Willeke Kemkers & Gretchen Ramos – Greenberg Traurig

# The California Consumer Privacy Act – The U.S.'s first try at a GDPR-like data protection law

**The GDPR – often referred to as the most comprehensive and far-reaching data protection law in the world – is no longer unique, both in the sense of its territorial scope and its privacy protection.**

In Brazil, the 'Lei Geral de Protecao de Dados Pessoais' ('LGPD') enters into force on August 15, 2020. The *LGPD*, just like the GDPR has an extraterritorial effect and aims to enhance the protection and control of privacy rights by consumers. In Thailand, the Personal Data Protection Act was approved on February 28, 2019 which is planned to enter into force on May 27, 2020. Just like GDPR, this act governs personal data under a broad definition, while it also has an extraterritorial scope. Data controllers and data processors in and outside Thailand are affected by the act.

In addition, beginning on January 1, 2020, the state of California will have a new data protection law, the 'California Consumer Privacy Act' ('the CCPA'). Unlike the GDPR, the CCPA is not territorial, rather it applies to businesses that process California residents' personal information, even when those businesses themselves are not in California. The CCPA is expected to have a large impact on the digital marketing industry. All the more reason to take a closer look at this latest addition to the privacy law family.

## Background

The call for a legal instrument to protect consumers from the continuously growing and increasingly powerful marketing and tech companies was present for quite some time. This call was, amongst others made by Alastair Mactaggart, who had become aware of Google's extensive knowledge about its users through a friend who worked at Google. After he became aware of these practices, Mactaggart worked tirelessly, with the assistance of a team of privacy experts on a new law for the protection of Californian consumers' privacy. He decided to dedicate his own time and money ($ 3,5 million) into this new law. Certain events in 2018 would change the process and the public opinion about this new law almost entirely.

The Cambridge Analytica scandal made more people aware of how companies were using and handling their data. The fact that personal information was harvested for political purposes on such a large scale (87 million users) without the users themselves being aware, led to the U.S. public to focus on personal data protection.

"Many prominent privacy groups were not in favor of Mactaggart's proposal."

Besides this major scandal, more companies suffered from extensive data breaches in 2017 and 2018.

With public opinion in favor of and the focus on a new privacy law to protect California's 40 million residents, the California Constitution expressly providing a right to privacy and with Mactaggart able to leverage the state's ballot initiative process, the CCPA was quickly signed into law on June 28, 2018. It was passed just a few days after its introduction to the California legislature as many organizations feared the proposed law would be enacted through the ballot process, which would have prevented them from later seeking to amend the law through the legislative process. In fact, in October 2018 and 2019, California's governor enacted several amendments to the CCPA text.

Important to note is that many prominent privacy groups were not in favor of Mactaggart's proposal. Some argued that the entire set up of the CCPA needed to be different; evolving around informed consent (similar to GDPR) rather than a regulated opt-out. Others simply did not agree with Mactaggart's approach and advocated for a much less stringent law.

Given the process of drafting and signing the CCPA into law moved so quickly, it is incomplete and contains confusing provisions that leave many important issues unresolved and companies struggling to understand what compliance actually requires.

Additionally, the California Attorney General's proposed CCPA regulations ("CCPA Regs") issued on October 10, 2019, in many ways added more confusion. While providing more detail, the CCPA Regs propose many 'new' requirements on businesses, and they are subject to public comment until December 6, 2019.
Thus, it is certain that they will not be finalized by the CCPA's January 1, 2020 effective date, leaving companies to further revise their CCPA compliance practices again in 2020 when the Regs are finalized.

## Similar to the GDPR?

*A bit, but much less comprehensive*

The CCPA is sometimes referred to as the American GDPR, or the 'GDPR-light'. In fact, the CCPA's definition of 'personal information' is as broad, and in some ways even broader than the GDPR's definition of 'personal data.' However, the actual similarities between both laws are in fact quite minimal.

