



Hogan
Lovells

CCPA Draft Regulations: *What You Need to Know*

October 17, 2019

Today's speakers



Tim Tobin

Partner, Washington, D.C.

T +1 202 637 6833

tim.tobin@hoganlovells.com



Melissa K. Bianchi

Partner, Washington, D.C.

T +1 202 637 3653

melissa.bianchi@hoganlovells.com



Mark Brennan

Partner, Washington, D.C.

T +1 202 637 6409

mark.brennan@hoganlovells.com



@MWBrennanDC



Bret Cohen

Partner, Washington, D.C.

T +1 202 637 8867

bret.cohen@hoganlovells.com



Scott Loughlin

Partner, Washington, D.C.

T +1 202 637 5565

scott.loughlin@hoganlovells.com



Introduction

California Attorney General Proposed Regulations


- Required to promulgate regulations
- Draft regulations still subject to change. Final regulations anticipated by July 1, 2020
- Four public hearings announced
 - **Sacramento** (Dec. 2)
 - **Los Angeles** (Dec. 3)
 - **San Francisco** (Dec. 4)
 - **Fresno** (Dec. 5)
- Comments due to the Attorney General by December 6, 2019, 5:00pm (PST)

Email:

PrivacyRegulations@doj.ca.gov

Mail:

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013



Article 2: Notices to Consumers

Types of Notices

1. Pre-collection notice (“at or before” point of collection)
2. Notice of the right to opt-out of sale of personal information
3. Notice of financial incentive
4. The privacy policy
5. New content requirements



Notices

Type of Notice	Key Points
Pre-Collection Notice	<ul style="list-style-type: none">• Provided <u>at or before</u> point of collection – for <u>online collection</u>, can be a link to the privacy policy• Includes categories of PI collected and the purposes for which <u>each of those categories</u> is used• Not required for businesses that <u>do not directly collect PI from consumers</u>, but additional pre-sale obligations apply to such businesses:<ul style="list-style-type: none">• Pre-sale obligation: (1) contact consumer and directly provide notice of opt-out right, OR (2) confirm and obtain attestation from <u>source</u> of PI that pre-collection notice was provided
Notice of Right to Opt-out	<ul style="list-style-type: none">• Must describe any proof required when a consumer uses authorized agent to exercise opt-out right out and a link to the business’s privacy policy• Must be posted on the webpage that a consumer arrives at after clicking on the “Do Not Sell My Personal Information” link• If a business substantially interacts with a consumer offline, the notice must be provided via an offline method (<i>e.g.</i>, on paper forms used to collect PI)
Notice of Financial Incentives	<ul style="list-style-type: none">• Must be available online or other physical locations where the consumer will see it before opting in to financial incentives.• Must include:<ul style="list-style-type: none">• A succinct summary of the financial incentive or price or service difference offered;• A description of the material terms, including categories of PI implicated by the program;• The method for opting-in to the financial incentive;• Notice of the right to withdraw consent and instructions on how to do so; and• An explanation of why the financial incentive provision is permitted under the CCPA (including a good-faith estimate and methodology of calculation).

Privacy Policies

Privacy policies must include (among other things):

- Description of the verification process
- The following information **for each category of PI** that is collected
 - categories of sources
 - business or commercial purpose for collection
 - categories of third parties with whom the PI is shared
- Whether the business sells the PI of minors under 16 years of age without affirmative authorization (which violates the law!!)
- Explanation of how a consumer can designate an authorized agent
- If the business is subject to the large business record keeping requirements, the information set out in those requirements
- Information on how a consumer with a disability may access the policy in an alternative format
- Be available in languages in which the business “in its ordinary course” provides info to consumers

New Opt-In Consent Requirement?

“A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and **obtain explicit consent from the consumer** to use it for this new purpose.”

An aerial photograph of a busy pedestrian crossing, likely in a city. The crossing is marked with white diagonal stripes on a dark grey pavement. Numerous people of various ages and ethnicities are walking across the crossing in different directions. The scene is captured from a high angle, providing a clear view of the flow of foot traffic. In the bottom right corner, there is a dark purple, semi-transparent rectangular overlay containing white text.

Article 3:
Business Practices
for Handling
Consumer
Requests

Accepting Requests to Know or Delete

- Businesses should account for the methods by which they primarily interact with customers in determining methods
- Deficient requests: accept or inform consumer how to correct the deficiency
- “Two-step process” for deletion requests:
 - Step 1: consumer submission of request
 - Step 2: separate confirmation consumer wants personal information deleted

Responding to Requests to Know or Delete

- Right to know:
 - Requests for “categories” must be individualized; general references to privacy policy insufficient (unless the policy is accurate with respect to all consumers)
 - Inform consumer of reason for denial (e.g., inability to verify or an exception)
 - Never disclose certain information (SSNs, DLNs, account password, etc.)
- Right to delete:
 - Must explain how satisfied (delete, de-identify, aggregate); archive/backups different
 - Choices okay, but global delete option “more prominent”
 - Inform consumer of reason for denial (e.g., inability to verify or an exception)
 - Disclose to consumer that record of request being kept

