California Privacy Deep Dive

The CPPA, Regulations, and Enforcement

April 6, 2023

Presenters

Austin Smith
CIPP/E
VP of Legal Product
SixFifty

Seth Barany
Legal Product Associate
SixFifty

Agenda

- California Consumer Privacy Agency
  - Structure
  - Responsibilities and Actions
- Global Privacy Control
- CPRA Regulations
  - Current
  - Next round
- Risk Assessments
- Enforcement

California Privacy Protection Agency

- Created by CPRA ballot initiative
- Structure
  - Five-member Board
  - Governor appoints Chair and one other member
  - AG, Senate Rules Committee, and Speaker of the Assembly
  - Executive Director
- Took over rulemaking authority from AG
- Consumer Privacy Fund
  - Distribute to nonprofits to promote and protect consumer privacy
  - Nonprofits and schools to educate children re online privacy
  - Law enforcement to fund int'l cooperation to combat fraud

Poll #1

CPPA Responsibilities and Actions

- Regulations
- Promoting public awareness
  - Public report re risk assessments
  - Advise businesses and CA legislature
  - Create self-certification mechanism for businesses to volunteer to comply with the CCPA
- American Data Privacy and Protection Act (ADPPA)
  - Opposed federal preemption in ADPPA (along with Governor and AG) twice
  - ADPPA was amended to give the CPPA some enforcement authority
- Joined the Global Privacy Assembly in October 2022

CPPA Board and Staff

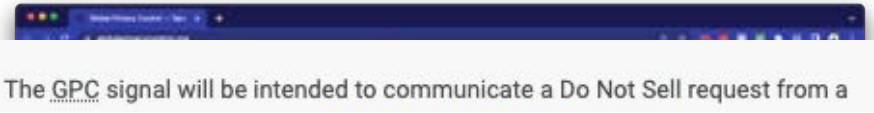
- Board Members
  - Chair: Jennifer M. Urban – Clinical Professor at UC Berkeley Law School
  - Alastair Mactaggart – Founder of Californians for Consumer Privacy
  - Lydia de la Torre – Professor at UC Davis Law
  - Vinhcent Le – Technology Equity attorney at Greenlining Institute
  - [empty spot]
- Executive Director: Ashkan Soltani
  - An architect of the CCPA
  - Chief Technologist of the FTC (2014–15)
  - Part of 2014 Pulitzer-winning team at Washington Post for NSA coverage
  - Helped develop the Global Privacy Control

Global Privacy Control

- GlobalPrivacyControl.org
- Developed in 2020
- One-time choice
- Signal sent to every website visited
  - HTTP Header
- Browser or browser extension
  - DuckDuckGo apps and extensions
  - Brave Browser
  - Firefox (opt-in)
  - Chrome extension (e.g., Privacy Badger)

Global Privacy Control: Q & (some) A

- What does it mean?
  - Opt out of sales ***and*** targeted ads?
  - Actively enabled or default?
  - Asking users to opt back in?
- California
  - Compliance with GPC mandatory
  - De facto opt out of sales and sharing
- Tangent: Colorado
  - Regulations finalized in March
  - Opt-out signal can't be default
  - Sale or targeted ads or both
  - AG will keep a list to comply with
  - Mandatory starting July 2024



The GPC signal will be intended to communicate a Do Not Sell request from a

Abstract

This document defines a signal, transmitted over HTTP and through the DOM, that conveys a person's request to websites and services to not sell or share their personal information with third parties. This standard is intended to work with existing and upcoming legal frameworks that render such requests enforceable.

CPRA Regulations

Effective March 29, 2023

Timeline

- CCPA charged the AG & CPPA with implementing wide variety of regulations to flesh out the statute
- Despite initial deadline of July 1, 2022, CPPA approved one set of regulations on February 3, 2023
  - Subsequent regulations will cover the areas listed in statute, but not addressed this round
- Became effective March 29, 2023

Key Points

- Opt-Out Preference Signals
- Required Links and Notices
- Clarified “Disproportionate Effort” Standard
- Data Minimization Principles
- Requirements for Designing “Choice Architecture”
- Service Providers and Contractors

What Are Opt-Out Preference Signals?

- Signal sent by “platform, technology, or mechanism” on behalf of a consumer that communicates the choice to opt-out of sale/sharing
  - Most commonly sent by browsers or browser extensions
- California provides very little guidance on exactly what types of signals businesses should look for
  - Must be in a format “commonly used and recognized by businesses” such as “an HTTP Header field or JavaScript object; and
  - Must make clear to the consumer that the “use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information”

What should you do when you get an OOPS?

