The Promise and Pitfalls of the California Consumer Privacy Act

By Salome Viljoen (Cornell Tech | New York University)
The Promise and Pitfalls of the California Consumer Privacy Act

By Salome Viljoen (Cornell Tech | New York University)

Beginning on January 1 of this year, California’s Consumer Privacy Act (the CCPA) went into effect. The CCPA is the first bill of its kind in the US. The law is widely considered to provide the strongest consumer data protection in the US, and has been the subject of considerable speculation (and lobbying) since it began as a popular referendum in 2017. While the CCPA does offers a suite of consumer protections to California residents, it also has several shortcomings that may significantly undermine some of the law’s most ambitious protections for privacy in the digital age. Below, I offer an overview of the bill as well as a few thoughts on what it does (and does not) achieve for consumer privacy.

Like any other law, the CCPA is best understood in two parts: the rights and protections it confers, and the scope of its application. This overview will consider the CCPA’s strengths and limitations along both dimensions—the substance of the protections the law affords, and how broadly its protections (and the exceptions to them) are applied.

Several features set the scope of a law’s application: the jurisdictional boundaries, the size of companies, and class of consumer to which the law applies, and the range of activities that are included or excluded. By including or excluding certain categories of activity or information from key definitions, and explicitly excluding certain activities from protection, the range of activity covered by the bill can be significantly expanded or reduced. Thus, the overview below covers both the protections and new authority the CCPA grants, and discusses how a few key terms have been defined, before offering some thoughts on key shortcomings in the law.

A. History
The CCPA began life as a statewide ballot initiative, started by businessman Alistair Mactaggart in September 2017.1 The initiative initially met with fierce opposition from industry, particularly companies like Facebook and Verizon. However, as the Cambridge Analytica scandal broke, technology companies—fearing additional bad PR—eased back their opposition.2 In a last minute attempt to stave off

1 In California, citizens can circumvent the legislative process, putting a proposed referendum on the ballot for voters to approve directly. To do so requires receiving the qualifying number of signatures, 5 percent of the votes cast for the last gubernatorial election. In 2017, this meant 365,880 signatures were required to get the referendum on the ballot in November 2018. By May 2018, the ballot initiative had 629,000.
2 See Committee to Protect California Jobs, Cal. Secretary of State, http://cal-access.sos.ca.gov/Campaign/Committees/Detail.aspx?id=1401518&session=2017&view=received; see also Sasha
the referendum (growing in popularity alongside public anger) the tech industry urged the legislature to step in and reach a compromise form of legislation. In June 2018, after reaching an agreement with its sponsors, the California General Assembly unanimously passed a version of the CCPA, signed into law by the Governor to take effect January 2020, and the ballot initiative was withdrawn.

**B. General Features of the CCPA:**

Along with additional consumer rights in the event of a data breach, the CCPA’s main function is to grant five key consumer rights with respect to the previously unregulated collection and use of consumer data. These rights apply only to California residents, with respect to commercial conduct undertaken in California, and only to companies that collect data on at least 50,000 people per year or have revenue of over $25 million a year.

**B.i. Data Access Rights and Enhanced Transparency.**

First, the law grants several forms of data access rights to Californians. Some are affirmative obligations at the point of collection, and some are at the request of the consumer:

1. The right to know that personal information is being collected about the consumer, before or at the time of collection, and the categories and purposes of collection.3
2. The right to know that consumers may request deletion of their data.4
3. Upon request, the right to know the categories and specific information being collected about the consumer.5 This includes the categories (though not the specific entities) of the *sources* from which information has been collected, and of the *third parties* with whom the business shares personal information.6
4. Upon request, the right to know whether the consumer’s personal information is being sold or disclosed to third parties for a business purpose.7 If it is, a consumer may request additional information regarding this information, including the categories of personal information being collected, the categories of third parties buying the information as well as the personal information sold to each kind of third party, and the categories of third parties to which information was disclosed.8

---

3 California Civil Code, Div.3, Part 4, Title 1.81.5, California Consumer Privacy Act of 2018, §§1798.100-1798.199 (hereafter referred to as the CCPA); §1798.100 (b)
4 CCPA, §1798.105 (b)
5 CCPA, §1798.100 (a)
6 CCPA, §1798.110
7 CCPA, §1798.110(3)
8 CCPA, §1798.115
B.ii. Data Deletion Rights
A consumer may also request deletion of any personal information collected by the business. This request covers not only personal information held by the business of which the request is made, but also any personal information held by service providers of the business. However, this right is subject to several exceptions, some of which are discussed further below.

B.iii. Opt-Out Right
Another first in the US, Section 1798.120 of the CCPA gives consumers the right to opt-out of the sale of their personal information. Any business that does sell personal information has to provide clear notice to consumers that information may be sold and of their right to opt-out, by linking to a form on their homepage (though they may maintain a separate homepage for California consumers) titled “do not sell my personal information”.

