A Readout of the California Privacy Protection Agency’s Draft Proposed CCPA* Regulations

Kelley Drye

Agenda

I. Overview and Regulatory Process

II. Key changes in these regulations

   A. Business Obligations

      - Obtaining Consent
      - Notice at Collection
      - Data Subject Rights

   B. Service Providers, Contractors and Third Parties

   C. Opt-out Preference Signals

   D. Enforcement

III. Takeaways

Overview and Process

- Draft regulations were posted as part of materials for the June 8 Meeting.
- CPPA will commence formal rulemaking by filing Notice of Proposed Actions (NOPA), marking the first day of the formal rulemaking process.
- Initial comment period will run at least 45 days and the CPPA will hold a public hearing.
- CPPA's talktrack is that the proposed regulations are less creating new requirements than clarifying existing requirements.
- Final rules will not be adopted by July 1, and not enforcement before then.
- Until CPRA enforcement begins, existing CCPA rules, regulations, and definitions will be used for enforcement.
- How likely are these regulations to change?

Consent

- In the proposed regulations, consent is dependent on “average consumer expectations” when PI was collected.
- Otherwise, “explicit consent” is required for further processing.
- Explicit consent is also required for any processing not disclosed in its “notice at collection” or for any additional use.
- Explicit consent is not defined, but “consent” in CPRA refers to granular opt-in consent without dark patterns.
- Examples: location on flashlight app.
- What does this mean for ad tech and personalized advertising?:
    - Would an average consumer expect a pixel?
    - CPPA further explains: CCPA does not require that businesses obtain opt-in consent for the sale of personal information

Dark Patterns

1. Unclear Choices

Not Acceptable

Yes | Ask me later

Acceptable

Yes | No

2. Requiring extra steps to opt out

Not Acceptable

Accept All | More Information

Acceptable

Accept All | Decline All

Notice at Collection: Privacy Policy

- A business must include the following information in its notice at collection:
  - the categories of sensitive personal information collected;
  - whether the categories of personal information listed are sold or shared; and
  - the length of time the business intends to retain each category of personal information listed (or the criteria used to determine the retention period).
- Not sufficient:
  - Directing consumers to the top of a privacy policy is not sufficient. Deep Link required.
  - Cookie banners

Notice at Collection: Naming Third Parties

A “first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party’s website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection.”

- Applicable when more than one party controls PI collection (e.g. digital ads).

□ "Notice at collection" would need to include "the names of all third parties" or third party's business practices.

  □ Ex: Company A has a third party analytics tag on its website. Third party analytics company's obligations?

□ Rationale: Entities in contractual relationships can "work together."

- First party and third party would need to honor opt outs of sale/sharing.
- Do both first party and third party need to provide notice at collection?

Kelley
Drye

Data Subject Rights: Biggest Changes

- Right to Know/Access
  - Extending look-back period past 12-months to Jan. 1, 2022.
  - Exemption: "impossible or involves disproportionate effort."
- Right to Delete
  - Instruct Service Providers/Contractors to delete & notify third parties to delete.
  - Exemption: "impossible or involves disproportionate effort."
- "Impossible or involves disproportionate effort" now has a set standard:
  - A detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request.

Kelley Drye

Data Subject Rights: Right to Correct

- In determining accuracy of the information, a business may consider the "totality of the circumstances," which include:
  - (i) the nature of the personal information;
  - (ii) how the business obtained the contested information; and
  - (iii) documentation relating to the accuracy of the information.
- Propagating correction: instruct Service Providers and Contractors.
- Deletion as alternative for consumer and business.
- Request to note that information is contested in records.
- When not the source of information, name the source.
- Confirmation of correction.

Data Subject Rights: Opt-Out

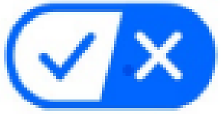
- Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business.
  - For example, the business may display on its website “Consumer Opted Out of Sale/Sharing” or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.
- A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

Data Subject Rights: Limit the Use of My Sensitive Personal Information

- Requirement of a link similar to Do Not Sell.
- As soon as feasibly possible, but no later than 15 days to limit the use of sensitive PI.
- Obligations to notify service providers, contractors, and third parties.
- Offering a confirmation that the request has been processed.

Alternative Opt Out Link and Icon

- Would your company be required to place BOTH a “Do Not Sell or Share My Personal Information” and a “Limit the Use of My Sensitive Personal Information” links?
- If so, the alternative opt out link and icon may be an option.
- Title the link, “Your Privacy Choices” or “Your California Privacy Choices”
- Include the following opt-out icon to the right or left of the title in approximately the same size as any other icons on the page



Propagating Data Subject Rights

	Deletion	Correction	Opt-Out of Sale/Sharing	Limit Use of Sensitive PI
Businesses				
Perform request	X	X*	X	X
Instruct/Notify SP/K	X	X		X
Instruct/Notify 3P	X*		X	X
Service Providers/Contractors				
Perform request	X	X		X
Instruct/Notify SP/K	X (any sub SP/K and other SP/K separate from business, unless *)			
Instruct/Notify 3P	X (if not at direction of business, unless *)			
Third Parties				
Perform request	X		X	X
Instruct/Notify SP/K			X	X (if disclosed to)
Instruct/Notify 3P			X	X (if disclosed to)

* unless impossible or involves disproportionate effort

Service Provider: DPA Implications

- Very granular contract requirements, beyond what most current privacy addenda (or technology provider terms and conditions) look like today, and include:

- Identify which specific business purposes and services are required for processing the business's personal information; cannot be stated generally with reference to the agreement, but rather requires a specific description.

