An Introduction to the California Consumer Privacy Act (CCPA)

By Prof. Eric Goldman*

July 9, 2018

After spending about $3M, a California real estate developer with a yen for privacy and money to burn qualified a substantial privacy regulation as an initiative for the November 2018 California statewide ballot. If passed by voters, the initiative's language—which had numerous provisions that were toxic to the business community—would be exceptionally difficult to amend, functionally locking in problematic policy permanently.

Following ballot certification, the developer offered the California legislature a "deal": if it passed a law substantially similar to the initiative, he would withdraw the initiative from the ballot. This deal was attractive to all sides. The developer would get his desired policy outcome without spending the millions more needed to contest the $100M that opponents threatened to spend to fight the initiative. Meanwhile, for opponents and the legislature, passing a bill would retain the legislature's power to improve the language over time, plus the opponents would avoid spending the $100M that wouldn't guarantee defeat of the initiative.

This led to a chaotic 7 day period in which, with little or no input from most affected stakeholders, the California legislature introduced, amended and enacted AB 375. The result is a sweeping, lengthy (10,000 words!), insanely complicated, and poorly drafted privacy regulation that will govern the world's fifth largest economy. Needless to say, this rushed and non-inclusive process created a law with many defects, ranging from typos and drafting errors to terrible policy ideas. Everyone anticipates that the legislature will further amend the law to fix a few of its many rough edges, though it's not clear exactly what changes are likely; and the bill delegates some rule-making authority to the California Attorney General (AG), and the implications of that rule-making are also not clear. The law goes into effect January 1, 2020.

Who's Covered by 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, 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, 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."[1]

* Professor of Law, Santa Clara University School of Law; Co-Director, High Tech Law Institute; Co-Supervisor, Privacy Law Certificate. Website: http://www.ericgoldman.org. Email: egoldman@gmail.com. This section is excerpted from ERIC GOLDMAN, INTERNET LAW CASES & MATERIALS (2018).

[1] CAL. CIVIL CODE §1798.140(c). All subsequent citations to 1798 are to the Cal. Civil Code as well.

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."[2]

The law does not restrict itself to online businesses. Indeed, the law expressly says it is "not limited to information collected electronically or over the Internet, but [the law applies] to the collection and sale of all personal information collected by a business from consumers."[3] Thus, the law equally applies to online and offline businesses in California that collect personal information—which, given the overly expansive definition of that term, is virtually all businesses (offline or on). The IAPP has (conservatively) estimated that over a half-million businesses are regulated by the law, "the vast majority of which are small- to medium-sized enterprises."[4]

Here's one reason why the law reaches so many small businesses despite its seeming attempt not to. The law applies to any business that "receives…the personal information of" 50k+ consumers. This would clearly cover the "receipt" of credit cards, and the 50k threshold is satisfied by any business that has an average of 137 unique credit card sales per day (or less than 14 sales per hour over a 10-hour business day)—a threshold many restaurants, coffee shops, and other small retailers are likely to clear.

Similarly, the law applies to any ad-supported website that "receives" 50k+ unique IP addresses a year, or an average of 137 unique IP addresses per day. This low threshold sweeps in all but the tiniest ad-supported websites.

The initiative was marketed as a way of curbing the excesses of the Internet giants like Google and Facebook. While the law certainly applies to them, the law treats the local pizza shop the same as Google and Facebook. It imposes costs on small businesses that will be much harder for them to bear than it will be for highly profitable companies like Google or Facebook. It seems puzzling that the California legislature actually intended to reach so many businesses that are not in a great position to afford the compliance costs.

What is "Personal Information"?

The law regulates the movement of consumers' "personal information." The law broadly defines "consumer" as any natural person,[5] which includes buyers and also employees/independent contractors of both the regulated business and its business customers and vendors.[6]

---

[2] 1798.145(a)(6).
[3] 1798.175.
[4] Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More Than Half A Million US Companies*, IAPP, July 2, 2018.
[5] 1798.140(g).
[6] *But see* Andrew Gray & Philip Gordon, *Unraveling The Latest in The Data Protection Juggernaut: What Does The California Consumer Privacy Act Mean For Employers?*, IAPP, July 3, 2018 (explaining how multiple provisions of the law don't make sense if it reaches employee data).

It's well-known in privacy circles that attempts to distinguish personal information from non-personal information are likely to be under- or over-inclusive.[7] The CCPA took the (massively) overinclusive route. The law defines "personal information" 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" (emphasis added),[8] with many specified examples, such as geolocation data and biometric information. The only exclusion is for "publicly available" data provided by the government; and even then, only if the data is used "for a purpose that is not compatible with the purpose for which the data is maintained and made available."

Other than government-provided information, what *isn't* personal information? Every piece of information about a person is *capable* of being associated with a particular person when combined with enough other data. For example, knowing someone is "male" doesn't uniquely identify them; but knowing a person's birthdate, zip code and gender allows the accurate unique identification of 87% of the population. So gender information should qualify as "personal information" because it is "capable of being associated with" a particular consumer. Indeed, all information about a consumer meets this "capable of being associated with" standard. Thus, any data related to individuals (consumers or employees) in a business' possession will qualify as "personal information."

The law excludes "consumer information that is deidentified or in the aggregate consumer information"[9] but does not attempt to harmonize the overly broad definition of "personal information" with deidentification or aggregation.

For example, the law defines "deidentified" information as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer" (with several additional obligations).[10] In theory, this means information is personal information if it's capable of being associated with an individual, but it's free to use so long as it's not "reasonably" capable of that association. If so, when is a person's gender "personal information," and when is it "deidentified" information, how will a business know, and what risks will the business be willing to take with this classification exercise?

