The California Consumer Privacy Act of 2018: GDPR Hits Close to Home

By Ronald Chichester

The California Consumer Privacy Act of 2018[1] ("CCPA") is a new form of privacy initiative that borrows from Europe's GDPR.[2] While the CCPA's penalties are not as severe as GDPR's,[3] the chances of encountering CCPA-entanglements are more likely for Texas companies. Moreover, CCPA is setting a trend that was started by GDPR, and more states may adopt CCPA-like statutes.

I. Some History About the Act

The CCPA had a very quick gestation. Indeed, the law was passed within a frantic seven-day legislative initiative that was clearly designed to thwart a possibly more draconian ballot initiative that was started by Alastair Mactaggart in 2017. That ballot initiative drew widespread industry condemnation and a $100M+ campaign to stop it. This short gestation period for CCPA is in stark contrast to the four-year gestation period for GDPR. Such haste led to the passage of the CCPA on June 28, 2018, and the passage of its first amendment (Senate Bill 1121[4]) on September 23, 2019. The CCPA does not take effect until January 1, 2020, so additional amendments are not out of the question, although *substantive* amendments are not deemed likely lest the ballot initiative be reinstated.

II. In General

The CCPA can be categorized as an opt-out (for adults, but opt-in for minors) privacy act that covers a broad range of information about California-located consumer transactions involving California residents. The CCPA has several GDPR-like provisions that are of interest to Texas businesses. In general, consumers have certain (limited) rights, and businesses have certain (limited) duties. While the CCPA has had its share of fear/hype, the provisions within CCPA have several major loopholes, so businesses may not have as much to fear as the media hype suggests.

The CCPA provides: a right to disclosure (for the consumer);[5] a right to delete (for the consumer);[6] delineates what businesses must disclosed;[7] duties imposed on

---

[1] TITLE 1.81.5. California Consumer Privacy Act of 2018 [§§1798.100 - 1798.199].

[2] General Data Privacy Regulation, (EU) 2016/679.

[3] See Eric Goldman, "A Privacy Bomb Is About to Be Dropped on the California Economy and the Global Internet", Technology and Marketing Law Blog, June 27, 2018, available at:

[4] See California Senate Bill 1121.

[5] CCPA §1798.100.

[6] CCPA §1798.105.

[7] CCPA §1798.110.

covered businesses;[8] opt-out provisions for a adult consumers and opt-in requirements for minors;[9] prohibition on discrimination of consumers (by a business) for exercising their rights under the CCPA;[10] the form of a request for disclosure;[11] additional duties on businesses related to opt-out;[12] a set of definitions;[13] some limitations on the duties of businesses;[14] violations/rights of action/remedies;[15] the right to seek the opinion of the Attorney General;[16] a consumer privacy fund (to compensate the state);[17] reference to other privacy laws;[18] preemption of other state and local rules and regulations;[19] requirements of the Attorney General;[20] an anti-circumvention provision;[21] no-waiver of CCPA provisions by contract;[22] a plea for liberal construction of the law;[23] a limitation on preemption;[24] the date of enforceability (January 1, 2020);[25] and early operability of the date of enforceability and limited preemption provisions (September 23, 2018).[26]

III. Covered Transactions

The CCPA only covers certain data-capturing transactions that occur in California that concern California residents. For companies that use mobile apps to collect data, an obvious way to avoid the CCPA would simply record the data from the California transaction and then upload the data *after* their customer has left the state. Not so fast. The CCPA anticipated such an attempt at circumvention, and prohibited it.[27]

---

[8] CCPA §1798.115.
[9] CCPA §1798.120.
[10] CCPA §1798.125.
[11] CCPA §1798.130.
[12] CCPA §1798.135.
[13] CCPA §1798.140.
[14] CCPA §1798.145.
[15] CCPA §1798.150.
[16] CCPA §1798.155.
[17] CCPA §1798.160.
[18] CCPA §1798.175.
[19] CCPA §1798.180.
[20] CCPA §1798.185.
[21] CCPA §1798.190.
[22] CCPA §1798.192.
[23] CCPA §1798.194.
[24] CCPA §1798.196.
[25] CCPA §1798.198.
[26] CCPA §1798.199.
[27] *See* CCPA §1798.190. ("If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the