- Regs suggest that a one-size-fits-all DPAs for all vendors processing personal information for different business purposes or functions might not be sufficient—very concerning from a resource and practicality standpoint.

- Note CPRA imposes similar contract requirements on business relationship with third parties.

Service Provider: Business Intrudes

- Contract requires service provider or contractor to comply with all applicable sections of the CCPA and the regs (e.g., help business with DSRs; implementation of security procedures).
- Business has right to take reasonable and appropriate steps to ensure that service provider is performing its obligations.
    - Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.
- Notification to business within 5 business days if the service provider determines it cannot meet its obligations.
- CPPA can evaluate whether the business conducted any due diligence to support a reasonable belief of privacy compliance, and whether and how the business enforces its contract terms, including performing audits.

Service Provider: Ad Tech Implications

- Service provider/Contractor cannot contract with a business to provide cross-contextual behavioral advertising (CCBA).
    - "A person who contracts with a business to provide [CCBA] is a third party and not a service provider or contractor.”
- What's new?
    - The examples suggest CCBA is defined broadly.
    - Regs do not contemplate:
        - Inquiry into commitments made by the vendor.
        - Availability of other business purposes related to advertising.

Service Provider: Examples

- Examples of what Service Providers can do:
  - Company hires a social media company as a service provider to advertise on the social media company's platform. Social media company can provide non-personalized advertising services on its platform based on aggregated or demographic information, but not business's customer PI list to identify users on the platform to serve ads.
  - Company hires ad agency as a service provider. OK for agency to use company PI to provide contextual advertising services.

Service Providers: Internal Use

- Service provider is restricted from using customer PI for its own purposes, except for internal use to build or improve the quality of its services, provided that the service provider does not use the PI to perform services on behalf of another person.
- Examples suggest that where service provider uses are to facilitate personalized advertising or data sales, they would not fit within a service provider/contractor role.

Opt-Out Preference Signals (GPC-->OOPS)

- Simple, easy to-use method that allows automatic opt-out of sale/sharing with all businesses consumers interact with online rather than via individual requests with each business.
- Requires processing any opt-out preference signal that meets the following requirements:
  - Signal is in a format commonly used and recognized by businesses, e.g., HTTP header field.
  - Platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer via its configuration or public disclosures that using the signal is meant to opt the consumer out of the sale and sharing of their PI.

OOPS—Not optional (Friction)

- Even if business posts opt-out sale/share/limit sensitive PI links, it must still process opt out preference signal, but may do so “in a non-frictionless manner."

- If business processes signal in a frictionless manner, includes certain disclosures in its privacy policy, and fully honors the opt out (online/offline), it does not need to post other opt-out links on its site.

- Frictionless = not charging a fee/requiring valuable consideration, change consumer’s experience with the product/service, or display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to signal (other than opt out status).

OOPS: No for Sens. PI, Yes for third parties

- Regs explicitly state that signals do not need to express consumer's request to limit the use and disclosure of sensitive PI.
- Also do not need to contemplate opt-in consent from children (or their parents).
- A third party that collects PI from a consumer online (e.g., through a first party’s website) and receives an OOPS shall recognize the signal as a valid request to opt-out of sale/sharing and shall not retain, use, or disclose that PI unless informed by the business that the consumer has consented to the sale or sharing of their PI or the third party becomes a service provider.
- Business not required to undertake identity resolution in response to OOPS.

Kelley Drye

Enforcement—Empowered Agency

- While there are provisions about requiring consumers to file sworn complaints, the CPPA can accept and initiate investigations on unsworn and anonymous complaints, and on its own.
- Probable cause determination is final and not subject to appeal, but…
- The probable cause hearing does not result in a fine or a judgment on violations. It results in a prob cause determination by CPPA which can be resolved with a settlement (any settlement would be public). Alternatively, company can proceed to an administrative hearing before an ALJ.
- Agency has broad power to initiate and undertake audits.

Takeaways

- Data mapping/inventory is more crucial than ever.
  - Flows among business, service providers, contractor, third party (business).
  - Detail in notice at collection and privacy policy.
- This is a heavy lift—use software.
- The regs make Calif even more the outlier among state privacy laws, but...
- Don't delay preparation waiting for a Federal Bill—just be surprised (overjoyed?) if it comes.
- (*CPPA has indicated a second round of rulemaking may focus on automated decisionmaking, cybersecurity audits, and privacy risk assessments; the timeline for issuance of additional rules is currently unclear*).

Kelley Drye

QUESTIONS?

ROBERT B. CUNNINGHAM
SPECIAL COUNSEL
RCUNNINGHAM@KELLEYDRYE.COM

ROD GHAEMMAGHAMI
SENIOR ASSOCIATE
RGHAEMMAGHAMI@KELLEYDRYE.COM

Kelley Drye

USE OUR LINKTREE

TO FIND ALL OF OUR UPDATES ON CONSUMER PROTECTION, ADVERTISING AND PRIVACY LAW TRENDS, ISSUES, AND DEVELOPMENTS

LINKTR.EE/KELLEYDRYEADLAW