Decoding The California Privacy Rights Act

Peter Stockburger
Partner, San Diego

Rachel Ross
Associate, San Diego

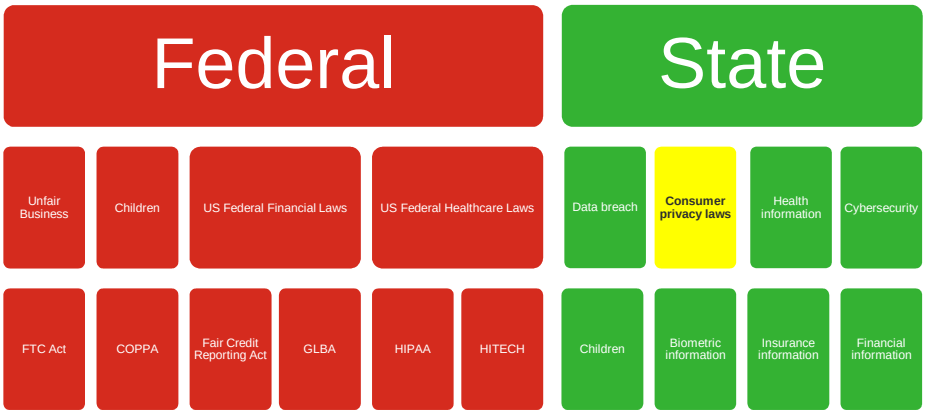
Dentons CLE Seminar for In-House Counsel
2021 Winter Webinar Series
January 6, 2021

Decoding The California Privacy Rights Act
Roadmap

- How We Got Here & Where We're Headed
- CCPA v. CPRA - What You Need To Know
  - What's effective now…
  - What's effective in 2023…
- Enforcement, Regulations & Private Right of Action
- Key Takeaways
- CPRA Planning - Roadmap Through 2023
- Questions

How We Got Here & Where We're Headed

US Privacy Snapshot



大成 DENTONS

How We Got Here & Where We're Going

Setting The Table

CCPA passed, signed on **6/28/18**, amended once **9/23/18**, effective **1/1/20**

Further set of **CCPA** amendments signed in **2019** and **2020**

AG began **CCPA** enforcement on **7/1/20**, regulations took effect **8/14/20**

CPRA passed by California voters on **11/3/20, effective 12/16/20**

CPPA to begin regulatory activities **7/1/21**

CPRA mostly operative **1/1/23**

大成 DENTONS

CCPA v. CPRA - What You Need To Know

What's Effective Now

Employee / Job Applicant Exemption

- **CCPA** amendments signed in October 2020 extended exemption to 1/1/22.
- **CPRA** extends exemption through 1/1/23.
- **Future amendments to CPRA unknown** because **CPRA** has limited amendment provision.

B2B Communication Exemption

- **CCPA** amendments signed in October 2020 extended exemption to 1/1/22.
- **CPRA** extends exemption through 1/1/23.
- **Future amendments to CPRA unknown** because **CPRA** has limited amendment provision.

CPPA Formation / Authority

- **California Privacy Protection Agency (CPPA)** is being formed now.
- **5 board positions** to be appointed. Staffing to take place throughout 2021.
- **$10m budget**. 40-50 employees.
- **Regulatory authority** switches on 7/1/21.
- **Enforcement** will begin on 7/1/23, with some lookback.

大成 DENTONS

CCPA v. CPRA - What You Need To Know

What's Effective In 2023

Change	CCPA	CPRA
New Definitions	➢ Limited definitions of "business". ➢ Expansive definition of PI, narrow "publicly available" exception.	➢ Alters existing definitions for "business", and adds new definitions. ➢ Creates new category of sensitive PI, and expands "publicly available" definition.
Expanded Notices	➢ Limited application and scope for notices at collection.	➢ Expanded application and scope for notices at collection.
New Processing & Retention Standards	➢ No processing restrictions. ➢ Limited data retention requirements.	➢ New processing restrictions. ➢ New and expanded retention standards.
Expanded Consumer Rights	➢ Limited to right to know, delete, opt-out of sale, non-discrimination.	➢ Adds rights to correct and limit processing of sensitive PI. ➢ Expands right to opt-out to include "sharing".
Expanded Contract Standards	➢ Limited to service providers / non-third parties.	➢ Required for expanded group, including contractors and sale partners.
Expanded Private Right of Action	➢ Limited to negligent data breach based on existing data breach law.	➢ Affirmative security obligation added. ➢ Expands definition of trigger for private right of action.
Enforcement	➢ California Attorney General as regulator and enforcer.	➢ California Attorney General remains for civil enforcement. California Privacy Protection Agency for administrative enforcement and regulations.

