SQUIRE PATTON BOGGS

What Choice Do You Have?

Unpacking New State Law Requirements and Industry Standards

October 1, 2021

Ashok Chandra
Hannah Speirs
Elliot Golding
Kyle Fath

Today's Presenters

Ashok Chandra
Senior Privacy Counsel
Criteo

Elliot Golding
Partner, Squire Patton Boggs
(Washington, DC)

Hannah Speirs
Associate Counsel, Compliance
Carvana

Kyle Fath
Of Counsel, Squire Patton Boggs
(Los Angeles/New York)

Agenda

- State Privacy Laws Overview
- A Deeper Dive – Opt-ins and Opt-Outs
- AdTech Industry Standards and Evolving Technologies
- The Countdown to 2023: Start Preparing Now
- Questions

SQUIRE PATTON BOGGS

State Laws Overview

- California Privacy Rights Act (“CPRA”)
- Virginia Consumer Data Protection Act (“CDPA”)
- Colorado Privacy Act (“CPA”)
- Current California Consumer Privacy Act (“CCPA”) Enforcement Priorities

State Laws Overview

SQUIRE PATTON BOGGS

California Privacy Rights Act ("CPRA")

- Amends the California Consumer Privacy Act ("CCPA")
- Effective January 1, 2023, although administrative and civil enforcement will not commence until July 1, 2023

Virginia Consumer Data Protection Act ("CDPA")

- Inspired by CCPA/CPRA and GDPR
- Effective January 1, 2023

Colorado Privacy Act ("CPA")

- CDPA, CCPA/CPRA and GDPR inspired
- Effective July 1, 2023

Who Must Comply?

- CPRA: Similar to CCPA – $25mm annual revenue or data thresholds – with some nuances
- CDPA and CPA – Data collection/processing and/or sale thresholds + targeting residents with products/services
- All three impose statutory obligations on service providers/processors (unlike current CCPA)

Data Covered + Notable Exemptions

SQUIRE PATTON BOGGS

	CPRA	CDPA	CPA
Data Covered	• Personal information, with enumerated categories (including new category of Sensitive PI) • HR and B2B data in scope	• Personal data (no enumerated categories) • Sensitive data	• Personal data (no enumerated categories) • Sensitive data
Exempted Data	• Deidentified data • Publicly available data; aggregate consumer information • Preserves limited exceptions for data subject to other laws (e.g., GLBA, HIPAA, COPPA)	• Employment data • Deidentified data; publicly available data • B2B data	• Deidentified data; publicly available data • Data maintained for employment records purposes • Data subject to other laws (e.g., GLBA, HIPAA, FCRA, COPPA) • Data of individuals acting in "a commercial or employment context"
Exempted Organizations	• Government agencies, nonprofits	• Entities subject to other laws, including GLBA, HIPAA • State agencies • Nonprofits, higher ed institutions	• Air carriers • Financial institutions subject to GLBA

Consumer Rights & Business Obligations

SQUIRE PATTON BOGGS

Consumer Right	PICICA	CCPA	CPRA	CDPA	GDPR	CPA
Right to access	×	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	×	Implied	Implied	✓	✓	✓
Right to data portability	×	✓	✓	✓	✓	✓
Right to delete ~	×	✓	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	×	×	✓	✓	✓	✓
Notice and transparency requirements	✓	✓	✓	✓	✓	✓
Right to opt-out of sales	✓*	✓*****	✓*****	✓****	✓**	✓*****
Right to opt-out of targeted advertising (CO and VA) / cross-context behavioral advertising sharing (CA)	×	×***	✓	✓	✓	✓
Right to object to or opt-out of automated decision-making ~ ~	×	×	✓	✓	✓	✓
Opt-in or opt-out for processing of "sensitive" personal data? – "sensitive is defined differently under CPRA, CDPA and CPA	×	×	Opt-out†	Opt-in	Opt-in††	Opt-in†
Right to object to/restrict processing generally	×	×	×	×	✓	×
Right to non-discrimination	×	✓	✓	Limited	Implied	Limited
Purpose / Use / Retention Limitations	×	Implied	✓	✓	✓	✓
Applies to both consumers and in HR and B-to-B contacts	×	+	++	×	✓	×
Privacy and security impact assessments sometimes required	×	×	✓	✓	✓	✓
Obligation to maintain reasonable security	×	✓	✓	✓	✓	✓

For explanation on nuances to the chart, see:
https://www.squirepattonboggs.com/en/insights/publications/2021/09/cpra-cdpa-cpa-unpacked-develop-a-preparedness-plan-now