B.iv. Non-discrimination
Businesses are not allowed to discriminate against consumers exercising their rights under the CCPA, by denying them goods or services, by lowering the quality of goods or services, or by charging (or suggesting they may charge) a different price for goods or services. Importantly, this non-discrimination right extends to consumers exercising the right to opt-out of sale of their personal information. However, like the opt-out right, the non-discrimination right is subject to several important exemptions.

B.v. Data Portability
The CCPA also provides some measure of data portability, requiring personal information requests delivered electronically to be in a “portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.”

Alongside these new consumer rights, the CCPA confers new authority on the California Office of the Attorney General. It grants the Office standing to sue for noncompliance with the law and for failures to safeguard consumer data. It also gives the Office the power to promulgate new regulations under the CCPA, as well as the authority to issue opinions and guidance on compliance with the law. The Office is actively working to issue new rules clarifying consumer rights and providing guidance for businesses on how to comply.

---

9 CCPA, §1798.105
10 CCPA, §1798.135
11 CCPA, §1798.125
12 CCPA, §1798.100(d)
13 CCPA, §1798.185
D. Key Definitions

As is true with all legal documents, the definitions section is key to evaluating the CCPA. Several of its greatest strengths and weaknesses lie in the way the law defines certain terms.

The law’s definition of “personal information” is more comprehensive than any other US law—an important win for privacy advocates, since like other consumer privacy laws, the CCPA’s protections and rights only apply to personal information. Thus, what is covered under the term functionally defines the scope of the law.

It includes anything 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.” The definition goes on to list several examples, notably including “inferences drawn” from any other personal information to create a profile of the consumer. The inclusion of inferences is significant, and suggests that, unlike under the GDPR, certain profiling activities would fall under the CCPA definition of “personal information.”

While more robust than other definitions, the CCPA’s definition of “personal information” leaves open a few key ambiguities discussed further below. Most notably, the original language in the bill as passed defined personal information to include anything that “is capable of being associated with” a consumer. Although reasonability can be established in several instances to provide consumers with protection, the introduction of the standard does shift more discretion towards businesses.

The definition of “personal information” (and thus the applicability of many of the rights and obligations of the law) also includes notable exceptions. First, it excludes “publicly available information,” from the definition, arguably its biggest exception and a key way in which the scope of the law may be limited. It also generally excludes from the requirements of the law (in other words, gives companies free rein to “collect, use, retain, sell or disclose”) de-identified information and “aggregate consumer information,” which is information that “relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.” This exception is significant from an industry perspective, since trading in aggregate consumer information and the insights derived from them make up the core of the platform and mobile app industries. Nevertheless, the definition of “aggregate consumer information” is fairly good, since it wouldn’t allow businesses to get around protections of personal information simply by de-linking a few types of information, or simply by tracking a unique identifier linked to a phone rather than a person.

---

14 CCPA, §1798.140
15 CCPA §1798.140(o)(1)
16 CCPA §§1798.140(a), 1798.145(5)
The definition of “de-identified” information is also stronger than in other US laws. Laws like HIPAA, for example, define de-identified information narrowly, based on whether information excludes certain enumerated identifiers commonly thought of as sensitive, like birthday and social security number. Yet today, individuals are identifiable using a wide range of fairly innocuous-seeming data. This means that in practice, information that is “de-identified” to this legal standard can readily be used to identify someone in the wild. CCPA takes a functional approach to de-identification to close this glaring loophole. Under the CCPA, de-identified information means information that “cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer,” and imposes conditions of technical safeguards and business processes on businesses to ensure such information is not reidentified. Again, this language was the subject of some lobbying, and the subsequent introduction of the “reasonableness” standard for identification provides businesses with some discretion in how they exempt information from the consumer rights the CCPA provides.

E. Shortcomings of the CCPA
The CCPA creates a suite of consumer digital privacy rights, but the law has several limitations. Ultimately, these shortcomings significantly undercut the law’s ability to provide the kind of sweeping consumer privacy it might otherwise have offered Californians.

Many of the limitations of the CCPA stem from a more general one: since its inception, the law has been the subject of a sustained, effective lobbying campaign from industry that has managed to win several exceptions and exclusions during the time between the bill being signed into law in 2018 and becoming effective this January. Lobbyists have been particularly focused on limiting privacy protections for worker data, weakening the definition of “de-identified data”, and allowing businesses to discriminate based on access to consumer data, requesting data in exchange for discounts and loyalty benefits. This industry pressure is likely to continue, with the lobbying focus now shifting to the Attorney General’s office as it issues guidance under the new law.

While several of these shortcomings reflect the erosion of the bill over its lifecycle from referendum to law, others were due to structural or conceptual decisions in the CCPA from its onset. Most notably, law never transcended the mold of a consumer rights bill; giving rights over access to information, but not prohibiting certain purposes to which consumer information may be put, such as targeting, profiling or sale of information to data brokers. Instead, it relies on mechanisms of consumer requests and consent to regulate these activities, in the mold of other US consumer privacy laws.