大成 DENTONS

CCPA v. CPRA - What You Need To Know
Changes To Definitions Of Business & PI

Business Definition

- **Changes To Definition #1: CPRA** changes the scope of the three gating thresholds by: (1) clarifying when the annual gross revenue is to be calculated; (2) expanding the number of consumers from 50k to 100k, and reducing the type of activity covered; and (3) expanding the 50% revenue threshold to those who have revenue from advertising.
- **Changes to Definition #2**: **CPRA** changes the control / controlled framework to require that the entities share information for advertising purposes, and share common branding.
- **New Definitions**: The **CPRA** adds two new categories of persons who may be a covered business: (1) joint ventures (ownership of at least 40%); and (2) volunteers (i.e., those who volunteer to be subject to the law).

PI Definition

- **CCPA** definition of PI remains largely unchanged.
- **CPRA** includes expansion of publicly available exclusion to include information that a business has a **reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer**…
- **CPRA** includes new category of personal information - "**sensitive personal information**" which means PI that reveals information such as SSN, DL, precise geolocation data, protected characteristics or union membership, and emails and texts (unless meant for the business).

CCPA v. CPRA - What You Need To Know
Expanded Notice, Processing & Retention Standards

Expanded Notice at Collection

- **Expanded Businesses Covered**. **CCPA** only required those businesses that collect PI directly from the consumer to provide notice. **CPRA** expands to cover those businesses that control the collection as well.
- **Expanded Notice Obligations**. **CCPA** only required categories of PI and purposes for use to be disclosed. **CPRA** expands to include length of retention, as well as information related to categories of sensitive PI.

New Processing & Retention Standards

- **Processing Restriction**. **CPRA** introduces a new requirement that businesses may only collect, use and store PI that is reasonably necessary and proportionate to achieve the purposes for which the PI was originally collected.
- **Retention Restriction**. **CPRA** introduces a new requirement that PI may only be retained for as long as necessary to effectuate its original and/or noticed purpose.
- **Tip**. Ensure the notice of collection is adequately detailed!
- **Security Restriction**. **CPRA** introduces a new affirmative security requirement around PI collected. Does this mean expanded private right of action?

CCPA v. CPRA - What You Need To Know

New Consumer Rights To Correct And Limit Processing

Right To Correct PI

- **CPRA** provides new right to correct PI in the possession of the business.
- **Subject to** verifiable request.
- **Must be** disclosed in privacy policy.

Right to Limit Processing Sensitive PI

- **Right**: Limit use to that which is "necessary" to perform the services or provide the goods "reasonably expected by an average consumer", or as otherwise authorized by statute or regulation.
- **Notice**: If a business uses sensitive PI beyond purposes other than those specified, there must be notice and there must be a right to limit.
- **Consent**: After direction, can only use it for other purposes if direct consent from user.
- **Direction**: Business must direct service providers and contractors to do the same.
- **Exception**: Sensitive PI collected or processed "without the purpose of inferring characteristics about a consumer" is exempt.
- **Link**: New link that says "Limit the Use of My Sensitive Personal Information" (but technology allowed, streamlining exceptions may apply).

CCPA v. CPRA - What You Need To Know

Expanded Opt-Out Right

Still Applies To A Sale

- "**Sell**" or "**sale**" is defined broadly as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, PI by the business to another **business** or **third party** for **monetary** or **other valuable consideration**.
- What is "**other valuable consideration**?
- **California contract law** may govern in the interim.
- **Excludes** intentional sharing, sharing with service providers, non-third parties, with consent, and sharing during an acquisition or merger.

Now Includes "Sharing"

- **Share** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally a consumer's PI from a **business** to a **third party** for "**cross-context behavioral advertising**" - whether or not for money or other valuable consideration (more expansive than "sale").
- **Cross-context behavior advertising** means the targeting of advertising to a consumer based on the consumer's PI obtained from the consumer's activity across business, distinctly-branded websites, applications, or services, other than the business with which the consumer intentionally interacts.
- **Excludes** intentional sharing, sharing with service providers, sharing with contractors, with consent, and sharing during an acquisition or merger.