Enforcement & Potential Penalties

SQUIRE PATTON BOGGS

	CPRA	CDPA	CPA
Enforcement Authority	• State attorney general • Also enforceable by California Privacy Protection Agency ("CalPPA"), which has right to conduct compliance audits and rulemaking authority	State attorney general, who also has rulemaking authority	• State attorney general and district attorneys • State attorney general also has rulemaking authority
Private Right of Action?	limited for consumers whose nonencrypted, nonredacted PI was subject to unauthorized access and exfiltration	No private right of action	No private right of action
Opportunity to Cure?	• No more cure period for any alleged violations • AG has discretionary authority to determine appropriate cure period	30 days	60 days for any alleged violation until 2025
Potential Penalties	administrative fines c/o CalPPA, civil penalties c/o CA AG; $2,500 for each violation or $7,500 for each intentional violation or violations involving data of minors	$7,500 per violation + reasonable expenses incurred in investigation and case preparation (e.g., attorney fees), injunction	calculated per consumer, per violation; civil penalties = $2,500; max = $500K for related violations; injunction

California AG CCPA Summaries and Complaint Tool

SQUIRE PATTON BOGGS

- On July 19, 2021, the California Attorney General issued a press release summarizing its first year of CCPA enforcement

- **Key findings:**
  - 75% of companies that received notice to cure came into compliance within 30-day cure period or under ongoing investigation (but again, the CPRA gets rid of the cure period)
  - Provided summaries of 27 resolved exemplary cases, most dealing with notice deficiencies and inadequate disclosures, including financial incentives (e.g., loyalty programs), and consumer rights request program inadequacies
  - Cases seem to indicate that collection by a third-party cookie provider, absent a service provider commitment by such provider, may be a "sale" to such provider

- New online consumer complaint tool launched, allowing consumers to answer certain gating questions to create a notice of noncompliance that can be sent to a business.

California AG's Examples of Non-Compliance

SQUIRE PATTON BOGGS

- The 27 total examples of noncompliance included the following industries:

Data Broker (3)	Automotive	Education Technology	Online Dating
Grocery Retailer (3)	Children's Toy Distributor	Email Subscription Platform	Online Marketing Services
Social Media (3)	Consumer Electronics	Mass Media and Entertainment	Online Platform (Classified Ads)
Video Game (3)	Digital Experiences Partnerships	Online Advertising	Pet Industry
Online Event Sales (2)	Digital Media	Online Clothing Retailer	

- Most prevalent types of noncompliance:

Description of Non-Compliance	Frequency (#)	Frequency (%)
Missing Method to Submit Requests or Missing Proper Instructions Related to Consumer Rights	15	23%
Missing Reference to Sale Position (e.g., "No knowledge of sales in prior 12 months")	9	14%
Missing Do Not Sell My Personal Information Link or Opt-Out Process	9	14%
Missing Pre-Collection Notice at Point of Collection	8	13%
Missing Consumer Rights Instructions Regarding Discrimination	4	6%
Privacy Notice or Opt-Out Process was Difficult to Understand and Needed Revisions	3	5%

