recollective

Recollective & the CCPA

What is the CCPA?

On June 28, 2018 the California Legislature passed the **California Consumer Privacy Act** (CCPA). It was signed into law on October 11, 2019 and became effective on **January 1, 2020**.

The legislation creates significant new requirements for identifying, managing, securing, tracking, producing and deleting consumer privacy information. It is very similar to the **General Data Protection Regulation** (GDPR) introduced in May 2018 by the European Union.

Among other things, the CCPA grants California consumers new privacy rights:

- The right to know what personal information businesses collect about them and request a copy of or delete such information
- The right to opt out of the sale of personal information
- The right to hold businesses accountable for not safeguarding their personal information, including the right to bring a lawsuit for data breaches

Who must comply?

As a threshold, the CCPA applies to for-profit businesses that collect and control California residents' personal information, do business in the State of California, and meet one of these three requirements:

- Have annual gross revenues in excess of **US$25 million**; or
- Receive or disclose the personal information of **50,000 or more California residents**, households or devices on an annual basis; or
- Derive **50 percent or more** of their annual revenues from selling **California residents'** personal information.

Organizations exempt from the act include small companies that do not meet any of the above requirements, as well as public agencies and non-profit organizations. Also, any information collected while commercial conduct takes place "wholly outside California" is exempt. In addition, the Act applies to any entity that controls or is controlled by a covered business or shares a common branding with a covered business, such as a shared name, service mark, or trademark.

Why is CCPA important?

Although CCPA primarily affects California residents, any business that conducts substantial activity in California and collects, sells, or discloses California consumers' personal information may be subject to CCPA. California is also considered a trendsetter when it comes to U.S. privacy laws, so other states will likely follow suit. Since CCPA was passed in June 2018, many states have introduced similar new laws and bills.

Opt-In vs. Opt-Out

Unlike Europe's General Data Protection Regulation (GDPR), the CCPA does not require consumers to "opt in" for the sale or use of their personal information. However, the CCPA requires very specific privacy notices as well as providing the right to opt out of the sale or use of personal information. Furthermore, businesses are prohibited from "discriminating" against consumers in the event they exercise these opt-out rights.

These notices need to inform consumers about what personal information categories will be collected and the intended use or purpose for each category. The CCPA requires that businesses provide specific information to consumers and establishes delivery requirements. Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.

Key Definitions

Personal Information

The CCPA defines personal information extremely broadly as "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."

In other words, the State recognizes a "broad list of characteristics and behaviours, personal and commercial, as well as inferences drawn from this information" that can be used to identify an individual.

Examples of covered personal information include:

- Personally identifiable information such as name, address, phone number, email address, social security number, driver's license number, etc.
- Biometric information, such as DNA or fingerprints.
- 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.
- Inferences drawn from any of the above examples that can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.

The CCPA does not restrict a business's ability to collect, use, retain, sell, or disclose consumer information that is deidentified or aggregated. However, it does set a high bar for claiming data is deidentified or anonymized. Data that has been pseudonymized may still be considered personal information under the CCPA's broad definition of personal information, because it remains capable of being associated with a particular consumer or household.

Selling

The CCPA defines "selling" as "renting, disclosing, releasing, disseminating, making available transferring, or otherwise communicating personal information for monetary or other valuable consideration." Note that selling does not necessarily involve a payment to be made in exchange for personal information.

Processing

The CCPA defines "processing" as "any operation or set of operations that are performed on personal data" by either automated or not automated means. However, the term "processing" is only used in the definitions section.

Consumer Rights

The CCPA takes the position that consumers "own" their privacy information and provides them five general "rights" for their personal information. Under the Act, California consumers will have the right:

To know what personal information is collected about them: Consumers will have the right to know, through a general privacy policy or notice (and with more specifics available upon request) what personal information a business has collected about them, its source, and the purpose for which it is being used.

To know whether and to whom their personal information is sold/disclosed, and to opt-out of its sale: Companies that provide or make consumer data available to third parties for monetary or other valuable consideration are deemed to have sold the data and will need to disclose this. Subject to certain exceptions, consumers will then have the further right to opt out of the sale of this information by using the "Do Not Sell My Personal Information" link on the business' home page, which is required by the Act. Moreover, those 16 years-old and under must opt in to have their information sold. Note that the term "sold" is not limited to the actual sale of

privacy information but can be interpreted broadly to include sharing of privacy information with other parties.