- It's easy, just treat the signal as any other opt-out request
  - Stop selling/sharing covered data within 15 days of receipt
  - Notify all third-parties business has sold to or shared with
- Information disclosed to Service Providers or Contractors pursuant to a written contract does not qualify as sale/sharing

Who is opting-out?

- It can be hard to tell who is sending an OOPS, especially if they are using a new device/browser
- Businesses must opt-out the specific browser/device that sent the signal and any consumer profiles associated with the browser/device
  - If known, must opt-out the consumer as well
- MAY ask for additional information to facilitate opt-out
  - If the consumer does not provide that info, still must process opt-out

Required Links & Notices

Do Not Sell/Share My Personal Information

- Required for all businesses that sell/share PI
- Must be located in the header/footer of the business' homepage

AND

Limit the Use of My Sensitive Personal Information

- Required for businesses that process sensitive PI for non-exempt purposes
- Must be located in the header/footer of the business' homepage

OR

Alternative Opt-Out Link

- "Your [California] Privacy Choices"

- Must direct consumers to explanation of both rights and mechanism to exercise them

“Disproportionate Effort”

- Used several places in the context of responding to consumer requests
    - Allows businesses not to comply with certain requirements if doing so would be unreasonably difficult or costly
- Applies when the “time and/or resources expended” by the business “significantly outweighs the reasonably foreseeable impact to the consumer” of not complying with a given requirement
    - Generally required to explain facts to consumer when claiming disproportionate effort
- Another area to monitor for development as enforcement begins

Data Minimization

- Businesses must conduct a set analysis to ensure privacy practices are in line with minimization obligations
- Two discrete tests –
  - One to ensure a purpose is appropriate and consistent with consumer expectations
  - Another to ensure data collection/processing are reasonably necessary and proportionate to that purpose

“Choice Architecture”

- Detailed requirements for how to offer consumers privacy choices
  - I.e. when a business asks for consumer consent, how should that look?
- Emphasizes simplicity, symmetry, and ease of use
- Methods shall:
  - Be easy to understand;
  - Be symmetrical in choice;
  - Avoid confusing language or interactive elements;
  - Avoid impairing consumer ability to choose; and
  - Be easy to execute

Service Providers and Contractors

- Data disclosed to these entities is not “sold” or “shared”
- Both are defined by required written contract with the business
  - Service Providers must “process Personal Information on behalf of a business”
- Written contract must contain several required provisions
  - Must set forth the specific Business Purposes for which data is disclosed, and require the SP/C to only use disclosed data for those purposes;
  - Must require SP/C to comply with CCPA; and
  - Must grant business the right to monitor compliance and take remedial action
- CANNOT contract to provide targeted advertising

What's Next?

CPPA Currently Accepting Public Comment on Second Round of Regulations

Three Areas of Focus

Cybersecurity Audits

- Novel requirement
- Must be conducted annually by some businesses
- CPPA to clarify:
  - Applicability
  - Scope
  - Process
  - Standards

Risk Assessments

- Similar to Data Protection Impact Assessments
- Must be conducted before engaging in high-risk processing
- And submitted to CPPA "on a regular basis"
- Factors to be considered in line with existing laws

Automated Decision-making

- Consumers can opt-out and request details of decision-making process
- Potentially significant impact on HR data practices
- A lot of leeway for CCPA to define the scope of these rights

Poll #2

Amendments

- **AB 1194** would exclude Personal Information related to reproductive health from certain CCPA exemptions
- **AB 1546** would significantly lengthen the statute of limitation for AG enforcement actions (up to 5 years)
- **AB 947** would expand definition of Sensitive Personal Information to include citizenship/immigration status

Enforcement

Past and Future

Past Enforcement

- AG release of enforcement case studies
  - 75% of businesses cured alleged violations
- Sephora settlement
  - $1.2M
- Attorney General Bonta announced an investigative sweep of mobile apps Jan. 2023
- NB: AG enforcement, not the CPPA

Sephora Settlement

- 2022 Sephora Settlement with CA AG
- Alleged violations included:
  - Ignoring GPC signals
  - No disclosure of sales (3rd-party trackers)
  - Missing Do Not Sell link
- Outcome
  - $1.2M
  - Add info about sales to privacy notice
  - Process GPC signals
  - Update service provider agreements
  - 2 years of reporting to AG on GPC

CPPA Enforcement

- Begins July 1, 2023
  - Current enforcer is the AG
- Procedure
  - Consumer complaints
  - Investigations
  - Probable cause proceeding
  - Administrative hearing (5-year statute of limitations)
- Fines
  - $2,500
  - $7,500 for intentional violations or minors' data
  - Good faith cooperation taken into account
- Judicial Review
- NB: The Attorney General has concurrent enforcement authority

Thank you!

Connect with us
on social media