SQUIRE PATTON BOGGS

A Deeper Dive

Opt-ins and Opt-outs

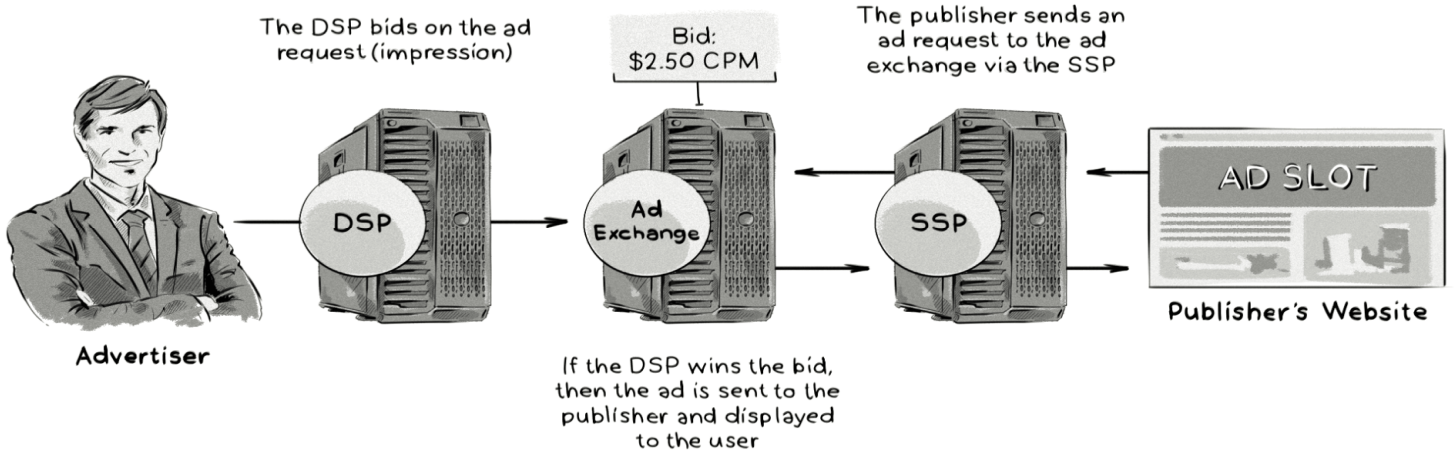
2023: Year of the Opt-Outs

- Opt-out rights applicable to digital advertising activities in the U.S.:
  - Currently:
    - Sale (CCPA)
    - Interest-based advertising (cookie and hashed-email based) self-regulatory opt-outs (DAA and NAI) (but, opt-ins required for certain activities)
  - 2023:
    - Sale (CPRA, VA, CO)
    - Sharing for cross-context behavioral advertising (CPRA)
    - Certain Sensitive PI Processing (CPRA)
      - But, opt-in for CO and VA
    - Targeted Advertising (VA, CO)
    - Profiling/Automated Decision-making (CPRA, VA, CO)
    - Interest-based advertising (cookie and hashed-email based) self-regulatory opt-outs (DAA and NAI)

*References to CPRA on this slide are to the CCPA as amended by the CPRA

AdTech 101

- "***Advertisers***" are the company seeking to deliver an ad to a user.
- "***Publishers***" are the entity that displays the ad to the user, such as on a website or digital platform.
- An "***Ad Exchange***" sits in the middle of the Advertiser and Publisher and facilitates a "***Real Time Bidding***" (RTB) auction between Advertisers trying to place ads and Publishers selling ad space.
- "***Demand Side Platforms***" (DSPs) and "***Supply Side Platforms***" (SSPs) help manage bids from multiple Advertisers and Publishers, respectively.



Assessing Consumer Rights and Applicable Choice(s)

- **Sale** (CPRA, CDPA, CPA)
- **Sharing** (in the context of cross-context behavioral ads) (CPRA)
- **Targeted advertising** (CDPA, CPA)
- **Processing of sensitive PI/PD** (CPRA, CDPA, CPA)
- **Profiling/Automated Decision-making** (CPRA, CDPA, CPA)
- *If so, how to provide consumer choice?*

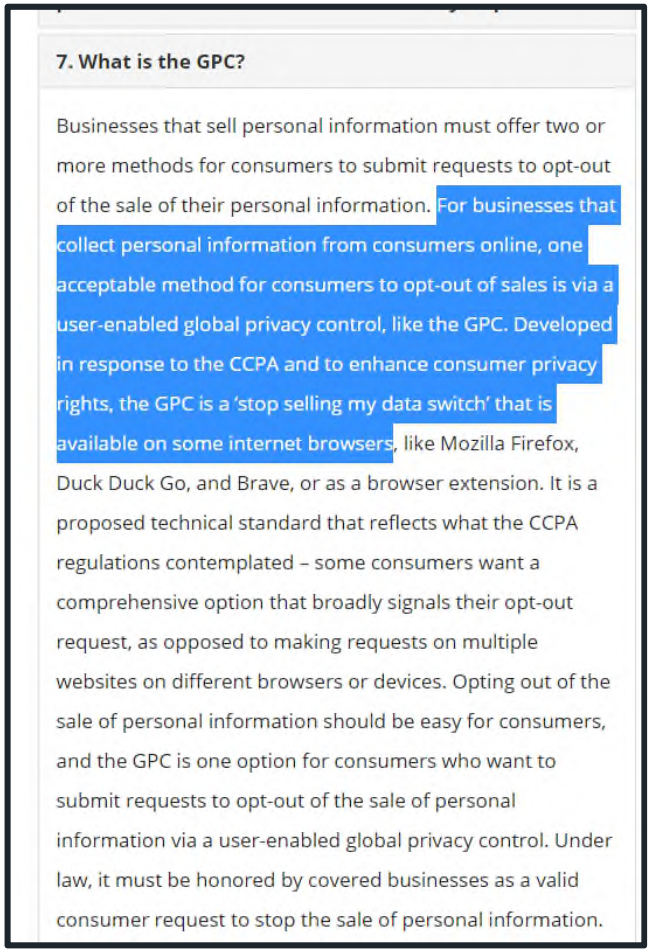
SQUIRE PATTON BOGGS

AdTech Industry Standards and Evolving Technologies

Global Privacy Control ("GPC")