Responding to Sale Opt-Outs and Sale Opt-ins

- Opt-Out

- At least two methods, including “Do Not Sell My Info” link
- Choices okay, but global delete option “more prominent”
- User-enabled privacy controls (e.g., browser plug-in) signaling sale opt-out must be honored
- Timing requirements: 15 days; flow down to recent (90 days prior) sale recipients

- Double Opt-In

- Two-step process (request + separate confirmation)
- May inform consumer who has opted-out of opt-in right when a transaction requires the sale of PI

Service Providers

- Service Providers can include entities that provide services to a person or organization that is not a business (*e.g.*, non-profit and government entities).
- Additional data use limitations.
 - Not use PI received from one person or entity, or through direct interaction with a consumer, for the purposes of providing services to another person or entity.
- Exception for security incidents and fraud detection.
- Know/delete obligations.
 - Provide consumers with explanation for denying request to know/delete PI.
 - Inform consumers who submit know/delete requests to service provider that requests should be submitted directly to business on whose behalf the service provider processes the PI.
- Comply with CCPA for any PI it processes outside of service provider role.

Training & Recordkeeping

- Training obligations
- Recordkeeping requirements
 - Maintain records of CCPA consumer requests and response for at least 24 months
 - Retain records in ticket or log format
- Requirements for large businesses (businesses that annually process PI of at least 4mm consumers for commercial purposes):
 - Compile for the previous calendar year:
 - The number of consumer (a) access, (b) deletion, and (c) opt-out requests the business (1) received, (2) complied with in whole or in part, and (3) denied; and
 - The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.
 - Disclose the above information in its privacy policy or posted on website and accessible from a link included in the business' privacy policy; and
 - Establish, document, and comply with training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

Article 4: Verification of Requests



General Rules Regarding Verification

- No verification of sale opt-outs
- Avoid sensitive data collection unless necessary (and *try* to use what you have)
- Consider various factors including sensitivity of PI and risk of harm to consumer or fraud
- If collecting PI to verify, delete after processing request
- Verifying through existing password-protected account okay
- No account: PI maintained in manner not tied to named person, then can require consumer to show they are “sole consumer” tied to PI (fact-based with factors above relevant)
- No way to verify: tell consumer, and if applies to all, state in privacy policy

Verification for Non-Accountholders

Verification of Requests to Know Categories of PI

A business must verify consumers making such requests to a “reasonable degree of certainty.”

- This may include matching at least two data points provided by the consumer to data points maintained by the business (if the business has determined that such data are reliable for verification purposes).

Verification of Requests for Specific Pieces of PI

A business must verify consumers making such requests to a “reasonably high degree of certainty.”

- This may include matching at least three pieces of PI.
 - The consumer must also provide a signed declaration under penalty of perjury that the requestor is the consumer whose PI is the subject of the request.
 - The business must maintain such declarations as records.

Verification of Deletion Requests

A business may verify deletion requests to either a “reasonable” or a “reasonably high” degree of certainty depending on the sensitivity of the PI and the risk of harm posed by unauthorized deletion.

- E.g., deletion of web browsing history (lower standard); deletion of family photos (higher standard).



Article 5:
Special Rules
Regarding Minors

Sales Involving Minors

Children Under Age 13

- Must use a “reasonable method for determining” that the person affirmatively authorizing a sale is the child’s parent or guardian.
 - COPPA-like standards for verifiable parental consent.
 - BUT COPPA parental consent ≠ CCPA parental sale opt-in.
- Parents must be informed of their opt-out rights at the time they opt in.

Minors 13-“16” Years of Age

- Minors in this age range do not need parental consent
 - Businesses with actual knowledge that they collect PI of children ages 13, 14, and 15 must establish, document, and comply with a “reasonable process” for allowing children to opt-in to sales.
- Minors must be informed of their opt-out rights at the time they opt in.



Article 6: Non-Discrimination

Discriminatory Practices

- Clarifies that businesses do not discriminate if the price or service difference is “reasonably related” to the value of the consumer’s data.
- The value for data can be calculated using one of seven described methods, or any “practical and reliable method” used in good-faith.
- Expressly allows for limitation of certain rights, such as sale opt out, to higher-cost tiers of service (so long as the difference in price can be justified).
- Raises questions about limits, especially with respect to deletion.



Key Questions

Key Takeaways

Questions

- Should we submit comments?
- Should we wait to implement the *draft* regulations? What should we do by January 1?
- How do we modify our privacy policy?
- How do we address adtech?
- Has the AG gone beyond the scope of the statute?

New Issues

- Impact on scope of “service provider”
- Combine categories of PI with sources, purposes, third parties
- Consent for purpose changes
- No notice at collection for non-consumer-facing businesses; can sell with source “attestation”
- Opt-out flow-down
- Comply with browser opt-out signals
- Requirement to record metrics



www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.