws attention, in language the business uses in contracts, etc, and accessible to disabled. Must include:

- Categories of PI collected
- Purposes for each category
- Link to privacy policy

Note: If a non-consumer-facing business (ad networks, ISPs, social networks, operating systems and platforms) wants to sell PI, it must contact 1) consumer directly with opt-out and 2) consumer-facing business to confirm proper notice was provided

### Regs require notice of Opt-Out

“Do Not Sell My Personal Information” or “Do Not Sell My Info”

- Must link to Notice or relevant section of privacy policy

Must be easy to read, draws attention, in language the business uses in contracts, etc, and accessible to disabled. Must include:

- Description of right
- Web form
- Instructions for other opt-out methods
- Proof required to use an “authorized agent”
- Link to the privacy policy

AG solicits suggestions for an opt-out logo

### Regs require notice of Financial Incentive offer

Purpose is to inform consumer of financial incentive or price or service difference a business may offer in exchange for personal information

Must be easy to read, draws attention, in language the business uses in contracts, etc, accessible to disabled, and available online or offline where a consumer will make decision. Must include:

- A “succinct” summary
- Description of the material terms
- How the consumer can opt-in and opt-out
- Legal justification
- Good faith estimate of value of consumer data
- Description of method used to calculate estimate

Regs require “Comprehensive Description” of a business’ online and offline practices

Must be easy to read (language and format), in language the business uses in contracts, etc, accessible to disabled, available in a format that is printable and found via a “privacy” link on homepage or download page of an app. Must include:

- Right to Know about Collection, Disclosure and Sale
- Right to Delete
- Right to Opt-Out
- Right to Non-Discrimination
- Metrics
- Miscellaneous



### Privacy Policy must include:

Explanation of Right to Know about Collection, Disclosure and Sale

- How to submit request with a link to do so
- How business will verify identity and what info must be provided
- Categories of PI collected in preceding 12 months
- Sources of data and purposes
- Categories of 3<sup>rd</sup> parties that will receive data
- Statement re whether business has sold data in last 12 months
- Categories of PI sold for “business or commercial” purposes
- Statement re whether business sells PI of under 16 year olds without affirmative consent

## CCPA Regulations – Requirements for Privacy Policy

---

### Privacy Policy must include:

#### Explanation of Right to Delete

- How to submit request with a link to do so
- How a business will verify identity and what info must be provided

### Privacy Policy must include:

#### Explanation of Right to Opt-Out

- (From Sec 999.306)
- Description of right
- Web form
- Instructions for other opt-out methods
- Proof required to use an "authorized agent"

#### Explanation of Right to Non-Discrimination

### Privacy Policy must include:

Metrics: (from Sec 999.317) "A business that alone or in combination, annually, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall" disclose for the previous 12 months:

- # of requests to know (complied and denied)
- # of requests to delete (complied and denied)
- # of requests to opt-out (complied and denied)
- Median number of days to substantively respond to each category

### Privacy Policy must include:

#### Miscellaneous:

- Explanation of how a consumer can use an “authorized agent” to make a CCPA request
- Contact information for consumers to ask questions or express concerns (method must reflect primary way business interacts with consumers)
- Date the policy was last updated

# CCPA Regulations – Practices for Handling Consumer Requests

---

## Methods for Requests:

### Request to Know:

- Business must provide a minimum of 2 methods
  - Toll free # (required)
  - Interactive web form (if business has a website)
  - Other methods include: email or hard copy form
  - Must consider how a business primarily interacts with consumers

### Request to Delete:

- Business must provide a minimum of 2 methods
  - Toll free #, Link or webform, Email, Hard copy form
- 2 step process: submit request, then verify
- If consumer uses a different method or request is deficient, business must treat request as valid or direct consumer to proper method

## CCPA Regulations – Practices for Handling Consumer Requests

---

### Responding to Requests to Know or Delete:

Acknowledge receipt of request and explain process within 10 days

Must substantively respond within 45 days

- May take up to 90 days if business provides explanation to consumer
- Request should include data from 12 months preceding date of request