- **CCPA:** Businesses are required to honor GPC signals (per regs)

- GPC endorsed by former CA AG Becerra; included as part of CA OAG online guidance under current AG Bonta (*see* CA OAG CCPA FAQs)



7. What is the GPC?

Businesses that sell personal information must offer two or more methods for consumers to submit requests to opt-out of the sale of their personal information. For businesses that collect personal information from consumers online, one acceptable method for consumers to opt-out of sales is via a user-enabled global privacy control, like the GPC. Developed in response to the CCPA and to enhance consumer privacy rights, the GPC is a 'stop selling my data switch' that is available on some internet browsers, like Mozilla Firefox, Duck Duck Go, and Brave, or as a browser extension. It is a proposed technical standard that reflects what the CCPA regulations contemplated – some consumers want a comprehensive option that broadly signals their opt-out request, as opposed to making requests on multiple websites on different browsers or devices. Opting out of the sale of personal information should be easy for consumers, and the GPC is one option for consumers who want to submit requests to opt-out of the sale of personal information via a user-enabled global privacy control. Under law, it must be honored by covered businesses as a valid consumer request to stop the sale of personal information.

Global Privacy Control:
To Implement or Not To Implement?

SQUIRE PATTON BOGGS

- **CPRA:** Statutory text ambiguous as to whether honoring GPC signals is required, but will certainly be clarified in the Regs

- **CDPA:** No explicit provisions requiring businesses to honor GPC signals

- **CPA:** Required under CPA, but suggests that controller may authenticate as it would an agent request

Industry CCPA Frameworks/Tools

- **Interactive Advertising Bureau ("IAB") CCPA Compliance Framework**
  - Technical signal integrated with a publisher's "Do Not Sell My Personal Information" Link
  - Limited Service Provider Agreement
  - Publisher-level opt-out

- IAB's Interpretation of Sale: Publishers are the "business" collecting PI and "making available" the PI to AdTech/cookie vendors → absent SP relationship, sale by publisher

- *Recent AG enforcement seems to have tacitly endorsed the IAB's interpretation*

Industry CCPA Frameworks/Tools

- **Digital Advertising Alliance ("DAA") CCPA Opt-Out Tools**
  - Both Web and Mobile
  - Notably, the Opt-Out Tools are separate and distinct from the DAA's interest-based advertising opt-out mechanisms
  - Opt-out is at the AdTech vendor level, not at the publisher level

- DAA's Interpretation: AdTech/cookie vendors are independent businesses collecting PI and downstream selling PI to other third parties

- *Recent AG enforcement summaries seems to call DAA's interpretation into question*

BigTech Data Use Limitation Features

- In late 2019, Google and Facebook introduced features that, when activated, limit their respective processing activities to those of a CCPA Service Provider (along with corresponding contractual commitments)
  - Facebook Limited Data Use (LDU)
  - Google Restricted Data Processing (RDP)

- Apply by default for certain products/services (based on location – e.g., IP address)

- For those products/services where LDU/RDP does not apply by default:
  - LDU and RDP may be activated on a product-by-product basis for all Californians such that SP status applies and thus, no sale occurs; OR
  - features may be activated in response to DNS request from a particular consumer

Recap: Assessing Consumer Rights and Applicable Choice(s)

SQUIRE PATTON BOGGS

- Is the activity:
  - a sale (CA, VA, CO)?
  - a sharing (CA)?
  - targeted advertising (VA, CO)?
  - processing of sensitive PI/PD (CA, VA, CO)?
  - Profiling/automated decision-making (CA, VA, CO)?

- If so, how to provide consumer choice?
  - Opt-in or opt-out?
  - Industry developed tools (IAB)?
  - Vendor-specific tools (Google RDP, Facebook LDU, etc.)?
  - GPC?

Countdown to 2023: Timeline for Preparation

Workstream	Goal	Timeline
1	Assess compliance and gaps, and prepare 2022 notices and 2023 preparedness plan.	Q4 2021
2	Create or update data inventories and develop and deploy data management capabilities	Q4 and throughout 2022
3	Update privacy policy(ies) and remediate practices	Q4 2021
4	Refine your consumer request procedures	2022
5	Implement privacy-by-design and data governance	2022
6	Update or implement a vendor and data recipient management program	Q4 2021 and throughout 2022
7	Update policies	2022
8	Implement reporting, recordkeeping and training	2022
9	Shore-up data security and breach preparedness	2022
10	Project audit and go-live	Q4 2022

Thank you!