An Introduction to the California Consumer Privacy Act (CCPA)

Professor Eric Goldman*
Santa Clara University School of Law
July 1, 2020

By spending about $3M of his personal fortune, a California real estate developer with a yen for privacy and money to burn qualified a privacy initiative for the November 2018 California statewide ballot. If passed by voters, the initiative's language—which contained numerous provisions that were toxic to the business community—would have been exceptionally difficult to amend, functionally locking in problematic policy permanently.

Following the ballot certification, the developer offered the California legislature a "deal": if it immediately passed a law substantially similar to the initiative, he would withdraw the initiative from the ballot.[1] This deal was attractive to all sides. The developer would get his desired policy outcome without spending millions more to sway voters. Meanwhile, for opponents and the legislature, passing a bill would retain the legislature's power to improve and superintend the law over time, plus the opponents would avoid spending an estimated $100M to fight the initiative.

In a chaotic 7 day period in June 2018, the California legislature introduced, amended, and enacted AB 375, the California Consumer Privacy Act ("CCPA"). The legislature didn't hold any hearings on the law and, behind closed doors, it got minimal input from affected stakeholders. This is how California got a sweeping, lengthy, insanely complicated, and poorly drafted privacy law that governs the world's fifth largest economy (and beyond).

Following passage of the CCPA, the California legislature made numerous, but mostly cleanup or minor, amendments in 2019. The legislature will likely adopt a few more (mostly minor) amendments in 2020.

In parallel, the law required the California Attorney General's Office (the "DOJ") to develop regulations, a process that took two years. The DOJ issued its final regulations in June 2020, just a few weeks before the DOJ could start enforcing the law.

Collectively, the CCPA and regulations create a 21,000+ word unreadable mess. This note provides a roadmap to the law, but *bonne chance* if you ever have the misfortune of reading the law yourself.

Who Has to Comply With the Law?

The law applies to any business that "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others,

* Professor of Law, Santa Clara University School of Law; Co-Director, High Tech Law Institute; Supervisor, Privacy Law Certificate. Website: http://www.ericgoldman.org. Email: egoldman@gmail.com. This chapter is excerpted from ERIC GOLDMAN, INTERNET LAW CASES & MATERIALS (2019)

[1] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley —and Won*, N.Y. TIMES MAG., Aug. 14, 2018, https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

determines the purposes and means of the processing of consumers' personal information, that does business in the State of California" and satisfies one of these three requirements:

1) has $25M+ in annual revenues (from anywhere, not just California), or
2) derives 50%+ of its revenues from selling consumer data, or
3) "annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices" (1798.140(c)).

The law excludes the collection or sale of "a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California[, i.e.,] if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold" (1798.145(a)(6)). Despite this apparent overreach into activity occurring in other states (which raises significant Constitutional problems), the law only applies when companies are "doing business in California." Due to the ambiguity of what qualifies as "doing business" in a state, many out-of-state businesses have felt compelled to comply with the law despite not having any employees or property in California.

The law expressly says it is "not limited to information collected electronically or over the Internet[; the law applies] to the collection and sale of all personal information collected by a business from consumers" (1798.175). Thus, the law applies equally to online and offline businesses that collect personal information. The DOJ estimated that the CCPA applies to up to 400,000 businesses in California, including many small- and medium-sized businesses.[2]

The law reaches so many small businesses because it covers any business that "receives…the personal information of" 50k+ consumers, including the "receipt" of credit cards and IP addresses. A business can clear that threshold with an average of 137 unique credit card sales per day (14 sales/hour over a 10-hour business day)—which describes many restaurants, coffee shops, pizzerias, frozen yogurt shops, and other low-revenue retailers. Similarly, the law applies to any ad-supported website that "receives" an average of 137 unique IP addresses per day, a tiny amount of traffic. While the ballot initiative really targeted the data practices of Google and Facebook, the law counterintuitively treats a local pizza shop the same as it treats Internet giants.

What is "Personal Information"?

The law applies to consumers' "personal information." "Consumers" are natural persons who are California residents (1798.140(g)), including customers, prospective customers, employees/contractors, and business contacts (like vendor salespeople). In 2019, the California legislature excluded employees/business contacts from the law for a year; it may temporarily renew this extension in 2020.

[2] *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std399.pdf.

As with the GDPR, attempts to distinguish personal information from non-personal information are likely to be under- or over-inclusive.[3] The CCPA took the overinclusive route. The law defines "personal information" as 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" (1798.140(o)). The statute specifies many examples of personal information, including geolocation data, biometric information, and olfactory information. The reference to "household," an undefined term not in the GDPR, creates numerous potential problems, but the regulations mostly ameliorated those concerns.

