Stradling

The CCPA Has A New Enforcer

Everything You Need To Know About The California Privacy Protection Agency

November 7, 2023

Presented by: Travis P. Brennan, Shareholder

Traditional “Consumer” Privacy Enforcement – U.S. vs. E.U.

U.S.A. – Enforcement by generalists

- Federal Trade Commission
- State Attorneys General

E.U./U.K. – Enforcement by privacy specialists

- Each member state has its own Data Protection Authority
- European Data Protection Board

CCPA Rulemaking & Enforcement Before July 1, 2023

Enforcement and rulemaking powers exclusive to the CA Attorney General's Office.

- No administrative enforcement power. (AG must sue violators in court to impose penalties.)
- No audit powers

CCPA implementing regulations currently in force were issued by the AG's office.
Heavy focus on:

- Right to opt-out of "sale"
- Verification of consumer requests
- Notice of financial incentive

CCPA Rulemaking & Enforcement Before July 1, 2023, cont.

AG's office delivered "notice of alleged noncompliance" to companies in various industries between 2020 and 2022, demanding that violations be "cured" within the CCPA's 30-day mandatory cure period.

- Enforcement case examples: https://oag.ca.gov/privacy/ccpa/enforcement
- Heavy focus on sale/opt-out issues, notice of financial incentive

To date, AG has brought a single, settled enforcement action, *People v. Sephora, Inc.* (Aug. 2022)

- Sephora didn't disclose that it was "selling" personal data by using common third-party cookies, didn't offer the opt-out required under CCPA
- Sephora agreed to a civil penalty of $1.2 million and two years of compliance monitoring (without conceding violations)
- **"Both the trade of personal information for analytics and the trade of personal information for an advertising option constituted sales under the CCPA."**

Poll!

In *Sephora*, the AG took the position that the CCPA requires businesses to honor the Global Privacy Control. (GPC is like a new version of “Do Not Track.”)

Does your company’s website honor the GPC signal?

- Yes
- No
- I don’t know

The California Privacy Rights Act (CPRA)

CPRA was a batch of significant amendments to the CCPA

- Enacted by ballot initiative in November 2020
- Effective January 1, 2023
- Enforceable as of July 1, 2023

Among other things, the CPRA established the ***California Privacy Protection Agency.***

Agency Creation and Structure

Vested with “full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act.”

The first, and so far, only, government agency in the United States dedicated exclusively to data privacy. (Similar to a European Data Protection Authority.)

Annual budget of $10,000,000

Agency Creation and Structure, cont.

Governed by a five-member board, including the chairperson

- Chairperson and one other member appointed by the Governor
- The AG, Senate Rules Committee, and Speaker of the Assembly each appoint another member

Current board members:

- Jennifer M. Urban, Chairperson (Law Professor)
- Alistair Mactaggart (Founder of Californians for Consumer Privacy)
- Lydia de La Torre (Researcher and int'l data protection expert)
- Vinhcent Le (consumer privacy attorney)
- Jeffrey Worthe (real estate developer and UCSB Foundation trustee)

Agency Creation and Structure, cont.

Key members of Executive staff:

- Ashkan Soltani, Executive Director
- Lisa Kim, Senior Privacy Counsel and Advisor
- Michael S. Macko, Deputy Director of Enforcement

Board held first public meeting in June 2021; has held six meetings so far in 2023

One takeaway from last meeting (Sept. 8):

- The Agency has filled about 55% of its full-time staff positions. Only 10% of enforcement positions filled to date.

Key Agency Powers

CPRA directed/empowered the Agency to (among other things):

- Provide guidance to consumers about their rights; guidance to businesses about their duties
- Appoint a Chief Privacy Auditor to conduct compliance audits (scope of this power to be defined by regulation)
- Conduct administrative enforcement actions, with power to impose fines
- Promulgate new implementing regulations on a wide swath of topics to clarify and supplement statutory requirements

Rulemaking

Rulemaking topics to be addressed include (among other things):

- Updating definitions of personal information, sensitive personal information, deidentified information and unique identifier to address changes in technology or data practices
- Adjusting the annual revenue threshold for a regulated “business” to reflect CPI increases
- Establishing rules and procedures for implementation of consumer requests
- Further defining and adding to the “business purposes” for which personal information may be used
- Defining what types of businesses must perform annual cybersecurity audits and regular privacy impact assessments
- Defining the scope and process for exercising the Agency’s audit authority
- Defining requirements and specifications for opt-out preference signals

Rulemaking, cont.

Rulemaking, Round One:

- Agency adopted its first set of regulations on March 29, 2023, after a very late start to the process
- Topics addressed include
  - Defined collection of employment-related information, including for the purpose of administering employment benefits, as an authorized “business purpose”
  - Mandated honoring opt-out preference signals (GPC)
  - Defined restrictions on collection and use of PI
  - Further defined methods for submitting and processing consumer requests and preferences, with a focus on prohibiting “dark patterns”
  - Updated requirements for notices at collection and privacy policies
  - Implementation of new CPRA rights, such as right to opt-out of “sharing” and right to limit use of SPI
  - New requirements for contracting with service providers and third parties

Another poll!

Has your company updated its privacy policy and notices to cover CA employees and job applicants?

- Yes
- No
- I don’t know

Rulemaking, cont.

But, a California court has delayed enforcement of these Rules to March 29, 2024!

- Ruling resulted from a suit filed by the CA Chamber of Commerce against the Agency
- Held that CPRA required Agency to issue rules by July 1, 2022, and that rules were not meant to be enforceable until one year after being finalized
- Establishes a one-year grace period for future regulations as well
- No effect on enforcement of statutory requirements
- On August 4, the Agency and AG appealed the ruling

Rulemaking, cont.

Rulemaking, Round Two

- On February 10, 2023, Agency invited preliminary comments on proposed rulemaking for: cybersecurity audits, risk assessments and automated decisionmaking
- Agency very recently published draft regulations for cybersecurity audits and privacy impact assessments. Early takeaways:
  - Incorporating AI or automated decision making into services will trigger requirement to perform PIA
  - “Selling” or “sharing” personal information will trigger requirement to perform PIA
  - Using employee monitoring tools will trigger requirement to perform PIA
  - Agency is considering limiting annual cybersecurity audit requirement to businesses whose annual revenue, or employee headcount, exceeds certain threshholds

Enforcement

Enforcement process:

- Enforcement division commences an investigation, files a Notice of Probable Cause Proceeding
- Legal Division conducts a Probable Cause Hearing and makes findings (at least 30 days after notice to company). Hearing is not public unless company requests it.
- Enforcement division files an Accusation (Complaint) in compliance with Administrative Procedures Act
- Administrative law judge presides over evidentiary hearing and renders proposed decision
- Agency board meets in closed session to decide whether to adopt, amend or reject decision
- Board's final decision may be appealed to Superior Court

Enforcement, cont.

To date, Agency has not announced any enforcement actions, but the mandatory grace period has expired.

On July 31, 2023, the Enforcement Division announced its first initiative: “a review of data privacy practices by connected vehicle (CV) manufacturers and related CV technologies.”

My guess - initial enforcement actions likely to focus on:

- Sale/sharing of PI and opt-out rights
- Dark patterns
- Use of precise geolocation data
- Children’s privacy

Audits

Agency has yet to hire a Chief Privacy Auditor.

Agency must still issue regulations “to define the scope and process for the exercise of the agency’s audit authority, to establish criteria for selection of persons to audit, and to protect consumers’ personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.”

My guess – unlikely to see routine audits begin until late 2024 or 2025 at the earliest.

Questions?

tbrennan@stradlinglaw.com