IV. Businesses Covered

The CCPA defines a "business" broadly, but the law is directed to for-profit entities that do business in California.[28] However, a business that is covered by the CCPA must also satisfy one of the following "thresholds":

1. Has annual gross revenues in excess of twenty-five million dollars ($25,000,000)
2. 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; or
3. Derives 50 percent or more of its annual revenues from selling consumers' personal information.

These thresholds exclude many small businesses. The second threshold, however, begs a question: was that 50,000 *California* consumers, or just consumers in general? The CCPA defines "consumer" as "a natural person who is a *California* resident."[29] How businesses are supposed to track whether a consumer is a California resident (or not) can be difficult, but the effort may be worthwhile for businesses on the cusp of the threshold. Large corporations that focus on consumer surveillance (regardless of where they are located) are obviously affected - indeed they were the intended targets of the Act.

V. Disclosure Requirements

California residents have the right to request that a covered business disclose the categories and specific pieces of personal information collected.[30] The disclosure

---

intermediate steps or transactions for purposes of effectuating the purposes of this title.")

[28] *See* CCPA §1798.140(c)(1).

[29] *See* CCPA §1798.140(g).

[30] *See* CCPA §1798.100(a). CCPA §1798.140(o)(2) excludes publically available information. However, CCPA §1798.140(o)(1) defines personal information broadly to include "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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

A. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

must occur at the time of, or *before*, the transaction takes place. Interestingly, exactly *what* gets disclosed differs depending on whether the business has *sold* the personal information or merely *disclosed* the personal information to a third party. The covered business may disclose (as part of its privacy policy) or otherwise be required to disclose:

- If the business has ***sold*** personal information about consumers, then the business must provide a list of categories of personal information that it has sold about consumers in the preceding twelve months that most closely describe the information that was sold;
- If the business has **not** sold personal information, that fact must be disclosed;
- If the business has disclosed (but not sold) personal information about consumers, then the business must provide a list of the categories of personal information that it has disclosed for a business purpose in the preceding twelve months that most closely describe the personal information disclosed;
- If the business has ***not*** disclosed personal information about consumers, then that fact must be disclosed;
- The specific pieces of personal information that the business has already collected from the consumer;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting or selling or disclosing personal information; and

---

B. Any categories of personal information described in subdivision (e) of Section 1798.80.
D. Characteristics of protected classifications under California or federal law.
D. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
E. Biometric information.
F. 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.
G. Geolocation data.
H. Audio, electronic, visual, thermal, olfactory, or similar information.
I. Professional or employment-related information.
J. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
K. 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.

- The categories of third parties with whom the business shares personal information.[31]

By using "categories," covered businesses are relieved from telling consumers the actual identity of the third parties that receive their personal information. An obvious way to satisfy that requirement would be to post a notice at the retail establishment, or on a website. However, the California Attorney General will likely be asked to opine as to suitable disclosure mechanisms.

One of the key phrases in the CCPA is "a verifiable consumer request." This important definition is covered in §1798.140(y).[32] One of the loopholes in the Act is that businesses are not required to disclose data or delete data if they cannot verify the identity of the consumer making the request. Presumably the verification process should not be onerous, but it may require effort on the part of the consumer, and that might be enough to nullify the effect of the law for many consumers – particularly if they have to go through the process with many businesses. Moreover, consumers can only obtain such a disclosure at most twice in a 12-month period. Importantly, the information used to verify the request can be used only for the purpose of verification.[33]

Once the verified customer request has been received, the covered business must deliver the information promptly - and free of charge.[34] Delivery can be made electronically or by mail. If made electronically, the information must be in a form that can be copied or forwarded easily by the consumer (*i.e.*, no digital rights management or other mechanisms to prevent printing, copying or forwarding of the

---

[31] *See* CCPA §1798.100(b) and §1798.110 for a full list of the disclosure requirements.

