The California AG's Draft Regulations & the Road to CCPA Enforcement

Webinar No. 3 of IAB's Privacy Law Webinar Series

May 19, 2020

Today's Speakers

Michael Hahn

SVP & General Counsel
IAB & IAB Tech Lab

Austin Mazzella

Legal Director, Data Protection & Privacy
Dentsu Aegis Network

Andrew Hall

Director of Compliance and Consumer Affairs
DISH Network L.L.C.

Monika Jedrzejowska

Chief Privacy Officer and Counsel
Hearst

Alysa Hutnik

Partner
Kelley Drye & Warren LLP

Julia Shullman

General Counsel & Chief Privacy Officer
TripleLift

Timeline

- CCPA effective date was Jan. 1, 2020
- AG enforcement permitted as of July 1, 2020
- Draft regulations not finalized
  - AG missed May 31st deadline for July 1 regulations enforcement
  - Unclear if the AG is aiming to finalize for October 1st or will use emergency process to implement the regulations sooner
- No Safe Harbor:

  If that were [the case], then you could murder someone today and if we couldn't figure out who did it for a month, would that mean you get to go scot-free? I don't think so. The law's the law.

  Attorney General Xavier Becerra

"Personal Information"

- Does business maintain information that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."
- For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

Proposed: Feb. 10, 2020 (2nd Draft)

Removed: Mar. 11, 2020 (3rd Draft)

Third Parties and Service Providers

- **Identification of Third Parties for Consumers**
  - "Categories of Third Parties" means types or groupings of third parties with whom the business shares personal information, described with **enough particularity** to provide consumers with a meaningful understanding of the type of third party.
    - They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

- **"Service provider" may also be a "business."**
  - Service provider that is a business shall comply with the CCPA and these regulations with regard to any PI that it collects, maintains, or sells outside of its role as a service provider.

Restrictions on Service Providers

- A service provider shall not retain, use, or disclose personal information obtained in the course of providing services **except**:

1. To process or maintain personal information ***on behalf of the business that provided the personal information***, or that directed the service provider to collect the personal information, ***and in compliance with the written contract for services required by the CCPA***.

2. ***For internal use by the service provider to build or improve the quality of its services***
   - provided that the use does not include building or modifying household or consumer profiles to use in providing services to *another business*, or
   - correcting or augmenting data acquired from *another source*.

What Notices Are Required?

- **Privacy Policy**
  - ID **categories of PI** the business **collected**; the **categories of sources** from which the PI is collected; and the **business or commercial purpose** for collecting or selling PI.
  - ID **categories of PI disclosed for a business purpose or sold** to third parties…. **For <u>each</u> category of PI identified**, provide **categories of third parties** to whom the information was **disclosed or sold**.
- **Notice at Collection**
  - Timely notice **at or before the point of collection** about the **categories of PI** to be collected from them and **the purposes** for which the PI will be used.
  - **Mobile:** When a business collects PI … for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary … and a link to the full notice.

Entities without direct consumer relationships

- **No Notice if No Onward Sale:** A business that does not collect PI directly from a consumer does not need to provide a notice at collection … if it does not **sell** the … PI.

- **Data Brokers:** If registered with AG, data broker does not need to provide a notice at collection to the consumer if its registration submission includes online privacy policy link with opt out instructions.

- **Statutory Requirement (1798.115(d)):** Third party **shall not sell purchased PI** unless consumer received **explicit notice** and opt out opportunity

Handling Rights Requests: Verification

- **Verification Process Considerations:**
  - PI type, sensitivity, and value
  - Risk of harm to consumer if unauthorized access
  - Likelihood that fraudulent or malicious actors would seek PI
  - If PI provided to verify is sufficiently robust
  - How the business interacts with the consumer
  - Available technology

- **Suggestions on Verification:** "Whenever Feasible," "Avoid," "Generally Avoid," "Reasonable security measures."
  - Avoid requesting new PI – especially sensitive PI. Instead, match provided PI to PI already held; or use a third-party verification service
  - Establish reasonable security measures to detect fraud

- **Reduced complexity for verification via password protected accounts versus non-accountholders.**
  - For non-accountholders, match at least 2 data points for category requests and 3 data points for specific PI requests.

Handling Rights Requests: Special Verification Procedures

- **Authorized Agent Requests**
  - An authorized agent must be a person or business entity registered with the Secretary of State to conduct business in California.
  - A business may require the consumer to:
    - Provide the authorized agent signed permission to submit a request
    - Verify the consumer's own identity directly with the business
    - Directly confirm with the business that they provided the authorized agent permission to submit the request.
- **Household Requests**
  - A business shall not comply … unless the following are satisfied:
    - All consumers jointly make the request
    - The business individually verifies all members.
    - The business verifies that each member making the request is currently a member of the household.

Handling Rights Requests: Access & Deletion Requests

- **Timeline:** 10 business days to acknowledge request, 45 calendar days to respond.
- **Verification:** If can't verify consumer within 45 days, business may deny the request.
- **Procedures:** Draft regulations provide specific procedures for handling access and deletion requests. For example:
  - What to provide to the consumer in response to an access request.
  - How to delete PI, and how to handle deletion exceptions.
  - If deleting PI in response to request, disclose compliance retention
  - If denying deletion request, offer opt out opportunity

Handling Rights Requests: Access Request Exemptions

- **Not required to search for records if:**
  - PI not maintained in a searchable or reasonably accessible format;
  - PI maintained solely for legal/compliance purposes;
  - Business does not sell the PI or use it for commercial purposes; ***and***
  - Business describes to the consumer the categories of records … that it did not search in accordance with this exemption.
- **Sensitive Records:** A business shall not disclose sensitive PI, including biometrics.

Handling Rights Requests: Opt Out of Sale

- **Methods of submitting a request:** DNSMPI link, toll-free phone number, email address, form, user enabled global privacy controls such as a browser plugin or privacy setting, device setting, or other mechanism.
- **Timeline:** As soon as feasible, but no later than 15 business days from receipt of the request.
- **Third Parties:** If a business sells PI *after* receipt of the opt out, the business shall notify the third party and direct them not to further sell the PI.
- **Verification:** No verification is required.

User-Enabled Privacy Controls (i.e., browsers)

- **Rule for Collection of PI Online:** The business shall treat user-enabled global privacy controls, ***that communicate or signal the consumer's choice to opt-out of the sale of their personal information*** as a valid request …
  - **Examples:** Browser plugin or privacy setting, device setting, or other mechanism.
  - **Clear Consumer Expectations:** Any privacy control … shall clearly communicate or signal that a consumer intends ***to opt-out of the sale of personal information.***

THANK YOU