## CCPA Regulations – Practices for Handling Consumer Requests

---

### Responding to Requests to Know Specific Data Points:

Business can deny request if it cannot verify identity

- Note: should consider providing info about categories of data
- For all denials, business should refer consumer to privacy policy

Business shall not disclose info if it would create “substantial, articulable and unreasonable risk” to security of personal information, consumer’s account or security of business

Business shall not disclose: SS #, Driver’s license #, Govt ID, Financial account, Health insurance or medical ID, or Account password or security Q&As

Explain other conflicting laws if that is basis for denial

Use reasonable security when transmitting personal information

May use “password-protected account” portal to right to know requests



### Responding to Requests to Know Categories of Data:

Can refer consumers to privacy policy if answer is the same for all consumers

Response should include:

- Categories of sources of data
- Business or commercial purpose for collection
- Categories of 3<sup>rd</sup> parties for sale and disclosure
- Business or commercial purpose for sale or disclosure

### Responding to Requests to Delete:

3 possible responses:

- Erase all data from systems (exception for archive or backups)
- De-identify
- Aggregate

If business cannot verify, it should treat as an “opt-out”

## CCPA Regulations – Service Providers

---

Allows for service providers to combine data from multiple businesses to “detect security incidents or protect against fraudulent or illegal activity.”

## CCPA Regulations – Right to Opt Out

---

Business must provide 2 methods:

- "Do Not Sell My Personal Information" or "Do Not Sell My Info"
- AND
- One of: toll free #, email, hard copy form, or user-enabled browser controls
    - must consider how business primarily interacts with consumers
    - In online setting, user-enabled browser controls are valid
  - Business may present consumer with choice to opt out of certain "sales" as long as global option is more prominent
  - Must respond to opt-out within 15 days, notify 3<sup>rd</sup> parties within 90 days and notify consumers of 3<sup>rd</sup> party notice
  - May deny opt-out if business has a "good faith" reason to believe it's fraudulent

Business can ask consumer to reconsider their opt-out

- Opt-in must be a 2 step process
  - Consumer request, then confirmation

Business must keep records of all CCPA requests for past 24 months

Must include:

- Request date
- Nature of request
- Method
- Date of response
- Nature of response
- Basis for denial

## CCPA Regulations – Training/Record Keeping

---

Metrics: (from Sec 999.317) "A business that alone or in combination, annually, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall" disclose for the previous 12 months:

- # of requests to know (complied and denied)
- # of requests to delete (complied and denied)
- # of requests to opt-out (complied and denied)
- Median number of days to substantively respond to each category

## CCPA Regulations - Verification

---

Stringency of verification should match sensitivity of data

Encouraged to not collect additional information

For password-protected accounts, existing authentication methods can be used

For non account holders:

- Disclosure of categories requires "reasonable degree of certainty"
- Disclosure of specific or sensitive data requires "reasonably high degree of certainty"

NOTE: AG allows for scenario where business would not be able to ID any of its consumers



## CCPA Regulations – Children and Minors

---

12 and under: Actual knowledge

Business must “establish, document and comply with a reasonable method for determining that the person affirmatively authorizing the sale ... is the parent”

- “in addition to COPPA requirements.”

Reasonable methods include:

- Hard copy form by mail, fax or scan
- Use of credit card or online payment system that notifies account holder
- Government issued ID
- Toll free #
- Video conference
- In person

## CCPA Regulations – Children and Minors

---

### 13-15: Actual knowledge

Business must “establish, document and comply with a reasonable process for allowing such minors to opt-in to the sale of their information”

- Must also provide notice to minors of their right to opt-out

Note: a business that exclusively targets offers of goods or services directly to consumers under 16... and does not sell the personal information of such minors without their affirmation authorization or...their parent or guardian for minors under 13...is not required to provide the notice of right to opt out”

## CCPA Regulations – Non-Discrimination

---

Business may offer different price or service to consumers who exercise CCPA rights if difference is related to the value of a consumer's data

Possible formulas:

- Marginal value to the business of a consumer's data
- Average value
- Revenue or profit generated from categories of consumers with differing value
- Revenue or profit generated from sale
- Expenses related to sale or offer
- Any other practical/reliable method in “good faith”

# Questions?

---