Because computer scientists are clever about reidentification and combining datasets, what data *isn't* reasonably capable of being associated with a particular consumer? For example, standing alone, a person's gender isn't a unique identifier; it only narrows the potential pool of people who might be that individual by roughly half. However, knowing a person's birthdate, zip code and gender allows the accurate unique identification of 87% of the population.[4] So the CCPA likely treats gender information—*standing alone*—as "personal information" because it is "reasonably capable of being associated with" a particular consumer when combined with other datasets. Applying the same logic to other data types, it's likely that *all* data about individuals possessed by a business qualifies as "personal information."

"Personal information" excludes "information that is lawfully made available from federal, state, or local government records" (1798.140(o)(2)) and "consumer information that is deidentified or in the aggregate consumer information" (1798.145(a)(5)). However, it's unclear if data can be sufficiently deidentified or aggregated to satisfy the statutory standards; and the scope of the government records exception also remains unclear.

The CCPA categorically does not apply when other specified privacy laws apply, such as information covered by Health Insurance Portability and Accountability Act of 1996 (1798.145(c)(1)), Fair Credit Reporting Act (1798.145(d)), Gramm-Leach-Bliley Act (1798.145(e)), Driver's Privacy Protection Act of 1994 (1798.145(f)), and more.

Consumer Rights Created by the Law

The CCPA provides six consumer rights:

1) and 2) "Right to Know" and Right of Data Portability

The CCPA lets consumers learn about businesses' data practices (both online and offline). Businesses are required to make disclosures about their generic collection practices (1798.100) and their data sales or transfers (1798.115). Upon request, businesses must also disclose the specific categories of personal information they have collected from the consumer and the "specific pieces of personal information it has collected about that consumer," in a portable format (1798.110). The CCPA has detailed requirements for

[3] See, e.g., Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010)
[4] LaTanya Sweeney, *Simple Demographics Often Identify People Uniquely*, Data Privacy Working Paper 3. Pittsburgh 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf.

privacy policies (especially 1798.130(a)(5)), and the regulations add many more requirements. For example, web pages containing the statutory disclosures must comply with W3C accessibility standards.

These rights create pathways for malefactors to illegitimately obtain highly valuable consumer data. To prevent this outcome, the CCPA required the DOJ to define what constitutes a "verifiable consumer request." (1798.140(y)). The DOJ mostly told businesses to figure it out, saying that "determining the appropriate verification standard is fact- and scenario-specific" and providing a multi-factor test for businesses to ponder. As a result, businesses often must make individualized assessments for each verification request, a process that is not scalable for businesses receiving many requests.

To ease the burden slightly, the DOJ provided some categorical rules:

- A business can decline a request when it can't reasonably verify the consumer.
- Password-protected accounts often qualify as reliable verifiers.
- For consumers' requests to know the categories of information collected about them, businesses may match "at least two data points provided by the consumer with data points maintained by the business."
- For consumers' requests to know their specific data, businesses may match 3 data points with their records and require consumers to sign a declaration of identity under penalty of perjury. The "penalty of perjury" sounds serious, but unless the DOJ actually prosecutes perjured declarations, it's an empty threat. For deletion requests (as opposed to right to know requests), the DOJ says businesses should decide between the 2- or 3-data point approach depending "on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion."
- In commentary, the DOJ said that businesses can require consumers to obtain notarization only if the business covers the notary costs.

3) Erasure Right (1798.105). Upon a consumer's request, a business shall delete any personal information about the consumer that the business collected from the consumer.

Businesses can refuse deletion requests when it "is necessary for the business or service provider to maintain the consumer's personal information" to: (1) complete the transaction or a reasonably anticipated transaction, (2) find, prevent, or prosecute security breaches or illegal activity, (3) "Debug to identify and repair errors that impair existing intended functionality," (4) exercise free speech (of the business or a third party) or "exercise another right provided for by law," (5) comply with the California ECPA, (6) engage in certain types of research in limited cases, (7) "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business," (8) comply with a legal obligation, or (9) "Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

4) Right to Say "No" to Data Sales

Consumers can control businesses' ability to sell their data:

- *Opt-Out of Data Sales* (1798.120(a)). Consumers can opt-out of sales of their personal information, and the business can't ask them to reconsider for at least 12 months (1798.135(a)(5)) with limited exceptions specified in the regulations.
- *Opt-In for Data Sales Related to Minors* (1798.120(d)). A business that knows (or "willfully disregards" the consumer's age) personal information related to consumers under 16 may not sell the personal information unless the consumer (ages 13-15) or parent/guardian (under 13) opts-in.
- *Opt-Out of Third-Party Data Resales* (1798.115(d)). "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out."
- *Specifications for Disclosing Opt-Out of Data Sales* (1798.135). If a business sells personal information, then it must "[p]rovide a clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information."

The CCPA defines "sale" broadly to include any disclosure from one business to another "for monetary or other valuable consideration" (1798.140(t)(1)). Due to the ambiguous meaning of "other valuable consideration," the law potentially applies to many legitimate activities and data transfers that are not straight cash-for-data.

