The California Consumer Privacy Act (CCPA)

What Grocers Need To Know

February 19, 2020
California Grocers Association

Peter Stockburger
Partner
Dentons US LLP
peter.stockburger@dentons.com
619.595.8018

The California Consumer Privacy Act (CCPA)

Agenda

- How We Got Here, Where We Are & Where We're Going
- The Who, What & Why (Definitions, Consumer Rights, Business Obligations)
- What's Your Risk? A Closer Look At Enforcement & The Private Right of Action
- Update On AG Regulations
- Known Unknowns - Security & Customer Loyalty Programs
- Not In Compliance? Quick Tips
- Questions

How We Got Here, Where We Are & Where We're Going

How We Got Here & Where We're Going

How We Got Here

Federal			State			
FTC Act	US Federal Financial Laws	US Federal Healthcare Laws	50 different data breach laws	**New consumer privacy laws (CA, NV)**	Shine the Light (CA, NY)	Cybersecurity specific (NY, CO)
Child online protections / Red Flag Rules	Fair Credit Reporting Act	GLBA	HIPAA	HITECH	Child online safety rules (CA)	Biometric Privacy Laws (IL)	Insurance privacy (CA, CT)	Financial information (CA)

How We Got Here & Where We're Going

Where We Are & Where We're Going

Passed, signed on **6/28/18**, amended **9/23/18**, effective **1/1/20**

Amendments final on **10/11/19**, AG draft regulations released **10/10/19**

AG released modifications on **2/7/20**, public comment - **2/24/20**

CCPA 2.0 looking at 2020 ballot

Federal discussions on federal data privacy law

Copycat CCPA

The Who, What & Why (Definitions, Consumer Rights, Business Obligations)

Key Definitions

Who Must Comply - Business

Definition #1

- **For-profit entity** that: (1) collects or determines the "purposes and means of the processing of" a California resident's personal information; (2) conducts business in California; and (3) satisfies one of the following three thresholds:
  - **Has an annual gross revenue** in excess of $25m USD, as adjusted;
  - **Buys, receives, sells, or shares** the personal information of 50,000 or more California residents, households, or devices per year (e.g., approximately 137 unique visitors per day); or
  - **Derives 50 percent or more of annual revenue** from "selling" California resident personal information.

Definition #2

- Any entity that **controls or is controlled** by a "business" as defined in definition #1, and that "shares common branding with the business."
- **Controls or is controlled** means: (1) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; (2) control in any manner over the election of a majority of the directors, or of individuals exercising similar function; or (3) the power to exercise a controlling influence over the management of a company.
- "**Common branding**" means a shared name, servicemark, or trademark.

Key Definitions

Who Is Protected - Consumers

Definition #1

- Any **natural person who is a California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations, “however identified.”
- “**However identified**” presents a potential strict liability standard.
- **Tip** - Consider putting burden on individual submitting request to confirm they are a California resident.
- **On face value includes** employees, competitors, B2B partners, owners, directors, officers, non-consumers, job applicants, and independent contractors.

Important Exemptions

- **Employee exemption until 2021**: The personal information of job applicants, employees, owners, directors, officers, and independent contractors is largely excluded from coverage under a majority of the CCPA (subject to notice and security standards).
- **Limited B2B exemption until 2021**: Personal information within the context of the “business conducting due diligence regarding, or providing or receiving a product or service” is exempted until 2021.
- **Tip**. Use opportunity to amend contracts, including with independent contractors to align with AB 5.

Key Definitions

What Is Covered - Personal Information

- **Information** that "identifies, relates to, describes, is **reasonably** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- **New proposed AG regulations** introduce clarification on limitations.
- **Does not include** publicly available, aggregate, or deidentified information (all separately defined).
- **Extremely broad definition** that could include surveillance footage, IP address, technical information not otherwise considered personal under previous laws.
- **Includes**, but is not limited to, the following categories:

- **Identifiers** such as real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Any **categories of PI** described in Civ. Code § 1798.80(e);
- **Characteristics** of protected classifications under California or federal law;
- **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- **Biometric** information;
- **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
- **Geolocation** data;
- **Audio**, electronic, visual, thermal, olfactory, or similar information;
- **Professional** or employment-related information;
- **Education information**, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (Civ. Code § 1798.140(o)(1)(A)-(K)); and
- **Inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Key Definitions

What Data Is Exempted

- **Employee data (2021).** Personal information of consumers in the course of the person acting as a job applicant, employee, contractor, officer, or director until 2021. Notice and security features still apply.
- **B2B communications (2021).** Personal information shared between a business within the context of the "business conducting due diligence regarding, or providing or receiving a product or service to or from such entity."
- **Health information.** Medical information under the CMIA or protected health information (PHI) under HIPAA, including the Privacy and Security Rules.
- **Consumer reporting information.** The sale of personal information to or from a consumer reporting agency if reported in or used to generate a consumer report under the FCRA.
- **Financial Information**: Information collected, processed, sold, or disclosed pursuant to the GLBA or California equivalent.
- **Driver's Information**: Certain information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994.

