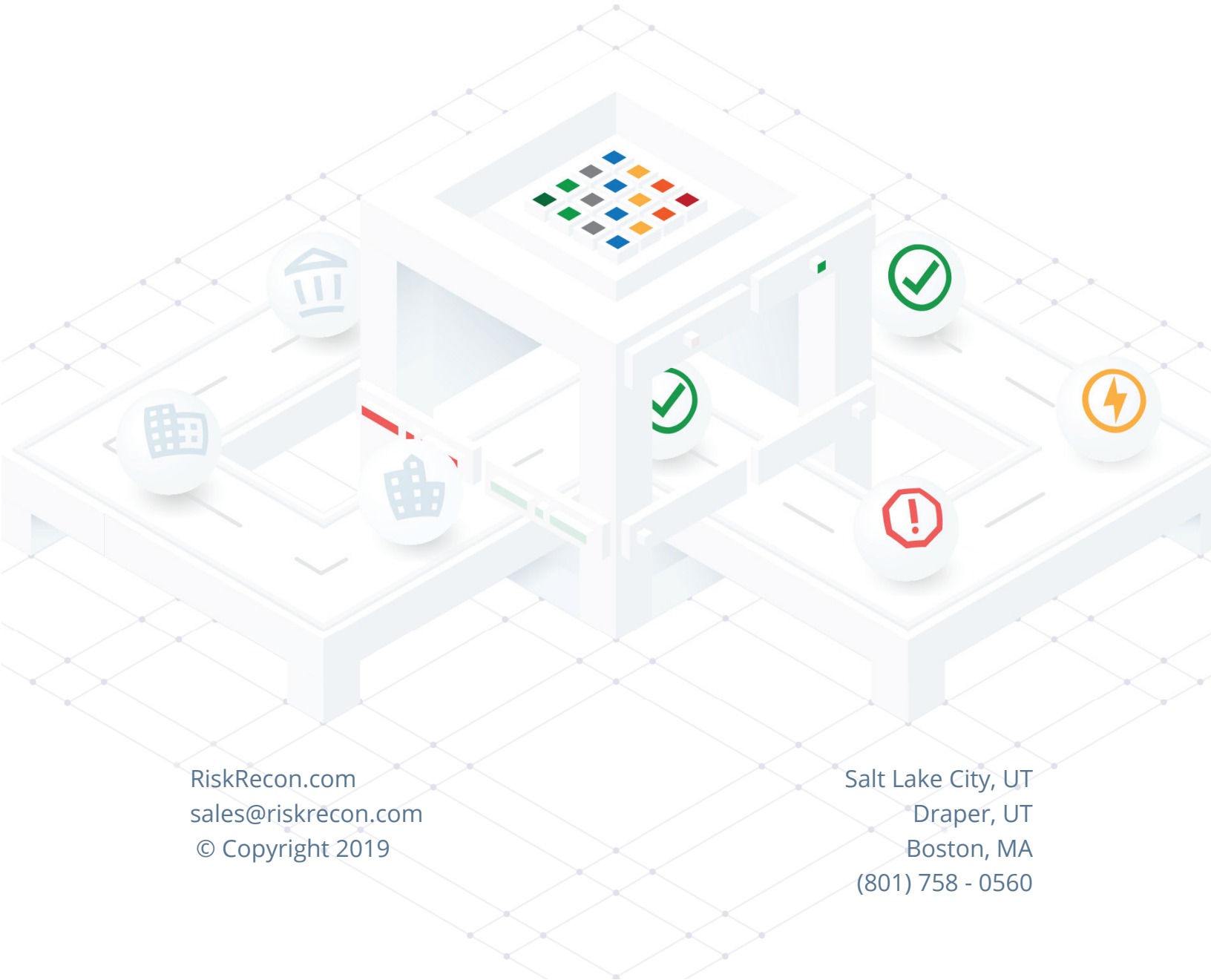




The Impact of the California Consumer Privacy Act

A guide for understanding the new data privacy regulation



RiskRecon.com
sales@riskrecon.com
© Copyright 2019

Salt Lake City, UT
Draper, UT
Boston, MA
(801) 758 - 0560

Table of Contents

CCPA: Scope & Definitions

3

CCPA: Requirements

5

CCPA: Enforcement & Fines

11

CCPA: Scope and Definitions

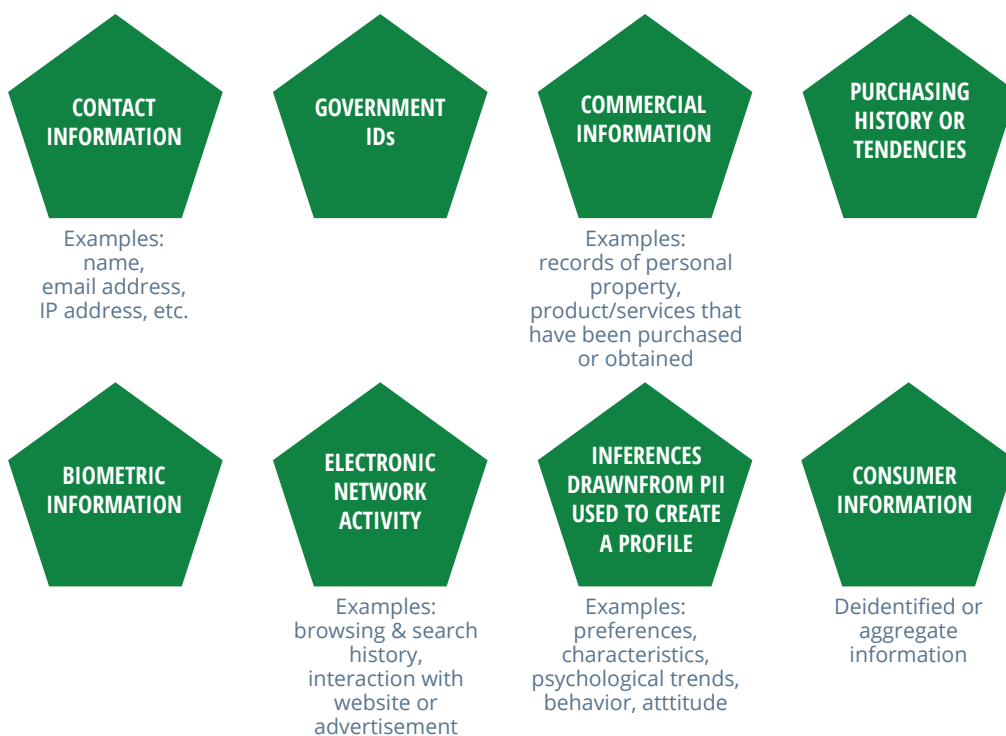
The right to privacy is regarded around the world as a fundamental human right. In fact, the UN's Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. . ." Recent events have shown, though, that many organizations have been consistently & routinely disregarding peoples' right to privacy. In this piece we will discuss the California Consumer Privacy Act and its impact on your organization.

Definition of Personal Information (PII)

When CCPA goes into effect on 1 Jan 2020, it will become one of the most impactful, general data privacy regulations in the United States. While other regulations, like HIPAA, deal with specific types of PII, CCPA broadly defines PII:

"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."

The bill contains examples of PII, though explicitly states that this list is by no means exhaustive:



Information made available from federal, state or local government records is not classified PII