[32] "'Verifiable consumer request' means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf."

[33] CCPA §1798.130(a)(7).

[34] CCPA §1798.100(d). However, if the requests are manifestly unfounded or excessive (by repetition), the business is allowed to charge a reasonable fee for those requests. *See* CCPA §1798.130(g)(3).

disclosed information).[35] Businesses have 45 days from the receipt of the verifiable consumer request to disclose the information.[36]

One foolproof mechanism for eliminating the disclosure requirement is simply not to collect personal information about the consumer. The CCPA does not require businesses to retain any personal information for a single, one-time transaction, if that information is not sold or retained by the business to re-identify or otherwise link information "that is not maintained in a manner that would be considered personal information." [37] Aggregated information (that does not identify a customer) is similarly excluded.[38]

Finally, the business must have disclosures on an online privacy policy (if it has one) or on a California-specific description of rights within the company's website.

VI. Right to Opt-Out

Consumers have a right to opt-out of selling their personal information.[39] Once the consumer has opted-out, the covered business is prohibited from selling that consumer's personal information from that point forward - unless the covered business obtains an express authorization from the consumer for the sale.[40] While businesses may *ask* the consumer for permission to sell their personal information, they may do so only after a 12-month period has expired.[41] Interestingly, consumers may use a *proxy* to exercise their opt-out rights.[42] Businesses may rightly fear the creation of for-purpose proxies to relieve consumers of the tedious chore of opting-out of sales of their personal information. In any event, businesses are encouraged to provide clear and conspicuous links on their websites entitled "Do Not Sell My Personal Information" that facilitates the exercise of the consumer's right to opt-out of the sale of their personal information.[43]

---

[35] *See* CCPA §1798.100(d).
[36] CCPA §1798.130(a)(2). Note, this deadline refers to the date when the verifiable consumer request was received, not when the request was actually verified. Verification is optional. The business may obtain a 45-day extension if it notifies the consumer of the extension. *Id.* Interestingly, CCPA §1798.145(g)(1) says that the second period is 90 days (not 45) if the business informs the customer within the first 45 days with an explanation for the delay. Presumably this discrepancy will be resolved before the law is enforced.
[37] CCPA §1798.100(e) and §1798.110(d).
[38] CCPA §1798.140(o)(2).
[39] *See, in general,* CCPA §1798.120 and §1798.135.
[40] CCPA §1798.120(c).
[41] CCPA §1798.135(a)(5).
[42] CCPA §1798.135(c).
[43] CCPA §1798.135(a)(1).

Finally, there is a general prohibition of selling personal information about children under the age of 16.[44] However, if the minor is between 13 and 16, they (themselves) may opt-in.[45] For children under 13, their parent or guardian must provide affirmative authorization.[46]

VII. Right to Delete

Upon receipt of a verifiable consumer request to delete the consumer's personal information, a covered business "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records."[47] Moreover, covered businesses must *inform* consumers of their right to have their personal information deleted.[48] This may prompt companies to sell the personal information as quickly as possible - before consumers have a chance to say, "delete."

There are several caveats to the deletion requirement. Businesses are not required to comply with a deletion request if:

1. The personal information is needed to complete a transaction that was requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise to perform a contract between the business and the consumer.[49]
2. The information is needed to detect fraud, malicious, or illegal activity (or prosecute those responsible for the bad acts).[50]
3. Detect and fix bugs in software and related-systems.[51]
4. Exercise free speech; ensure the right of another consumer to exercise his or her right to free speech; or exercise another right provided for by law.[52]
5. To comply with the California Electronic Communications Privacy Act.[53]

---

[44] CCPA §1798.120(d).
[45] CCPA §1798.120(c).
[46] *Id.*
[47] CCPA §1798.105(c).
[48] CCPA §1798.105(b).
[49] CCPA §1798.105(d)(1).
[50] CCPA §1798.105(d)(2).
[51] CCPA §1798.105(d)(3).
[52] CCPA §1798.105(d)(4). Sadly, I am at a loss to know what this means. How is the act of ***not*** deleting someone's personal information somehow free speech? If the data is somehow used as an affirmative defense to defamation/libel, perhaps?
[53] CCPA §1798.105(d)(5), specifically pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the California Penal Code.