Consumer Rights & Obligations

Right To Know

Consumer Rights

- The **right to know** the **categories** and **specific pieces of personal information** collected, sold, or disclosed for business purposes by a “business.”
- Request must be “**verifiable**” (subject to verification standards proposed by AG regs).
- **Right to receive notice** of the right in the privacy policy, and notice at or before the point of collection of categories and purposes of use.
- **12 month lookback** on requests.
- **Opt-in required** if use goes beyond what is originally disclosed in “just-in-time” notice.

Business Obligations

- **Notice at or before the point of collection** to inform consumers about the **categories** of personal information to be collected and the **purposes** for their use. (New accessibility requirements)
- **Make available** two or more designated methods for submitting a request, including “at a minimum” a toll-free telephone number and “interactive webform.”
- **Response.** Must confirm receipt within **10 days**, and respond within **45 days** subject to extensions.
- **Privacy Policy** disclosure requirements.
- **Reasonable security requirement** on transmitting specific pieces of personal information.

Consumer Rights & Business Obligations

Right To Delete

Consumer Rights

- **Right** to request that a business delete consumer personal information collected about the consumer (AG expanded).
- **Verification required** Request must be made by verifiable consumer request (AG standards).
- **Are you sure?** Consumer must verify twice the request to delete (required or optional?).
- **Deletion obligations** extend to “service providers.” Double-edged sword. But what does “direct” mean?

Business Obligation

- **Privacy policy** must contain a description of the right to delete, including instructions for how to submit a verified request and links to an online form or portal to make the request (if offered).
- **Make available** two or more designated methods for submitting a request. No required minimum (compare against right to know).
- **Response.** Must confirm receipt within **10 days**, and respond within **45 days** subject to extensions.
- **Extensive exceptions**, including: (1) to complete the transaction with the consumer; (2) to comply with a legal obligation; or (3) to enable solely internal uses aligned with the consumer’s expectations.

Consumer Rights & Business Obligations

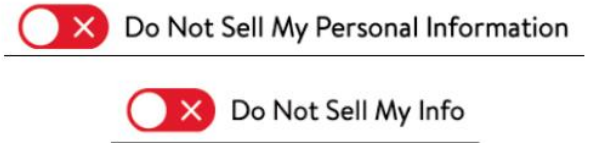
Right To Opt-Out

Consumer Rights

- Right to "**opt-out**" of the **sale** of personal information from a **business** to a **third party** (excluding service providers and non-third parties).
- **Notice required** of right and sale.
- **No verification required** (compare against right to know and right to delete).
- **No sale** under age of 16, unless under 13 with parental consent or between 13 and 16 with the minor's consent (**opt-in**).
- **Respect** the decision to opt-out for at least 12 months before requesting another sale.

Business Obligation

- **Request methods**. Requires two or more designated methods for submitting requests, including at a minimum a "**clear and conspicuous**" link on the homepage / website or landing page of mobile application that says "Do Not Sell My Personal Information" or "Do Not Sell My Info."



- **Disclosure** must be on the privacy notice.
- **Formatting and substance requirements** for notices (AG regs).

Consumer Rights & Business Obligations

What Does It Mean To Sell Personal Information

Definition

- "**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, a consumer's personal information 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.
- **Common examples**…

Statutory Exceptions

- **Example #1** - When a consumer intentionally directs or uses a business to disclose the consumer's personal information.
- **Example #2** - When a business uses or shares an "identifier" for the purpose of alerting a third party that a consumer has opted out of the sale of their personal information.
- **Example #3** - Personal information is disclosed to a "**service provider**."
- **Example #4** - Business transfers personal information to a third party as an asset that is part of a "transaction in which the third party assumes control of all or part of the business" provided the information is "used or shared" consistent with law.

