# California Consumer Privacy Act of 2018

## Analysis and Key Takeaways


Stephanie Duchene
Partner
Los Angeles
+1 213 892-2909
stephanie.duchene@dentons.com

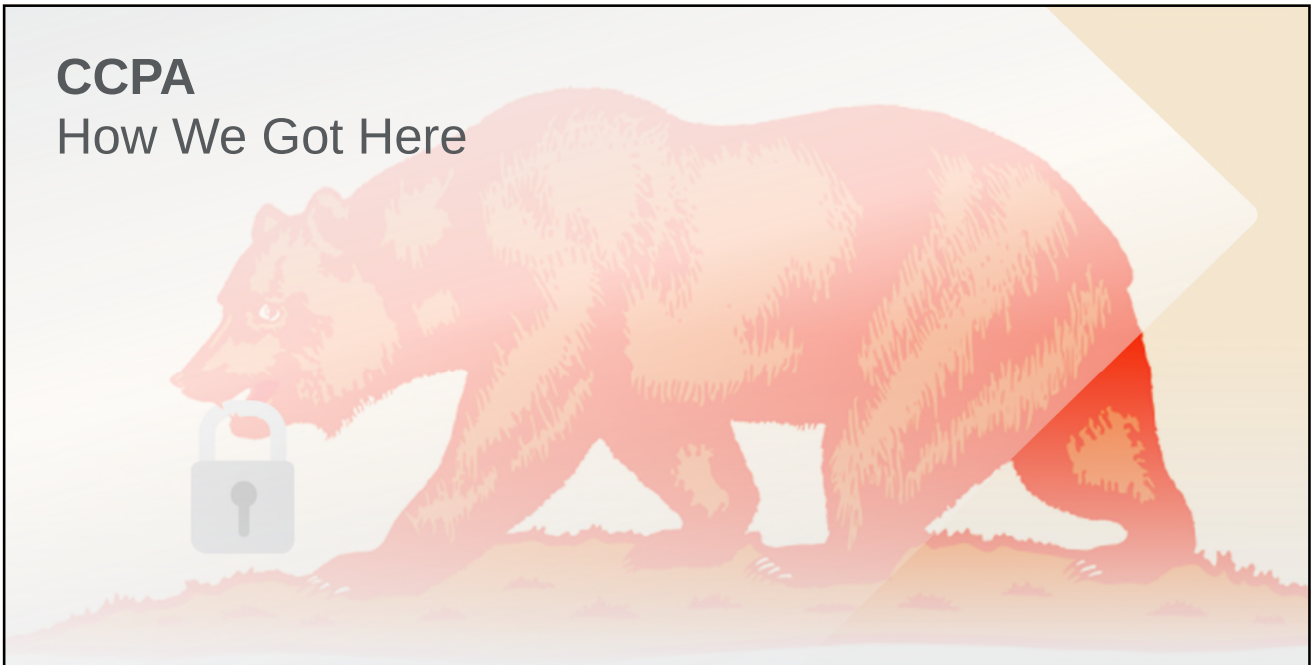
Peter Stockburger
Senior Managing Associate
San Diego
+1 619 595-8018
peter.stockburger@dentons.com


## Agenda

- Overview of CCPA
  - How We Got Here
  - Procedural Posture
  - Key Definitions
  - Summary Of Consumer Rights / Business Obligations
  - Regulations, Enforcement & Private Right of Action
  - Bells and Whistles
  - Exemptions
- Key Takeaways



## CCPA
How We Got Here



## CCPA - How We Got Here


1972 California Constitution amended to include the right of privacy as an “inalienable” right

Between 1972 and 2018 California adopted numerous privacy laws, including Online Privacy Protection Act, Privacy Rights for California Minors in the Digital World Act, Shine the Light, and Data Breach Law