6. Engage in public or peer-reviewed research *if* the consumer has provided informed consent.[54]
7. To enable *solely internal uses* that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.[55]
8. To comply with a legal obligation.[56]

VIII. Obligation Not to Discriminate

Businesses are prohibited from discriminating against consumers who have exercised their rights under the CCPA.[57] There are several specific types of discrimination that are delineated in the CCPA, including:

- The denial of goods and services to the consumer by the business;
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits (or even by imposing penalties); or
- Providing (or even *suggesting* that the business will provide) a different level of quality of the goods or services to the consumer when the consumer exercises his or her rights under the Act.

However, the provision about a price differential is not absolute. A business *may* charge a different price or rate *if* that difference is "reasonably related to the value provided to the consumer by the consumer's data."[58] Similarly, a "business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data."[59]

IX. Violations and Remedies

---

[54] CCPA §1798.105(d)(6).
[55] CCPA §1798.105(d)(7) and the closely aligned provision of §1798.105(d)(9). What is "reasonably aligned" and how do you discern "the consumer's relationship with the business"? Is it storing a credit card number (along with the consumer's name and address) so that the consumer can return to a website and purchase more product (assuming the consumer has checked some checkbox)? Hopefully the California Attorney General will shed some light on this within the first six months of enforcement of the Act.
[56] CCPA §1798.105(d)(8).
[57] *See*, *generally*, CCPA §1798.125.
[58] CCPA §1798.125(a)(2).
[59] CCPA §1798.125(b)(1).

Businesses are liable for unauthorized disclosure of unencrypted or non-redacted personal information.[60] Consumers have the right to civil actions, including class actions.[61] Consumer must, however, provide the business with a 30-day notice, and the business has those 30 days to cure the violation and inform the customer of the specifics of that cure.[62] The civil actions under the CCPA cannot be combined with actions under other laws.[63]

X. What to Do

The obvious work-around would be to collect only as much information, and for only as long as necessary, to satisfy critical business functions, such as facilitating the transaction itself.

Ensure that employees are trained about the CCPA. Specifically, businesses are responsible for ensuring that all individuals (regardless of whether they are employees or contractors) who are responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA understand all of the requirements and know how to inform consumers how to exercise their rights.[64]

XI. Conclusions

The CCPA was a rushed response to forestall a harsher sanction on businesses that routinely collect and sell consumer's personal information. Even though there are some internal inconsistencies in the Act, they will likely be ironed out before the law's enforcement. However, the sentiment and message is clear - California consumers will have some modicum of sovereignty over their personal information.[65] The penalties are individually modest, but collectively significant. The administrative overhead required by the Act, however, may make such data collection cost-prohibitive. Even though this law is limited to California, it may well be a template for other states and a harbinger of things to come. Clearly, there will be no more free lunches for the Marketing Department – ***IF*** consumers actually exercise their rights to opt out and delete, which is by no means certain.

---

[60] CCPA §1798.150(a)(1). Damages, under a civil action, include recovery of $100 to $750 per customer per incident or actual damages (whichever is greater); injunctive or declaratory relief; and any other relief the court deems proper. CCPA §§1798.150(a)(1)(A)-(C).

[61] CCPA §1798.150(b).

[62] *Id.*

[63] CCPA §1798.150(c).

[64] CCPA §1798.130(a)(6) and §1798.135(a)(3).

[65] This individual data sovereignty has been advocated by intellectuals such as Jaron Lanier in his book WHO OWNS THE FUTURE and other books. *See*, http://www.jaronlanier.com/futurewebresources.html