Additional Rights & Obligations

Right to Anti-Discrimination - General Overview

- **Business cannot discriminate** against a consumer for exercising rights under the CCPA, including but not limited to:
  - **Denying** goods or services to the consumer;
  - **Charging** different prices or rates for goods and services, including discounts, benefits, or penalties
  - **Providing** a different level or quality of goods or services; or
  - **Suggesting** the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
- **Exceptions**
  - **Value Exception**. A business may charge a consumer a different price or rate or provide a different level of or quality of goods or services if the difference is “reasonably related” to the value provided to the consumer by the consumer’s data. (AG standards)
  - **Financial incentive exception**. A business may offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information if it is “reasonably related” to the value provided to the business by the consumer’s data. (AG standards)

Additional Business Obligations

Record Keeping & Training

- **Limited record keeping.** Consumer requests, including how the business responded to requests for at least 24 months (2 years). The records may be maintained in a ticket or log format if the format includes certain information. There are data use restrictions for records maintained.
- **No requirement for broader record keeping**. No express data retention requirements otherwise.
- **4m metrics**. A business that alone or in combination annually buys, receives for a business purpose, sells, or shares for commercial purposes, the personal information of 4m or more consumers must prepare certain metrics and disclose such metrics on the privacy policy.
- **Training**. Any individual responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA must be trained on the requirements of the CCPA and how to direct consumers to exercise their rights under the CCPA and the AG's regulations.

What's Your Risk? A Closer Look At Enforcement & The Private Right Of Action

Regulations, Enforcement & Private Right of Action

AG Enforcement & Private Right of Action

AG Enforcement

- Any business or third party may **seek the opinion** of the AG.
- **Safe harbor** - ability to cure (30 days).
- **AG regulations** now final.
- **If business fails to cure** within 30 days after being notified of alleged noncompliance, AG enforcement:
  - Injunction;
  - **Liability for a civil penalty** of not more than $2,500 for each violation or $7,500 for each intentional violation (NO CAP);
  - Penalties shall be **exclusively** assessed and recovered in an a civil action brought by the AG.

Private Right of Action

- **Limited** to when personal information, as defined under Civ. Code 1798.81.5(d), is: (1) nonencrypted **and** nonredacted; (2) subject to a breach resulting from the business's "violation of the duty to implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information."
- **Relief includes** damages, injunctive relief, other "relief".
- **Statutory damages** not less than $100 and not greater than $750 per consumer per incident or "actual damages", whichever is higher.
- **Ability to cure** (30 days).

AG Regulation Update

AG Regulations Update

When Will The Proposed Changes End?

- AG released draft regulations on **October 10, 2019**, open for public comment through **December 6, 2019**
- Law took effect on **January 1, 2020**
- AG released additional modifications on **February 7** and **February 10, 2020**, open for public comment through **February 24, 2020**
- New proposed modifications:
  - **Clarify** definition of personal information
  - **Clarify** accessibility standard
  - **Clarify** response obligations
  - **Clarify** service provider obligations

Current Rulemaking Activities

Revised Proposed Regulations – modified on February 10, 2020
Deadline to Submit Written Comments: February 25, 2020 at 5:00 p.m. (PST)

- Notice of Modifications, pdf [updated on 2/10/2020]
- Text of Modified Regulations – Redline Version, pdf [updated on 2/10/2020]
- Text of Modified Regulations – Clean Version, pdf [updated on 2/10/2020]
- Documents and Other Information Relied Upon

Initial Proposed Regulations – published on October 11, 2019

- Notice of Proposed Rulemaking Action (NOPA), pdf
- Text of Proposed Regulations, pdf

Known Unknowns: Security Footage, Customer Loyalty Programs & Grocer Concerns

Known Unknowns

Security, Customer Loyalty Programs & Grocer Concerns

Security Camera Footage

- **Scenario**: Customer submits a request to disclose security camera footage.
  - Can the business reasonably link the security footage to the requestor? Is the technology capable of doing so?
  - Do service providers have this capability?
  - Disclose fact of security camera footage, but can't disclose actual footage?
- **Scenario**: Customer submits a request to delete security camera footage.
  - Security exception to deletion.
  - Other regulatory obligations?

Customer Loyalty Programs

- Customer loyalty programs are not unlawful under the CCPA, they just need to be structured carefully.
  - **Step #1** - If the consumer exercises their right to know, delete, or opt-out, will that impact their loyalty / rewards program benefits?
  - **Step #2** - If the answer to #1 is yes, can the program be structured where the difference in service or price is based on the value of the consumer's data, as it relates to the business?
  - **Step #3** - If the answer to #2 is yes, is the business adequately disclosing in a financial incentive notice the value of the consumer's data?