The CCPA introduces consumer rights which are conceptually similar to those in the GDPR. Californian residents now have, for example, the right of access to their personal information, the right to be forgotten and the right of data portability. In addition, the CCPA obliges businesses to provide information about their processing activities in a privacy notice.

A closer look at the actual provisions however, shows that the effects of these rights in practice shall differ from those in the GDPR. One example is that many more exceptions apply to the right to be forgotten, which makes this right much weaker than its EU counterpart. In addition, the CCPA Regs propose a two-step deletion process requiring a consumer who requests deletion to confirm again the deletion (like a double-opt out) before the business honors the request.

In addition, while the GDPR is an all-encompassing law, covering privacy by design or default, legal bases for processing and data governance, the CCPA is not. Rather, the CCPA is a first attempt at limiting companies' large-scale monetization of California residents' personal information and increasing consumers' control of how and when their personal information is used. The most important and remarkable elements of the act are assessed below.

## Who must comply?

*Applies to any organization in the world that meets the CCPA's definition of business*

The CCPA applies to a 'business'. The CCPA's definition of business includes for-profit legal entities that determine the processing purposes and means of California residents' (consumer) personal information and that do business in California.

As mentioned, the CCPA's territorial scope is not limited to the location of the business. Consequently, a business

that is established outside California but does business in California, is also affected if it meets this criteria and at least one of the following:

- (a) it has annual gross revenues of more than $ 25,000,000
- (b) it alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;
- (c) it derives 50 percent or more of its annual revenues from selling consumers' personal information.

"The CCPA is an opt-out law that focuses on 'selling' of personal information, and providing consumers the right to opt-out of the sale."

The above requirements illustrate the purpose of the CCPA, which is the protection of consumers' rights from the large-scale use and monetization of their personal information by the major commercial companies. Also, an organization that does not meet the definition above, but is controlled by or controls an organization that meets the above 'business' definition and shares common branding, is subject to the CCPA.

Non-profits, small businesses, and businesses without a data focus are exempted. This is contrary to the GDPR, where almost every organization that processes personal data falls under the regulation's scope.

### Who is protected?

*Consumers, which includes all California residents*

As the name itself reveals, the CCPA protects consumers. A consumer is defined as a natural person who is a Californian resident. In October 2019, the CCPA was amended to include certain exceptions to this qualification, for example where the consumer acted as an employee, job candidate, owner, director or contractor or when personal information from employee of another company that is collected in a business relationship. While these categories are not entitled to assert any individual rights, a business will still need to provide notice of the personal information collected and the purpose of such collection to the first category.

Moreover, these carve-outs will end on January 1, 2021, making all the CCPA provisions applicable to these individuals. Apart from these exceptions, the definition of consumer is quite clear and is not a major source of confusion.

### What is protected?

*Personal Information in the broadest sense of the word*

A definition that is considered unclear and ambiguous, is that of personal information. Whereas personal data under GDPR only covers 'any information relating to an identified or identifiable natural person', personal information encompasses:

*'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'.*

As personal information encompasses *information which could reasonably be linked, directly or indirectly, with a particular consumer or household*, no actual identification of an individual person is required. Even information that is linkable to a household is considered personal information.

In addition, the CCPA gives the following greatly varying examples of personal information:

- 'classic' personal information such as names, email addresses, IP addresses and phone numbers;
- 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 audio, electronic, visual, thermal, olfactory, or similar information; 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.

In addition to this all-encompassing definition of personal information, the activities regulated under the CCPA extend far beyond the GDPR.