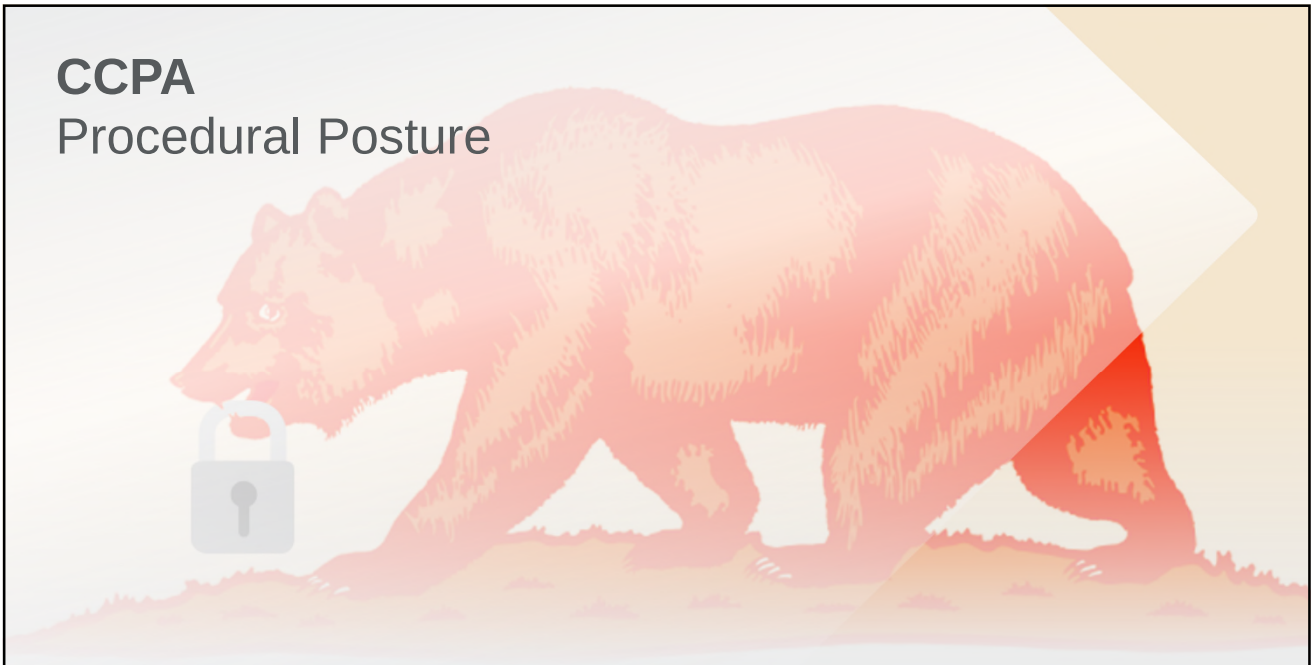
Cambridge Analytica

In March 2018 the Cambridge Analytica scandal highlighted potential privacy abuses domestically and abroad

In May 2018 Californians for Consumer Privacy announced it had obtained sufficient signatures to place the California Consumer Privacy Act on the November 2018 ballot