Who the Law Covers

Individuals

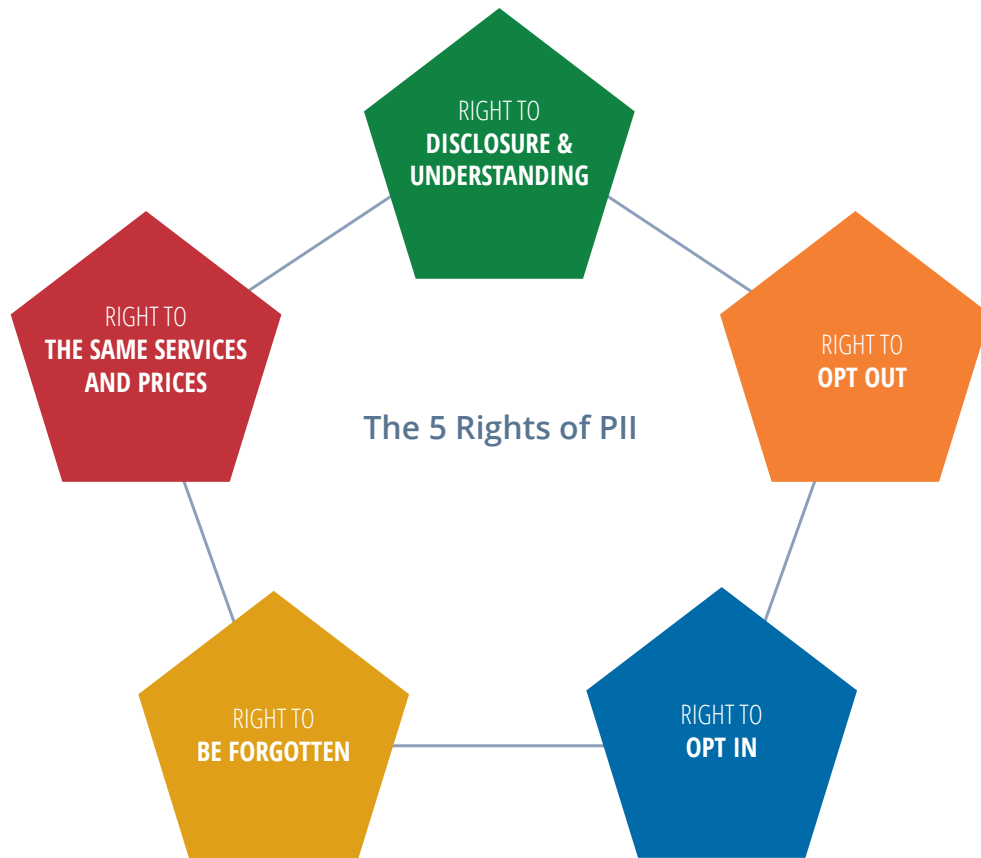
CCPA covers the processing of PII of residents of California ("processing" is, essentially, any interaction with personal data). With California being the world's fifth largest economy (as of May 2018), this regulation will undoubtedly affect many organizations.


Organizations

Any organization that collects, sells or transfers PII of California residents (referred to hereafter as "individuals").

CCPA: Requirements

CCPA specifies five privacy rights individuals have and the standards organizations must follow in order to respect those rights. In this section, we'll describe CCPA's specific requirements for each privacy right as well as the Act's general provisions.





Recent events have shown that many organizations have been consistently and routinely disregarding peoples' right to privacy.

General Requirements

In addition to specific requirements for each right, CCPA has some general requirements as well. Organizations that process California residents' PII must:

- For minors (i.e., anyone under the age of 16 years-old):
 - Consent to sell their PII must be obtained prior to any sales
 - For minors under the age of 13, explicit consent from the minor's parent/guardian must be obtained
- Implement and maintain a security program that appropriately protects the types of PII the organization processes
- Update their online privacy policy to include a California Resident-specific section that contains:
 - A description of the individual's privacy rights under CCPA
 - At least one method for submitting requests
 - A list of the categories of PII the organization has collected about consumers during the previous 12 months
 - Two separate lists describing how consumers' PII was:
 - a. sold
 - b. disclosed
 - If no PII has been sold or disclosed in the previous 12 months, disclose this fact
 - Update this privacy policy annually
- Have a clear and obvious link on their homepage entitled "Do Not Sell My Personal Information" that links to a webpage that enables individuals to opt-out of the sale of their PII
 - Individuals must not be required to create an account in order to direct the organization to not sell their PII
- Third parties that the organization sells or discloses to may not sell PII they (the third party) have received from the organization unless individuals have:
 - Received explicit notice of the intent to sell their PII
 - Been given an opportunity to opt-out



1. The Right to Disclosure & Understanding

Individuals have a right to know what PII the organization has collected on them and what the organization is doing with that PII.