The definition of "aggregate consumer information" has the same defect; it applies to "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."[11]

[7] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).
[8] 1798.140(o).
[9] 1798.145(a)(5).
[10] 1798.140(h).
[11] 1798.140(a).

Overview of the Law

A summary of the law's primary obligations (this leaves out and glosses over many details; there's no substitute for reading the statute!):

Disclosure of Generic Collection Practices Upon Request.[12] Upon a consumer's request, a business shall disclose "the categories and specific pieces of personal information the business has collected."

Disclosure of Generic Collection Practices Upon Collection.[13] At or before collection of a consumer's personal information, a business shall "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." The business shall not collect undisclosed categories, or make undisclosed uses, of personal information.

Erasure.[14] 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."

Disclosures About Collected Personal Information to the Consumer.[15] Upon a consumer's request, a business shall disclose to the consumer the (1) "categories of personal information it has collected about that consumer," (2) "categories of sources from which the personal information is collected," (3) "business or commercial purpose for collecting or selling personal information," (4) "categories of third parties with whom the business shares personal information," and (5) "specific pieces of personal information it has collected about that consumer." The last element should be provided in a format to facilitate data portability.

Disclosures About Sold/Disclosed Personal Information to the Consumer.[16] If a business sells consumer information (where "sell" includes disclosing or disseminating the information "for monetary or other valuable consideration"[17] or "discloses it for a business purpose" (a narrowly

[12] 1798.100(a).
[13] 1798.100(b).
[14] 1798.105.
[15] 1798.110.
[16] 1798.115.
[17] 1798.140(t).

defined term)[18] upon a consumer's request, a business shall disclose to the consumer the categories of personal information that the business (1) "collected about the consumer," (2) "sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold," and (3) "disclosed about the consumer for a business purpose."

Request Mechanisms. The law specifies many operational details about how consumers may make their requests and how businesses must and cannot treat those requests. Among other things, for the disclosures about collected and sold/disclosed personal information, the business must allow the consumer to make requests by at least two methods, including a toll-free number and a website (if the business has a website).

Opt-Out of Data Sales.[19] Consumers can opt-out of sales of their personal information, and the business can't ask them to change that for at least 12 months.[20]

Opt-In for Data Sales Related to Minors.[21] A business that knows (or "willfully disregards" the consumer's age) personal information relates to consumers under 16 may not sell the personal information unless the consumer (ages 13-16) or parent/guardian (under 13) opts-in.

Opt-Out of Third-Party Data Resales.[22] "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.[23] 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."

Specifications for Privacy Policies.[24] Among other requirements, a business' privacy policy must notify consumers about their erasure rights, collections and sales/disclosures of personal information, the opt-out/opt-in rights for data sales, and restrictions on privacy-based discrimination.

Anti-Discrimination.[25] "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" (an undefined term) to

[18] 1798.140(d).
[19] 1798.120(a).
[20] 1798.135(a)(5).
[21] 1798.120(d).
[22] 1798.115(d).
[23] 1798.135.
[24] 1798.130(a)(5) and others.
[25] 1798.125.

compensate for the collection, sale or deletion of data, but not if the financial incentives are "unjust, unreasonable, coercive, or usurious in nature."

Attorney General Regulations. The law authorizes the AG's office to "adopt regulations to further the purposes of this title," including the following specifically identified topics:[26]

- Designating additional categories of personal information "to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns."
- Updating "the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns."
- Designating additional communication methods that consumers can use to make requests to businesses.
- Establishing exceptions to comply with federal or state law.
- Governing "business compliance with a consumer's opt-out request."
- Developing a uniform opt-out logo or button.
- Biannually increasing the $25M threshold to reflect CPI increases.
- "Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings."
- "Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity."
- Defining what constitutes a "verifiable" consumer request.
- Explaining how a consumer can designate a representative to opt-out of data sales.

Who Can Enforce the CCPA?

In general, the law does not allow for private causes of action, either directly or through indirect means like California Business & Professions Code § 17200, which creates a civil claim for any legal violations. Thus, with one exception, the law can be enforced only by the California Attorney General's office,[27] and the law gives businesses a 30 day cure period following notice.

[26] All but the last two bullet points are specified in 1798.185.
[27] 1798.155.

Civil penalties can run up to $2,500 "per violation," though if violations are intentional, the cap increases to $7,500 per violation.

The only exception to the AG's enforcement: 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."[28] In those cases, consumers are allowed to 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. Furthermore, the consumer must notify the California Attorney General's office of the lawsuit, and the AG can do one of three things: (1) nothing, in which case the lawsuit can continue, (2) express an intent to prosecute the defendant, in which case the lawsuit apparently stops if the AG actually prosecutes within 6 months, or (3) unilaterally veto the lawsuit.

What Will Happen Next?

How will the California legislature amend the law post-passage? How the Attorney General regulations shape the law's scope?

In 2011, the Supreme Court struck down a Vermont anti-data brokerage law as unconstitutional in *Sorrell v. IMS Health Inc*.[29] Do any parts of the law violate the First Amendment?

Though the law attempts to limit its reach to activities with a California nexus, it likely will have ripple effects throughout the country and the world. Does the law violate the Dormant Commerce Clause?

Are other aspects of the law susceptible to other Constitutional or legal challenges, such as a Takings Clause challenge or the unusual provision allowing the California AG to veto private causes of action?

Will Congress step in to preempt the law? Congress is deeply dysfunctional, so the odds of it being able to tackle this issue in a productive way are low. Still, the law's implications are so vast that opponents might decide it's worth fighting the law there.

[28] 1798.150.
[29] 564 U.S. 552 (2011).