## CCPA
Procedural Posture



## CCPA - Procedural Posture

Passed, signed on 6/28/18 as a compromise between activists and industry


Amended 9/23/18, effective 1/20/20

AG holding public forums throughout January and February for public comment

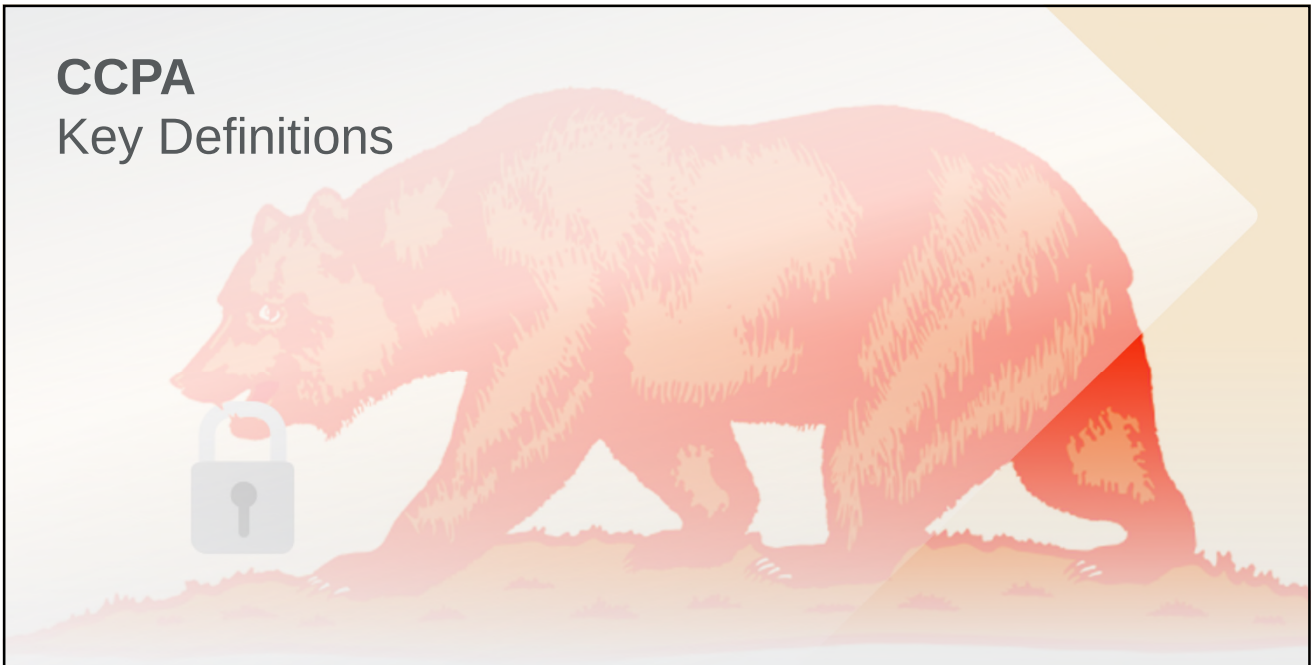


## Key Differences

### Ballot initiative v. law

| Ballot | Law |
|---|---|
| Notices to consumers | Notices to consumers |
| Right to access data | Right to access data |
| Right to opt-out of sale of information | Right to opt-out of sale of information |
| **Breach notification** | **Appropriate data security required, reference to existing data breach law** |
| **No contractual requirements for service providers** | **Contractual requirements for service providers** |
| No restrictions on processing of data, data transfers, or internal governance | Same |

# CCPA
## Key Definitions





## Key Definitions
### Drivers

Business

Consumer

Personal Information (PI)

## CCPA - Definitions and Scope
### Business Definition #1

- **Definition #1** - Any sole proprietorship, partnership, LLC, corporation, association, or "**other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners**" that:
- **(1) Collects** consumer PI, **or determines** the "purposes and means of the processing of" PI either alone or jointly with others;
- **(2) Conducts** business in California; and
- **(3) Satisfies** one of the following thresholds:
  - **Gross Revenue Threshold**. Gross revenues in excess of $25 million USD, as adjusted (Civ. Code § 1798.140(c)(1)(A))
  - **Collection Threshold**. Buys, receives, sells, or shares PI of 50,000 or more consumers, households, or devices (Civ. Code § 1798.140(c)(1)(B))
  - **Sale Threshold**. Derives 50 percent or more of its annual revenues from "**selling**" consumer personal information ((Civ. Code § 1798.140(c)(1)(A))



## CCPA - Definitions and Scope
### Business Definition #2

- **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" (Civ. Code § 1798.140(c)(2))
- "**Control**" or "**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 functions; or
  - (3) the power to exercise a controlling influence over the management of a company (Civ. Code § 1798.140(c)(2))
- "**Common branding**" means a shared name, servicemark, or trademark (Civ. Code § 1798.140(c)(2))