Known Unknowns

New AG Examples Of Anti-Discrimination

- **Example # 1** - A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt out of the sale of their personal information, then the practice is discriminatory, unless the $5 per month payment is reasonably related to the value of the consumer's data to the business.
- **Example #2** - A clothing business offers a loyalty program whereby customers receive a $5-off coupon to their email address after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete as their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them, pursuant to one of the deletion exceptions.
- **Example #3** - A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request, but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.
- **Example #4** - An online bookseller collects information about consumers, including their email addresses. It offers discounts to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons are reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete as the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

Not Ready Yet? Tips For Compliance

Tips For Compliance

Tip #1 - Know Thyself

- **Prepare data maps, inventories or other records** of all personal information pertaining to California residents, households and devices, as well as information sources, storage locations, usage and recipients. This process will help prepare for data subject requests, and will enhance the organization's ability to complete a vendor risk assessment.
- **Determine whether your organization sells data** to determine whether opt-out mechanisms need to be in place, including for minors.
- **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? How do they align with the record keeping requirements? Where are the gaps?
- **Build stakeholder teams** and start the discussion on preparing a data map that will engage and empower those impacted.

Tips For Compliance

Tip #2 - Make Strategic Decisions

- **What is the business approach to privacy?** Will the organization take a one-size-fits all approach, and adopt CCPA related rights and obligations across the board to all individuals (i.e., non-California residents, employees, etc.) or limit 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 CCPA is determining how the organization will want to treat data in the future. If the organization doesn't sell 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.

Tips For Compliance

Tip #3 - Negotiate Third Party Agreements

- **Inventory** current third-party agreements to determine whether the third party will be considered a service provider or a non-third party under the CCPA.
- **Develop and negotiate** third-party agreement riders / revisions / new agreements that will incorporate the required provisions of the CCPA to ensure carve-outs for service providers or non-third parties apply.
- **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.

Tips For Compliance

Tip #4 - Align Internal Processes / Loyalty Programs

- **Inventory** current data privacy and information security policies, processes, and standards to leverage for CCPA 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.
- **Align loyalty programs** to ensure appropriate notices and value determinations are made and documented.

Tips For Compliance

Tip #5 - Update & Create External Notices

- **Update external privacy policy** to include descriptions of CCPA 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.

Tips For Compliance

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 personal information 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.

Getting Ready For The CCPA

Tip #7 - Third Party Assessments

- **Gap / risk assessments** can help determine course of action for HR and Legal.
- **Vendors galore,** but not all created equal
- **Law firm advantage** - privileged report
- **Dentons advantage**
  - Leading in **CCPA analysis, counseling**
  - Leading in **data protection / privacy**
  - Leading in **cybersecurity**
  - Leading in **employment**
  - Leading in **contract negotiation**
  - Leading in **client service**

Speaker Bio

Peter Stockburger

Peter Stockburger
Partner
D +1 619 595 8018
peter.stockburger@dentons.com

Peter Stockburger is a partner at Dentons, and is a member of the Firm's global Employment, Intelligence and Strategic Services, and Privacy and Data Security teams. Peter's practice focuses on the unique intersection between cybersecurity, data privacy, and employment law. Peter regularly advises clients on a range of cutting-edge legal issues, including cybersecurity resiliency and preparedness, cyber gap and risk assessments, reviewing and updating data privacy programs, technology contract review and negotiation, and due diligence. Peter also has extensive experience handling trade secret and breach of contract disputes before all level of courts and administrative agencies. He has been recognized as a Rising Star by Southern California Super Lawyers Magazine every year since 2015.

In addition, Peter is a frequent author and speaker in the field of data privacy and cybersecurity, speaking and publishing with groups such as NATO in Estonia, the Daily Journal, and Today's General Counsel.

- **Global online-based wine distributor:** CCPA compliance and review of data privacy and information security programs.
- **Domestic telecommunications and cable company:** CCPA compliance.
- **Domestic fintech SaaS provider:** CCPA compliance and SaaS contract review / negotiation.
- **Domestic sports data company:** Information security resiliency gap assessment and program review, and SaaS contract review / negotiation.
- **Domestic property management company:** ALPR compliance, CCPA compliance.
- **Global cloud provider:** Compliance with data subject access requests, DMCA takedown requests, and contract review / negotiation.
- **Global digital advertising company:** CCPA compliance.
- **Global medical device manufacturer:** Company-wide cybersecurity risk assessment.
- **Global personal product manufacturer and distributor:** GDPR risk assessment and compliance program review, CCPA compliance.
- **Global real estate company:** GDPR compliance, including privacy program review.
- **Global transportation company:** GDPR compliance, including compliance program review.
- **Global title insurance and insurance company:** CCPA compliance, privacy program review, and cybersecurity gap assessment.
- **Global retail company:** IBPA compliance and CCPA compliance.

Thank you

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.