### Do consumers have the right to control how their personal information is used?

*Kind of, but only after the personal information is shared*

While the GDPR focuses on controllers having a legal basis for processing, the CCPA focuses on how personal information is used – and specifically defines the processing that constitutes a business purpose or a commercial purpose. And while both laws are premised on giving the user more control, how they do this drastically differs. The GDPR is an opt-in law requiring a data subject's consent where other legal basis are not applicable to a processing activity, whereas the CCPA is an opt-out law that focuses on 'selling' of personal information, and providing consumers the right to opt-out of the sale of their personal information. However, contrary to what you would expect, this term 'sale' does not refer to 'giving or handing something over in exchange for money'. The definition is much broader:

*'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 a third party for monetary or other valuable consideration'.*

The sole transfer of personal information for any type of valuable consideration or benefit is thus also a form of selling. One specific type of such transfer, which takes place on a large scale, concerns the transfer of personal information (collected by cookies) to analytic companies. As such transfer takes place to analyze and improve the functioning of a website this is considered 'for valuable consideration' so that the CCPA applies.

An interesting related element, which has caused some late-night thought experiments (with the authors), is that certain exceptions to 'selling' apply. One such exception is

> "Besides the right to opt out, consumers have the right to be informed about processing activities and their rights with regards to these activities."

when the consumer consents to the sale of its personal information. However, in case of transfers of personal information to analytic companies, which then transfer the information further to third parties for other commercial purposes, the consent must concern both transfers.

This obviously is problematic for the analytics company as it is not in direct contact with the relevant consumers. The burden to obtain the two forms of consent then shifts to the first company (that collects the cookies), but requesting two forms of consent – and explaining why this is necessary - is almost undoable. It is also highly questionable whether the consumer will take the required time to read and understand the message, for the consent to be considered genuine and reliable. Up until now, no suitable solution has been found for this issue, other than for businesses to provide consumers with the right to opt-out of having their information shared in such situations.

### Consumers' rights under CCPA

*A mixed bag*

Consumer rights under the CCPA are conceptually similar to data subjects' rights under the GDPR, but the practical effect of the rights differ greatly.

Under the CCPA, consumers can file access requests. These access requests may concern personal information collected or sold. Strangely, consumers must be informed by a reference to eleven pre-determined categories of personal information, such as 'identifiers', 'biometric information' and 'geolocation data'. The same goes for the 'categories of sources from which the personal information was collected' and the 'categories of third parties with whom the business shares personal information'. Following the notice requirements as written, either results in a very long privacy notice for California residents or a chart of information that is incomprehensible to the average consumer.

This hardly seems to meet the CCPA's goal of businesses providing more transparency on how they process consumers' personal information. Moreover, the variations mean that global companies with presence in the EEA and the U.S. will thus need different response policies and language for both types of access requests.

Secondly, consumers have the right to opt out of the sale of their personal information. Information about this right must be provided in a way that is easy to read and understandable to an average consumer. The actual notice itself must be displayed on the business's Internet homepage, with a link titled 'Do Not Sell My Personal Information'. In addition, a special opt-out button or logo may be used, but this does not seem to be an obligation.

"Besides Attorney General actions, consumers have a civil right of action for violations of the CCPA's security provisions."

Besides the right to opt out, consumers have the right to be informed about processing activities and their rights with regards to these activities. This specifically applies to financial incentives, such as client programs. Such financial incentives (including payments as compensation) may be offered to consumers for the collection, sale or deletion of personal information. The business may also offer different prices, rates or quality of goods or services if that price or difference relates to the value of the consumers' information. Businesses must however explain to consumers why the incentive is permitted, together with an estimation of the data's value in relation to the financial incentive. A description of the value's calculation method must also be provided. The CCPA Regs contain different calculation methods for the business. This practical approach illustrates the Californian legislature has clearly been more successful than the European legislature in moving forward with valuing personal information, and providing data subjects with the right to monetize their personal information.

Lastly, the CCPA Regs propose that large businesses that annually buy, receive, sell, or share for commercial purposes the personal information of more than four million consumers must keep track of all consumers' rights requests. They should be able to disclose the number of access, deletion and opt-out requests, the number of accepted or denied requests as well as the median number of days it took before the business responded to such request. This new requirement is expected to put a great administrative burden on these businesses.