## CCPA - Definitions and Scope
### Consumer Definition

- A **natural person who is a California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations, however identified, including by any **unique identifier** (Civ. Code § 1798.140(g))
- **California resident** is defined in Section 17014 of Title 18 of the California Code of Regulations as every "(1) individual who is in the State for other than a **temporary or transitory** purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents"

- What is a "**unique identifier**"?
  - A "**persistent identifier**" that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; IP address; cookies, beacons, pixel tags, mobile ad identifiers; customer name, unique pseudonym, user alias, telephone numbers ,or other "**persistent or probabilistic identifiers**" (Civ. Code § 1798.140(x))
- What is **temporary or transitory** purpose?
- Definition being **challenged** during lobbying process
- **Includes** employees, competitors, business-to-business transactions



## CCPA - Definitions and Scope
### Personal Information Definition

- **Information** that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" (Civ. Code § 1798.140(o)(1))
- **Does not include** publicly available information made available from government records (Civ. Code § 1798.140(o)(2))
- **Includes**, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- **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))
- **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

# CCPA
## Consumer Rights and Business Obligations



## CCPA - Consumer Rights and Business Obligations
### Right of Disclosure - General Rights and Obligations

#### Consumer Rights

- Consumer has a **right to request** the **categories** and **specific pieces of PI** collected, sold, or disclosed (2x per year) (Civ. Code § 1798.100(a),(c))
- Request must be a "**verifiable consumer request**" (Civ. Code § 1798.100(c))
- "**Verifiable consumer request**" must be made: (1) by the consumer, (2) by a consumer on behalf of the consumer's minor child, or (3) by a natural person or person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf (Civ. Code § 1798.140(y))
- Business is entitled to "**verify**" consumer identity. Method of verification will be defined by regulations adopted by AG pursuant to Civ. Code § 1798.185(a)(7)

#### Business Obligations

- **At or before the point of collection** inform consumers about the **categories** of PI collected and **purposes** for use (Civ. Code § 1798.100(b))
- **Make available** two or more designated methods for submitting a request for PI, including "at a minimum" a toll-free telephone number and, if applicable, website (Civ. Code § 1798.130(1))
- **Disclose and deliver** the PI "free of charge" within **45 days** of "receiving a verifiable consumer request" PI looking back **12 months** (*subject to extension, denial, and exceptions*) (Civ. Code § 1798.130(2))
- **Deliver** PI through consumer account (if one), mail, or electronically at consumer option (Civ. Code § 1798.130(2))

## CCPA - Consumer Rights and Business Obligations
### Right of Disclosure - Verifiable Consumer Request

- Business is **entitled** to "**promptly**" take steps to determine whether the request is a verifiable consumer request (Civ. Code § 1798.130(2))
- Business taking steps to determine whether the request is a verifiable consumer request **does not extend** the 45 day timeline to disclose and deliver PI requested (Civ. Code § 1798.130(2))
- Business **may extend** response up to 90 days where necessary "taking into account the complexity and number of requests" if notify consumer of reasons for delay (Civ. Code § 1798.145(g)(1))
- Business **shall not require** the consumer to create an account with the business in order to make a verifiable consumer request (Civ. Code § 1798.130(2))

- **Recommended Verification Methods**
  - **Associate** the information provided by the consumer in the request to any PI previously collected by the business about the consumer (Civ. Code § 1798.130(3)(A))
  - **Request** common forms of identification or proof of identification
  - **Use** two-factor authentication or codes
  - **Follow** digital identification recognition standards promulgated by the National Institute of Technology and Standards (NIST)



## CCPA - Consumer Rights and Business Obligations
### Right of Disclosure - Privacy Policy Requirements

- **Must disclose** on: (1) online privacy policy or policies; (2) California-specific description of consumer privacy rights; or (3) website:
- A **description** of the consumer's right to disclosure (collection / sale), non-discrimination, right of deletion, right to opt-out, and one or more designated methods for submitting requests (Civ. Code § 1798.130(a)(5)(A));
- A **list** of the categories of PI collected, sold, or disclosed for business purposes about consumers in the preceding 12 months by reference to enumerated categories listed in the CCPA that most "closely describe" the PI collected, sold, or disclosed for business purpsoes (Civ. Code § 1798.130(a)(5)(B)-C))