CCPA v. CPRA - What You Need To Know

Expanded Contracting Requirements

CCPA Contracting Requirements

- **No general contracting requirement.**
- **Service providers** require a contract that prohibits the service provider from retaining, using, or disclosing the PI for any other purpose other than that set forth in the agreement (including for a commercial purpose).
- **Non-third parties** require a contract that prohibits the non-third party from selling, retaining, using, or disclosing PI for any purpose other than that set forth in the agreement (including for a commercial purpose). Also includes a **certification requirement** for the non-third party.

CPRA Contracting Requirements

- **Broader contracting requirements** for third parties who receive a sale or sharing of data, service providers, and contractors.
- **Contracting requirements** are the same for all three groups of entities - contract must:
  - **Specify** the PI is sold or disclosed only for limited and specified purposes;
  - **Obligate** the third party, service provider, or contractor to comply with applicable obligations under the CPRA and obligate those persons to provide the same level of privacy protection as required under the CPRA;
  - **Grant** the business rights to take reasonable and appropriate steps to help ensure the receiving entity uses the PI in a manner consistent with the business's obligations;
  - **Require** the receiving party to notify the business if it makes a determination it can no longer meet its obligations under the CPRA; and
  - **Grant** the business the right to stop the receiving entity from using the PI for unlawful purposes.

大成 DENTONS

Enforcement, Regulations & Lawsuits

CCPA v. CPRA

CCPA

- **AG has sole authority** to investigate and enforce the law. 30 day cure period. Advisory function.
- **Enforcement** can include injunctive relief or penalties of $2,500 for each violation and $7,500 for each intentional violation (no cap).
- **Private right of action** limited to PI (as narrowly defined under CA data breach law) that is: (1) nonencrypted **and** nonredacted; and (2) subject to a breach resulting from the business's "violation of the duty to implement and maintain **reasonable security procedures and practices**[.]" Ability to cure.
- **Statutory damages** not less than $100 and not greater than $750 per consumer per incident or "actual damages", whichever is higher.

CPRA

- **New administrative enforcement** to be lead by new agency - California Privacy Protection Agency (CPPA). CPPA will take over regulatory authority. No right to cure.
- **Civil enforcement** remains with AG. Will focus on impact litigation.
- **Penalties** for enforcement expanded to $2,500 for each violation, $7,500 for each intentional violation, and $7,500 for minor data violations.
- **Private right of action expanded** to include e-mail and password. Limited cure options.

大成 DENTONS

Enforcement, Regulations & Lawsuits
Regulatory Outlook

- **Develop** uniform opt-out logo.
- **Outline details** around right to correct.
- **Develop standards** for requests that go beyond 12 months.
- **Further define** “business purpose”, “intentional interaction”, and “precise geolocation”.
- **Outline** higher standards for delivering PI.
- **New regulations** for requiring cybersecurity audit and risk assessment submission for businesses whose processing presents a “significant risk” to privacy or security.
- **Create** rights of access and opt-out regarding use of automated decision making, including profiling.
- **Regulations relating to** an opt-out signal.

Key Takeaways
Tip #1 - Know Thyself

- **Prepare data maps, inventories or other records** of all PI pertaining to California residents, households and devices, as well as information sources, storage locations, usage and recipients. This process will help prepare for new CPRA obligations of notice, retention, and processing restrictions. It will also help determine if the organization is no longer subject to the CPRA based on the narrowing of coverage thresholds.
- **Determine whether your organization shares data** to determine whether opt-out mechanisms need to be in place related to advertising. This may involve doing a deep dive on third-party cookies and related technologies on your digital platforms.
- **Review and understand** all existing data privacy / information security processes, procedures, and protocols. How do they align with “reasonable” standards for the private right of action, including the expanded definition? How do they align with the record keeping requirements and retention standards? Where are the gaps?
- **Build stakeholder teams** and start the discussion on preparing a data map that will engage and empower those impacted.

Key Takeaways
Tip #2 - Make Strategic Decisions

- **What is the business approach to privacy?** Will the organization take a one-size-fits all approach, and adopt CPRA rights and obligations across the board to all individuals (i.e., non-California residents, employees, etc.) or limit it to California? What is the outlook 5, 10 years down the road? Compliance focused, or take an industry-leading approach?
- **How does the business want to use its data in the future?** Equally important to determining how to comply with the CPRA is determining how the organization will want to treat data in the future. If the organization doesn't sell or share data now, will it? What types of data segregation / database consolidation efforts can be undertaken now?
- **Align strategy and approach** throughout the organization to ensure a privacy and security-by-design culture is in place, and future changes in the law can be addressed in a systematic fashion.