To access their personal information that has been collected: Consumers will have the right to request certain information from businesses, including the sources from which a business collected the consumer's personal information, the specific elements of personal information it collected about the consumer, and the third parties with whom it shared that information. The Act requires that businesses provide specific means for consumers to submit these requests, typically a toll-free number and a web link. Once the request is made, businesses must disclose the requested information free of charge within 45 days, with extensions of time available in certain circumstances.

To have a business delete their personal information: Consumers can request that personal information a business has collected be deleted. Some personal information is exempt from deletion requests, including information under legal hold (until the matter is adjudicated or until the hold is released) and for information that must be retained per legal or regulatory record keeping requirements.

To not be discriminated against for exercising their rights under the Act: The CCPA gives consumers the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act. As such, businesses may not "discriminate" against consumers for exercising these privacy rights. They cannot deny goods or services, charge different prices, or provide a different quality of goods or services to those consumers. There are some exceptions, however, on the service levels that can be provided.

Comparison to GDPR

The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data, whether the information was obtained online or offline.

The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered to be one of the most significant legislative privacy developments in the country.

Like the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy.

Key Differences

Disclosure requirements: GDPR had significant and unintended consequences for the market research industry, specifically by requiring the full identification of a research sponsor (namely, the brand commissioning the research study). As known to the industry, upfront sponsor

acknowledgment can create response biases. By comparison, CCPA compliance only requires category identification.

Opt-in requirements: Unlike the GDPR, which effectively requires a lawful base in order to collect personal data, California's new law is effectively "opt-out" because it does not require explicit consent (opt-in) to collect data and it doesn't have any defined legal grounds for processing.

Definition of personal information: CCPA covers California residents and protects personal information reasonably linkable to an individual consumer or a household, while GDPR covers EU data subjects (both business and consumer users) without regard to citizenship or residency requirements and protects personal data related to an individual only.

Covered entities: CCPA applies only to for-profit companies that meet certain minimum thresholds, while GDPR applies to all types of organizations, including public bodies and non-profit organizations.

Covered data: CCPA specifically excludes personal information covered by current federal privacy laws, such as the Health Information Portability and Accountability Act (HIPAA) or Gramm-Leach-Bliley Act (GLBA), while GDPR applies to all categories of personal data.

Consumer rights: Both CCPA and GDPR grant consumers the right to access a copy of their personal data or request that a business delete their personal data. CCPA's deletion right applies only to personal information collected from the consumer, while GDPR's deletion right covers all personal data regarding a data subject, regardless of the source.

Sale of data: CCPA allows California residents to opt out of the sale of their personal information, while GDPR allows a data subject to request the deletion of their data or that processing be restricted.

Security breaches: Unlike the European privacy requirements under GDPR, the CCPA does not directly impose data security requirements. However, it does establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law.

For an extensive comparison of the two laws, we recommend downloading "Comparing privacy laws: GDPR v. CCPA" (PDF download) by the Future of Privacy Forum. With regard to consumer rights, see pages 30 to 37.

Recollective and CCPA

By definition of the law, the California Consumer Privacy Act (CCPA) does not directly apply to Recollective. We may, on occasion work with an organization that must be compliant and thus we are committed to actively supporting our customers in meeting their legal requirements.

In 2018, Recollective conducted a privacy overhaul in preparation for the GDPR. The steps taken in both features and legal agreements will also support our customers wishing to be be compliant with the CCPA. We added features to collect consent, monitor opt-outs, export personal information, delete personal information for select users and more. At no time do we resell personal data in any way and our standard agreements stipulate this in writing.

Ultimately, responsibility for CCPA compliance is that of the organization utilizing Recollective. Such organizations may wish to revise their privacy policies, introduce updated consent statements (agreements), limit their data collection and carefully document their data usage, processing and storage upon completion of the study in Recollective.

Updated privacy statements can be added as a click-through agreement within Recollective and/or added as a persistent link in the footer of the Recollective site.

Please review our resource regarding Recollective and the GDRP to learn more about specific features in Recollective such as the ability to target the erasure of personal data for single user or group of users upon a request to be forgotten.

You may also wish to make use of the Agreements feature in Recollective to gain explicit consent on the collection of personal data and to provide another mechanism for consumers to opt-out of the research study and the use of their personal data.

If you plan to sell personal information, as defined by the CCPA, we suggest adding an optional agreement with the statement, “Do Not Sell My Personal Information”. The agreement will be presented to all registering participants and be unchecked by default. Smart Segments can be used to automatically group participants based on their response to agreements.