### Penalties and enforcement - *and a thirty day cure period for 'curable' violations*

Pursuant to the CCPA, the Attorney General may initiate civil action to seek an injunction and impose civil penalties on a business for violation of the CCPA. The penalties are $ 2,500 per violation or $ 7,500 per intentional violation.

Surprisingly however (most certainly for legal practitioners familiar with GDPR), a business is only in violation if it 'fails to cure an alleged violation within 30 days after being notified of alleged noncompliance'. The perceptions of such curable violation under the CCPA differ, but one could imagine that the complete lack of a system with which individual rights can be tracked and managed, may not be curable within 30 days. A violation of the duty to inform consumers online is obviously much easier to cure.

While penalties of $ 2,500 or $ 7,500 may seem low, these amounts will be calculated per consumer. In case of a sale of personal information against the will of 100,000 consumers, the fine may amount up to $ 250 million or even $ 750 million in case of an intentional violation.

Besides Attorney General actions, consumers have a civil right of action for violations of the CCPA's security provisions. A consumer may initiate a civil action if its personal information is subject to unauthorized access and exfiltration, theft and/or disclosure as a result of the business's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. The required actions range from recovery of damages (not less than $ 100 and not greater than $ 750), injunctive or declaratory relief or 'any other relief' the court deems proper.

### Outlook – *A moving target*

With the public comment period for the CCPA Regs ending December 6, 2019, it is certain they will not be finalized until sometime in 2020. In October 2018, the CCPA was amended so that its enforcement would begin six months after the CCPA Regs are finalized or July 1,

"The U.S. seems to be headed in the direction of providing consumers with more control over how their personal information is used."

2020, whichever date is sooner. January 1, 2020 however, remains the date on which compliance is required. The enforcement of the CCPA shall take place by taking into account the preceding six months, so businesses should not consider these months as extra time for working towards compliancy.

In September 2019, Mactaggart published the California Privacy Rights and Enforcement Act of 2020, a ballot initiative correcting some grey areas in the CCPA, and providing consumers with even greater rights to control their personal information. If it progresses as Mactaggart plan, this new privacy law will be on the ballot for the November 2020 election, and will replace CCPA. Thus, businesses subject to the CCPA can expect a rocky, ever-changing compliance landscape over the next twelve months.

As a more general outlook into the future, global companies will be challenged to adapt a global privacy strategy that complies with all extraterritorial privacy laws. A patchwork of national approaches and policies no longer seems viable. In particular, marketing activities and strategies will need to be reconsidered (as illustrated with the issue about consent and opt-out for third party analytic and behavioral advertising cookies). The U.S. seems to be headed in the direction of providing consumers with more control over how their personal information is used, with data protection legislation introduced in various other states and as the federal level in 2019.

Given that the U.S. is driven by commerce, it seems unlikely it will ever completely adopt a data protection law that requires the same transparency and provides data subjects with the control that they have under the GDPR. However, what appears certain is that there will be more data protection legislation introduced in the U.S. in 2020, so stay tuned as the CCPA is likely just the beginning of many changes to come on the U.S. data protection front.

**In short:**

- The CCPA aims to protect all Californian residents and their personal data from businesses even those located outside California;
- The CCPA holds a broader definition of personal data than the GDPR does;
- This act compels businesses to keep a keen eye on their administration, since it grants the consumer residing in California a considerable right to information in which said businesses are obliged to inform their consumers on the handling of their personal data.

**About the author**
Willeke Kemkers is an associate at Greenberg Traurig's Amsterdam office and specializes in Intellectual property and Privacy / data protection. She is also a member of Greenberg Traurig's global privacy team. In that capacity she worked at the San Francisco office with Gretchen Ramos, where she advised clients about GDPR and CCPA compliance.

**About the author**
As co-chair of Greenberg Traurig's Data, Privacy & Cybersecurity practice, Gretchen works with a variety of companies in determining the steps to take concering compliance with applicable data protection laws, including the GDPR, the CCPA, and various other U.S. laws. She regularly assists clients with DPIAs, data breaches and represents clients in data protection regulatory investigations.