Key Takeaways
Tip #3 - Inventory / Negotiate Third Party Agreements

- **Inventory** current third-party agreements to determine whether the third party will be considered a service provider, third party, or contractor under the CPRA.
- **Develop and negotiate** third-party, service provider, contractor agreements to align with new CPRA requirements.
- **Tip** - Watch-out for sneaky provisions giving the recipient of the data the right to use the data beyond the terms of the contract.
- **Tip** - Use the opportunity to review data breach, indemnity, warranty provisions.
- **Ensure security protocols**, and best practices are implemented across the third party environment.
- **Develop** third-party auditing standards, if not already in place.

Key Takeaways
Tip #4 - Align Internal Processes

- **Inventory** current data privacy and information security policies, processes, and standards to leverage for CPRA compliant policies, processes, and standards.
- **Develop new** internal policies, processes, and standards for handling data subject act requests, verifying identity, tracking opt-out requests, record retention, and training.
- **Ensure HR and IT** coordinate with the notices to job applicants and employees, and information is adequately secure.
- **Prepare and implement new systems, templates and databases** to facilitate data subject access requests and record keeping requirements.
- **Implement training** to ensure policies, processes, and standards are well integrated.
- **Prepare HR and others** for changes in 2023 relating to employee data privacy.

Key Takeaways
Tip #5 - Update & Create External Notices

- **Update external privacy policy** to include descriptions of CPRA rights, appropriate disclosures on categories of personal information collected, sold, or disclosed for business purposes, and provide the required link and disclosures for the right to opt-out.
- **Tip** - Use this opportunity to revise and streamline external facing privacy policy more generally. Adopt best practices, simplify, and consider how California rights will be displayed.
- **Create "Just-In-Time" Notices** that comply with the "at or before the point of collection" requirement. These notices must not only appear on websites and applications, but they also need to appear in employee handbooks, and any location where job applications and/or employee information is collected. Consider user-friendly notices, and ensure they are readable, accessible, and available in multiple languages.

Key Takeaways

Tip #6 - Don't Sleep On Cybersecurity

- **Biggest risk** for the private right of action is having protected data exposed in a data breach, and there not be reasonable security measures in place.
- **Measure security posture** against, at a minimum, the Center for Internet Security's Critical Security Controls (2016 AG) to determine "reasonable" security requirement. Consider additional frameworks and standards, such as NIST, HITRUST, or other industry standards that may better reflect reasonable security in 2019-2020.
- **Ensure California resident PI is encrypted and/or redacted** at rest or in transit. Review current data sets to see what can be deidentified or aggregated to minimize exposure.
- **Ensure third parties are audited** to protect against flow-down liability.

CPRA Planning

Key Dates

CPRA Planning
Roadmap Through 2023

Year		Task
2021	☑	**Develop A Strategy** Determine whether your organization will carve out California rights, or adopt a CPRA compliant strategy for the entire consumer / employee base.
2021	☑	**Map Your Data** This is a critical step before determining whether your organization has sensitive PI, is sharing or selling information, and how to craft notices.
2021	☑	**Coordinate Stakeholders** CPRA compliance will require a whole-of-enterprise approach, involving Legal, Marketing, C-suite, HR, IT, etc. Begin those conversations early!
2021-22	☑	**Streamline Vendor Contracts** Starting on this process early will ensure you identify and revise contracts relating to the sale and/or sharing of personal information.
2021-22	☑	**Leverage Technology** Technology will help assist the organization manage the vendor contracts, opt-outs, identify sensitive personal information, and manage consumer requests.
2021-22	☑	**Shore Up Security** There remains a significant exposure on a private right of action if there is "unreasonable" security for California personal information.
2022	☑	**Build Out Processes** Prepare for administrative enforcement by building out a robust set of holistic processes aimed at addressing CPRA compliance and ongoing risk assessments.
2022	☑	**Budget** Understanding the scope of tasks required for CPRA will help departments budget for compliance efforts, and mitigation measures.
2022	☑	**Socialize** Start talking about the changes early with employees and customers to avoid any shock in system changes.
2023	☑	**Launch** Hit the ground running on 1/1/23!

大成 DENTONS

Thank you

大成 DENTONS

Dentons US LLP
4655 Executive Drive, Ste. 700
San Diego, CA 92121
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.