## CCPA - Consumer Rights and Business Obligations
### Right To Opt-Out

- Right to "**opt-out**" from a sale of consumer PI from business to third party (Civ. Code § 1798.120(a))
- **Notice required** of right and sale (Civ. Code § 1798.120(b))
- **No sale** under age of 16, unless between 13 and 16 with parental consent (**opt-in**) (Civ. Code § 1798.120(c))
- "**Sell**" is defined as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to another business or third party for monetary or **other valuable consideration** (Civ. Code § 1798.140(t)(1))
- When a "**sale**" does not occur:
  - **Example #1** - When a consumer intentionally directs or uses a business to disclose the consumer's PI (Civ. Code § 1798.140(t)(2)(A))
  - **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 sale of their PI (Civ. Code § 1798.140(t)(2)(B))
  - **Example #3** - PI is disclosed to a "service provider" (Civ. Code § 1798.140(t)(2)(C))
  - **Example #4** - Business transfers PI 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 (Civ. Code § 1798.140(t)(2)(D))



## CCPA - Consumer Rights and Business Obligations
### Right to Opt-Out - Additional Notes

- **Must provide** a "clear and conspicuous link" on the business's homepage titled "Do Not Sell My Personal Information" that sends the consumer (or authorized rep) to a website to opt-out. No account should be required to opt-out (Civ. Code § 1798.135(a)(1))
- **Must include** a description of the right to opt-out, along with a separate link to the "Do Not Sell My Personal Information" page in privacy policy / California rights page (Civ. Code § 1798.135(a)(2)(A)-(B))
- **May have** a separate California rights page, and need not include it in omnibus privacy policy (strategy alignment) (Civ. Code § 1798.135(b))
- **Ensure** all individuals responsible for handling consumer inquiries about business's "privacy practices" or compliance with CCPA are informed of the right to opt-out and how to direct consumers to exercise the right (Civ. Code § 1798.135(a)(3))
- **Respect** the decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the PI (Civ. Code § 1798.135(a)(4))
- **Consumer may authorize** another person to opt-out of the sale on the consumer's behalf (subject to new AG regulations) (Civ. Code § 1798.135(c))

## CCPA - Consumer Rights and Business Obligations

### Right of Deletion - Rights and Obligations

- The right to **request** that a business **delete** consumer PI that has been collected (Civ. Code § 1798.105(a))
- Right must be **disclosed** on business privacy policy / website (Civ. Code § 1798.105(b))
- Request must be made by a **verifiable consumer request** (Civ. Code § 1798.105(c))
- Business must **delete** the consumer's PI from its records and "**direct any service providers** to delete the consumer's" PI from their records (Civ. Code § 1798.105(d))
- **Service provider** is defined as entity that "processes information on behalf of a business and to which the business discloses" a consumer's PI for a "business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing" the PI for any other purpose than specified
- Business or service provider **is not required to delete** PI if the business or service provider needs the PI to (Civ. Code § 1789.105(d)(1)-(9)):
  - **Complete the transaction** for which the PI was collected, provide a good or service requested by the consumer, or "reasonably anticipated" within the context of a business's "ongoing business relationship with the consumer," or otherwise perform a contract between the business and the consumer;
  - **Detect** security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for the activity;
  - **Debug** to identify and repair errors that impair existing intended functionality;
  - **Exercise** free speech or ensure the right of a consumer to exercise right to free speech (or any other right under the law);
  - **Comply** with the California Electronic Communications Privacy Act;
  - **Engage** in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to "all other applicable ethics and privacy laws" when the data deletion is "likely to render impossible or seriously impair the achievement of such research" if the consumer has provided informed consent;
  - **Enable** solely internal uses that are "**reasonably aligned**" with the expectations of the consumer based on the consumer / business relationship;
  - **Comply** with a legal obligation;
  - **Otherwise use** the PI "**internally**" in a "lawful manner that is compatible with the context in which the consumer provided the information"