Requirements

1. Organizations that collect PII must disclose to individuals that they have a right to have their PII deleted (i.e., the “right to be forgotten”)
2. Organizations must respect individual's request for information and, upon a verifiable request from an individual, disclose the following to the requesting individual:
 - a. The categories and specific pieces of PII that the organization has been collecting about the individual
 - b. The categories of sources from where the individual's PII has been collected
 - c. The business purposes for collecting the individual's PII
 - d. If the organization is selling PII, it must disclose:
 - i. The business purposes for selling the individual's PII
 - ii. The categories of:
 1. PII that was sold about the individual
 2. Third parties to whom the organization has sold the individual's PII
 - e. If the organization is disclosing PII, it must state the categories of:
 - i. Third parties to whom the organization has disclosed the individual's PII
 - ii. The categories of PII that have been disclosed about the individual
 - f. If the organization hasn't sold or disclosed any PII, it must state this fact

Exceptions

Organizations are not required to:

1. Retain any personal information related to a one-time transaction
2. Reidentify or otherwise link any data that, in the ordinary course of business, is not considered to be PII



CCPA specifies five privacy rights individuals have and the standards organizations must follow in order to respect those rights

2. The Right to Opt-Out

Individuals may opt-out of having their information sold.

Requirements

1. At anytime, an individual can direct an organization or its third parties to not sell their PII
2. When an individual opts-out of having their PII sold, the organization must:
 - a. Respect that decision going forward
 - b. Respect the individual's decision for at least 12 months
 - i. After 12 months, the organization may ask the individual organization may sell their PII
 - c. Not use any PII collected to full the individual's request

3. The Right to Opt-In

Minors must opt-in to having their data sold

Requirements

1. Organizations may not knowingly sell the personal information of minors
 - a. A minor is anyone under 16 years old
 - b. If the minor under 13 years old, explicit consent from the minor's parent/guardian must first be obtained
2. Organizations that willfully disregard an individual's age will be considered to have had actual knowledge of the individual's age



4. The Right to be Forgotten

Individuals may have their data deleted.

Requirements

1. 1. Individuals have the right to request that an organization delete any or all of the individual's PII that the organization has on the individual
 - a. Organizations must disclose this right to individuals
2. When an organization receives a verifiable request from an individual to have their PII deleted, organization must:
 - a. Delete the individual's PII from its records
 - b. Direct any and all third-parties that had the individual's PII to delete the individual's PII from their records

Exceptions

Organizations are exempt from complying with an individual's request to have their PII deleted if the PII is needed to:

1. Do any of the following:
 - a. Complete a transaction for which the personal information was collected
 - b. Enable internal activities that are reasonably aligned with the consumer's expectations of the business
 - c. Provide a good/service either:
 - i. Requested by the consumer
 - ii. Reasonably anticipated within the context of the business's ongoing business relationship with the consumer
 - d. Perform a contract between a business and the consumer
 - e. Detect security incidents
 - f. Protect against activities that are:
 - i. Malicious
 - ii. Deceptive
 - iii. Fraudulent
 - iv. Illegal activities
 - g. Prosecute those responsible for the aforementioned activities
 - h. Internally & lawfully use the individual's PII for other purposes in which the consumer provided the information
2. Identify & repair errors (e.g., debug) that impair existing, intended functionality
3. Allow for the:
 - a. Exercise free speech, either by the individual or another individual
 - b. Exercise of another right that's provided by law
4. Comply with the California Electronic Communications Privacy Act
5. Engage in the scientific, historical or statistical public or peer-reviewed research if:
 - a. The deletion of data is likely to seriously impair or make impossible the research
 - b. The research is in compliance with all applicable ethics and privacy laws
6. Comply with other laws & regulations



5.

The Right to the Same Services & Prices

Individuals are entitled to the same services and prices regardless of if they exercise their privacy rights or not.