18 CCPA §1798.140(h)
The law’s limitations may be broken down into three rough categories: ambiguities, absences, and exclusions. Some mechanisms in the law are ambiguous, clearing the way for lobbying efforts to secure favorable readings in advisory opinions from the Attorney General’s office. Other shortcomings stem from rights and protections that have been excluded from the law’s scope altogether, and rights and protections that are included, but subject to significant exemptions or limitations that weaken their effect.

E.i. Ambiguities

Some of the key definitions and exclusions in the CCPA create significant ambiguities around how the law may apply to certain activities and kinds of information.

For example, “inferences drawn” from other forms personal information are considered personal information, which suggests that profiling activities using inferences to target a consumer based on their behavior, preferences or attitudes, may fall under the protections of the law. However much of this activity stems from behavioral models that are arguably based on “aggregate consumer information,” used to create profiles that may infer similar things about a consumer, but stemming from more generalized population-level insights, and thus excluded from the definition of personal information. How broadly the law will end up applying to profiling activities thus remains unclear.

Another notable ambiguity concerns the definition of “publicly available information.” While the law does explicitly exclude biometric information collected by a business “without the consumer’s knowledge” (and thus capturing activity like Clearview AI’s scraping of publicly searchable face images), it leaves open the possibility of companies scraping non-biometric information from public searches that may nevertheless lead to invasive practices.

E.ii. Absences

A few absences in the law are worth highlighting.

1. Workers. Protections and rights for employees and contractors over their information are notably absent in the law. In fact, personal information collected about workers in the process of hiring, employment, and administering benefits are explicitly excluded from its application. This absence is notable, since greater protections for employee information were included in the original referendum bill.

2. Information related to credit rating. This exemption is meant to prevent the CCPA conflicting with existing privacy regulations over credit information, but is a shame, since in several instances the CCPA provides stronger rights than other laws regulating credit information.

3. Information related to health. Similar to credit, this exemption is tailored and worded to avoid conflicting with prior regulations, but also means that health information regulated by other laws

20 CCPA, §1798.145(h)
are broadly excluded from the rights granted under the CCPA. Along with credit information, this means that two categories of information over which consumers may be most interested in exercising these rights are not subject to them.

4. Private right of action. Perhaps the most significant absence from the law is a private right of action for individuals to sue companies for noncompliance with its rights and obligations. This is one of the notable ways in which the law differed from the goals of the referendum, and led to one of the architects of the initial referendum, Mary Stone Ross, calling the final version of the CCPA “largely toothless.” Instead, the law grants only the Attorney General’s Office standing to sue, creating significant resource constraints for enforcement. In fact, the AG’s office anticipates it only has resources to bring about 3 cases a year under the new law.

E.iii. Exemptions

The law is also weakened via several exemptions to the rights and obligations it does have.

1. Exemptions to the deletion right. A business or service provider is exempt from consumer requests to delete their information if that information is necessary for a number of functions. Some of these functions are reasonable, such as the need to complete the transaction with the consumer or to fulfill the terms of a warranty or recall. Some are in fact admirable, such as the exemption allowing companies to contribute information to scientific research with the informed consent of the consumer. Other exemptions have the potential to functionally negate the right to deletion altogether. For example, there are broad exemptions for internal uses “reasonably aligned with the expectations of the consumer,” and for exercising free speech, as well as “ensur[ing] the right of another consumer to exercise that consumer’s right of free speech, or exercise[ing] another right provided for by law.” Given the troubling trend of technology and other companies using free speech jurisprudence to fight a broad swathe of regulations, this exemption has big consequences for the CCPA.21

2. Exemptions to the non-discrimination clause. The non-discrimination right has also been subject to sustained lobbying. While the original referendum language, like that of the current law, contained some ambiguities, lobbying efforts from industry have secured some significant exceptions to the non-discrimination right. The result is language that seems at best vague, and at worst contradictory in a manner that may negate the right entirely. While the clause states that businesses may not charge “a consumer a different price or rate,” or provide “a different level or quality of goods or services to the consumer,” companies may in fact engage in these exact forms of discrimination, as long as they are “reasonably related to the value provided to the

---

business by the consumer’s data;” a low bar that almost any company, and certainly a technology company, should be able to meet. Moreover, while businesses may not use “discounts or other benefits” (again, unless reasonably related to the value the data provides) they may offer “financial incentives” including compensation, to consumers for their data. The difference between these two categories is economically indistinguishable, and legally unclear.

3. Opt-in versus opt-out. A final big concession in the law was the decision to move in a variety of places from opt-in to opt-out, most particularly with respect to the right to not have one’s personal information sold to third parties. This shifts the burden onto consumer’s to affirmatively exercise their rights, rather than onto companies to affirmatively seek permission to engage in these activities, as they must under the GDPR.