## CCPA

### Regulations, Enforcement & Private Right of Action

# CCPA - Regulations, Enforcement & Private Right of Action

## AG Regulatory Obligations

- **AG must "solicit broad public participation and adopt regulations"** on or before July 1, 2020 (Civ. Code § 1798.185(a)) Public hearings are being held between January and February 2019. What we know so far…
- Regulations must:
  - **Update categories of PI and definition of unique identifiers** to address "changes in technology, data collection practices, obstacles to implementation, and privacy concerns"
  - **Update designated methods** to submit requests" to obtain PI
  - **Establish exceptions** necessary to comply with state or federal law, including those relating to trade secrets and IP rights
- **Establish rules and procedures**:
  - **Relating to opt-out requests**, including the type of submission, business response obligations, and the development of a uniform "opt-out logo or button" on websites (Civ. Code § 1798.185(a)(4)(A)-(C))
  - **Adjusting the monetary threshold** in January of every odd-numbered year to reflect any increase in the CPI (Civ. Code § 1798.185(a)(5))
  - **Clarity and transparency** in business notifications provided to consumer, ensuring they are easily understood by the "average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer" (Civ. Code § 1798.185(a)(6))
  - **Facilitate a consumer's ability to obtain information** with the goal of minimizing the administrative burden on consumers, including rules on verifiable request (Civ. Code § 1798.185(a)(7))



# CCPA - 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 for "guidance" on how to comply with the CCPA (Civ. Code § 1798.155(a))
- **Safe harbor** - ability to cure (Civ. Code § 1798.155(b))
- **If business fails to cure** within 30 days after being notified of alleged noncompliance, business shall be in noncompliance and violate the CCPA, subject to:
  - Injunction
  - **Liability for a civil penalty** of not more than $2,500 for each violation or $7,500 for each intentional violation
  - Penalties shall be **exclusively** assessed and recovered in an a civil action brought by the AG

### Private Right of Action

- **Limited** to when PI is: (1) nonencrypted or nonredacted; (2) subject to unauthorized "access and exfiltration, theft, or disclosure"; and resulted from the (3) 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" (Civ. Code § 1798.150(a)(1))
- **Relief includes** damages, injunctive relief, other "relief" (Civ. Code § 1798.150(a)(1)(A)-(C))
- **Statutory damages** not less than $100 and not greater than $750 per consumer per incident or "actual damages", whichever is higher. Court can consider myriad factors in determining actual damages (Civ. Code Code § 1798.150(a)(2))
- **Written notice required** 30 days prior to initiating action identifying specific violations. Business may cure by "actually" curing and providing consumer an "express written statement" of said cure. If business breaches the written statement, consumer may initiate an action to enforce the written statement and statutory damages for each breach of the express written statement that post-dates cure (Civ. Code § 1798.150(b))
- **No notice required** for action "solely for actual pecuniary damages" (Civ. Code § 1798.150(a)(2)

# CCPA
## Exemptions



## CCPA - Exemptions
### CCPA Does Not Apply To…

- **Medical information or health care providers** governed by the Confidentiality of Medical Information Act or **protected health information and covered entities** governed by the privacy, security, and breach notification rules set forth in HHS regulations pursuant to HIPAA and HITECH
- Information collected as part of a **clinical trial** subject to the Federal Policy for the Protection of Human Subjects pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the U.S. FDA
- Sale of PI to or from a **consumer reporting agency** if that PI is to be reported in, or used to generate a consumer report
- PI collected, processed, sold, or disclosed pursuant to **Gramm-Leach-Bliley Act** or **California Financial Information Privacy Act** (doesn't apply to breach section)
- PI collected, processed, sold, or disclosed pursuant to **Driver's Privacy Protection Act of 1994** (doesn't apply to breach section)
- Definition of "**medical information**" is limited
- Definition of "**protected health information**" is limited
- **GLBA** defines PI in a more limited fashion than PI is defined under the CCPA
- **California Financial Information Privacy Act** defines nonpublic personal information the same as GLBA
- **Driver's Privacy Protection Act of 1994** has a limited definition of PI that is more narrow than the CCPA