Requirements

Organizations may not discriminate against individuals if they exercise any of their privacy rights, including but not limited to:

1. Denying goods/services to the individual
2. Charging the individual different prices or rates for goods/services, including through:
 - a. Providing discounts or other benefits
 - b. Imposing penalties
3. Actually offering or suggesting that the individual will receive a different level or quality of goods/services
4. Organizations may, however offer financial incentives (e.g., payments) to consumers for doing any of the following with a consumer's personal information:
 - a. Collecting
 - b. Selling
 - c. Deleting
5. Organizations offering financial incentives must notify individuals of these financial incentives
6. The material terms of the program must be clearly described
7. Businesses may not use financial incentive practices that are any of the following in nature:
 - a. Unjust
 - b. Unreasonable
 - c. Coercive
 - d. Usurious
8. Organizations may enter consumers into a financial incentive program only if the individual:
 - a. Chooses to opt-in
 - b. Can opt-out at anytime

Exceptions

Organizations may charge a different price/rate or a different level/quality of goods/services if that difference is reasonably related to the value provided to the individual by the individual's data.

CCPA: Enforcement & Fines

What Constitutes a Violation

1. An organization is in violation of CCPA if it fails to cure any alleged violations within 30 days of being notified of the potential violation
2. A “potential violation” is considered to have occurred when:
 - a. Any individual's unencrypted or non-redacted PII has been exfiltrated, stolen or disclosed in an unauthorized manner
 - b. The unauthorized exfiltration, theft or disclosure was a result of the business not implementing and maintaining a security program that appropriately protects the types of PII the organization handled

How an Organization Can be Fined

Individuals may bring a civil lawsuit (individual or class-action) against organizations who have potentially violated CCPA. This lawsuit may only occur if all of the following conditions are met:

1. The individual has provided the organization with 30 days' notice
 - a. The notice must specifically identify how the organization is believed to have violated (or be violating)
2. Within 30 days of filing a suit, the individual instigating the lawsuit must notify the California Attorney General that action has been filed
 - a. The Attorney General must do one of the following within 30 days of receiving the aforementioned notice:
 - i. Notify the individual that the Attorney General intends to prosecute within 6 months
 1. If the Attorney General does not prosecute within 6 months, the consumer may proceed with their action
 - ii. Refrain from acting within 30 days, allowing the consumer to proceed with their action
 - iii. Notify the individual that the individual may not proceed with their lawsuit

An organization may not be sued if all of the following conditions are met:

1. A fix is possible
2. The business:
 - a. Fixes the alleged issue within 30 days of the notice
 - b. Notifies the individual that the violations have been cured and that no further violations will occur
3. If an organization continues to violate CCPA, the individual may initiate action against the business

Fines

Fines are categorized into two types of violations - intentional and unintentional violations.

Fines for Intentional Violations

Any organization, service provider or person that intentionally violates CCPA is liable up to \$7,500 per violation.

Fines for Unintentional Violations

The following civil actions may be imposed on a violating CCPA:

1. Whichever is greater:
 - a. A fine of \$100–\$750/individual per incident
 - b. Actual damages to the individual
2. Injunctive¹/declaratory² relief
3. Any other relief the court deems proper

When assessing how much to fine, the courts are to consider any relevant information related to the case, including:

1. The nature/seriousness of the misconduct
2. The number of violations
3. The persistence of the misconduct
4. The length of time of the misconduct
5. The willfulness of the defendant's misconduct
6. The defendant's:
 - a. Assets
 - b. Liabilities
 - c. Net worth

Other Info

Any organization or third-party can receive guidance from California's Attorney General on how to comply with CPPA

¹**Injunctive relief:** A court-ordered act or prohibition

²**Declaratory relief:** When requested by one of the parties in court, a judge determines the parties' rights under law, with the hope that an early doing so will resolve some (if not all) of the case's issues

Sources

- https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
- <https://www.un.org/en/universal-declaration-human-rights/>
- <https://support.apple.com/en-us/HT208931>
- <https://www.cbsnews.com/news/california-now-has-the-worlds-5th-largest-economy/>