5) Non-Discrimination Provisions (1798.125).

"A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title," though a business may 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." Businesses may offer "financial incentives" (circularly defined as "a program, benefit, or other offering, including payments to consumers, related to the collection, retention, or sale of personal information") to compensate for the collection, sale or deletion of data, but not if the financial incentives are "unjust, unreasonable, coercive, or usurious in nature." The regulations provide numerous formulas to value data for justifying any price or service discrimination.

6) Private Right of Action for Data Breaches.

The law creates a private cause of action when "nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' 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" (1798.150). In those cases, consumers may obtain the greater of actual damages or statutory damages within a range of $100-$750 "per consumer per incident." To proceed with this private cause of action, consumers must first give the defendant a 30 day cure period; and if the business is able to cure the problem (whatever "cure" means in the context of a data theft), statutory damages become unavailable.

"User-Enabled Global Privacy Controls"

The regulations added a provision (not in the statute) requiring businesses to honor "user-enabled global privacy controls," defined as signals communicated through browser software or plug-ins indicating that consumers want to opt-out of data sales. This technology does not exist today, so the DOJ speculated that it might emerge in the future. This provision has numerous serious unresolved issues:

- How to interpret the signals when multiple consumers share the same browser software.
- How businesses can determine that new technology constitutes user-enabled privacy controls. The DOJ does not certify software as satisfying the legal standard, so businesses are supposed to figure it out themselves. There may be thousands of software programs and apps that might qualify, and monitoring all of them—on the off-chance that they suddenly became a "user-enabled global privacy control"—will be costly and overwhelming for even technologically sophisticated businesses.
- How the technology will be granular enough to effectuate the consumer's opt-out intent. If a consumer globally sends the opt-out signal to all websites, this will likely lead (due to the overinclusive definition of data sales) to unexpected consequences, such as losing access to key services the consumer actually wants.

Because the technology does not currently exist, most businesses are likely to ignore this provision until the DOJ makes further public announcements.

Transparency Reports

In another provision newly added in the regulations, a business that "buys, receives for the business's commercial purposes, sells, or shares for commercial purposes" personal information for 10+ million California consumers in a calendar year must publish a transparency report about certain types of consumer requests and their processing times and decisions. The DOJ claimed that these transparency reports will help it with enforcement priorities and provide valuable data to researchers, though those benefits remain highly speculative and come at a substantial cost to complying businesses.

Who Can Enforce the CCPA?

Other than consumers' private right of action for data breaches, the law does not allow for private causes of action (1798.150(c)), either directly or through indirect means like California Business & Professions Code § 17200, which ordinarily creates a civil claim for legal violations. Plaintiffs are testing this restriction in court.

Except for data breaches, the law can be enforced only by the California Attorney General's office (1798.155), and only after giving businesses a 30 day cure period (1798.155(b)). Civil penalties can run up to $2,500 "per violation," though if violations are intentional, the cap increases to $7,500 per violation (1798.155(b)).

The Future

The CCPA continues to evolve dynamically. The California legislature will likely enact additional amendments in 2020. The DOJ will begin enforcing the law, which will signal its enforcement priorities. Some of those enforcements may spill over into court, though contested enforcements will be rare because most businesses will correct violations in the 30-day cure period or strike a deal with the DOJ. There could also be prospective challenges to the law, but that seems unlikely.

The November 2020 ballot will include a new ballot initiative, the California Privacy Rights Act of 2020 (CPRA), an additional 20k+ words of law from the same team that funded the CCPA ballot initiative. Yes, before we know how the CCPA works, and while we are in the middle of a pandemic and a related economic depression that is already devastating small- and medium-sized businesses and the California economy, and while we are focusing on a presidential election with massive stakes for our country, the ballot proponents think it's a great time to abandon the CCPA "experiment," waste a ton of investments that have been already made by both governments and businesses to accommodate the CCPA, create a brand new government agency from scratch, and make significant parts of consumer privacy law impossible to superintend except through additional ballot initiatives. This decision to pursue a new initiative before the CCPA even became effective is a profound rejection of legislative governance. It also disrespects the hard work and significant expense that businesses invested to jump through the CCPA's onerous hoops.

Whether or not CPRA passes, the future of privacy regulation seems more dystopian than promising. The CCPA is problematic on its own. When other legislatures clone-and-revise it, the ensuing multi-state regulatory thicket will be overwhelming. Plus, there could be further privacy-related California ballot initiatives post-CPRA–which could create a perpetually moving target and a usurpation of legislative governance.

As a result, preemptive federal legislation is the only remaining path to achieve sensible consumer privacy regulation. Unfortunately, Congress has a full docket of structural problems to address, so it's likely we'll see more terrible privacy regulatory outcomes before Congress prioritizes solving the privacy regulatory challenge for the country.