# CCPA
## Bells and Whistles



## CCPA - Bells and Whistles
### Don't Forget…

- Contractual waivers are **against public policy** and are **void** (Civ. Code § 1798.192)
- CCPA **supplements** federal and state law, and can be **preempted** by federal law (Civ. Code § 1798.196)
- Covered businesses **must ensure** that all "individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance" with the CCPA are "informed of all requirements" of the CCPA and how to direct consumers to exercise their rights (Civ. Code § 1798.30(a)(6))
- Covered businesses **cannot discriminate** against a consumer because the consumer exercises CCPA rights. Examples include:
  - Denying goods or services to the consumer
  - Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties
  - Providing a different level or quality of goods or services to the consumer
  - Suggesting the consumer will receive a different price or rate for goods or services or a different level of quality of goods or services
- Businesses **may**, however, charge a consumer a "different price or rate" or provide a "different level or quality of goods or services to the consumer," if that difference is reasonably related to the value provided to the consumer by the consumer's data (Civ. Code § 1798.125(a)(2))

# CCPA
## Key Takeaways



## CCPA - Key Takeaways
### Takeaway #1 - CCPA v. GDPR

| | GDPR | CCPA |
|---|---|---|
| **Scope** | EU personal data processed | California resident PI collected, used, sold, disclosed |
| **Right to access** | Right to access all EU personal data processed | Right to access California resident PI collected in last 12 months |
| **Right to portability** | Must export and import EU personal data in user-friendly format | Must export PI requested in user-friendly format, no import requirement |
| **Right to correction** | Right to correct errors in EU personal data processed | No right |
| **Right to stop** | Right to withdraw consent or stop processing | Right to opt-out of selling PI only |
| **Right to stop automated decision making** | Right to have human make decisions that have legal effect | No right |
| **Right to deletion** | Right to delete under certain circumstances | Same |
| **Right to equal service** | Required | Required |
| **Private right of action** | Yes | Yes |
| **Regulatory Penalties** | Ceiling of 4% of global turnover (revenue) or $20m euros, whichever is higher | $2,500 per violation, $7,500 per intentional violation, no ceiling |

## CCPA - Key Takeaways

### Takeaway #2 - Align Approach, Data Mapping / Inventory

- **Compliance v. industry leader** approach to privacy
- **Align approach** across platforms and business units
- **Data segregation** by PI and how the data is processed will need to be included within even the most mature data inventories
- **Data mapping (asset inventory)** serves as a foundational tool for adequate cybersecurity practices as well
- **Start now!** January 1, 2019 lookback
- **Don't sleep on cybersecurity**
  - Encryption / redaction safe harbor

NIST National Institute of Standards and Technology U.S. Department of Commerce

HITRUST CSF Certified

ISO 27001 International Organization for Standardization



## CCPA - Key Takeaways

### Takeaway #3 - Internal / External Policies, Processes

- **Develop internal privacy program** that includes adequate training, policies, and processes
- **Policies** to address consumer rights, how they are exercised, and who is responsible
- **Processes** so everyone understands their role (and to satisfy CCPA requirements for training)
- **Information security program** to adequately address cybersecurity requirements (asset controls, incident response plan, etc.)
- **Review third party arrangements and relationships**. If service provider, needs contract with certain protections and provisions
- **Contractual waivers are void**. (Civ. Code § 1798.192)

## CCPA - Key Takeaways

### Takeaway #4 - Third Party Assessments

- **Gap assessments** can help determine course of action
- **Law firm advantage** - privileged report
- **Dentons advantage**
  - Leading global governance, privacy, cybersecurity firm
  - Leading in **cybersecurity** (*BTI 2017*)
  - Leading in **client service** (*BTI 2018*)



BTI CLIENT SERVICE 30 for 2018



# Thank you

大成DENTONS

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.