California Privacy Rights Ballot Initiative: Businesses, Watch This Space

CPRA would expand the California Consumer Privacy Act of 2018 (CCPA), a law that was also originally introduced as a ballot initiative but ultimately enacted by the California Legislature.

By **Lothar Determann** | May 22, 2020

Lothar Determann, with Baker McKenzie.

By May 4, 2020, more than 900,000 Californians gave their signatures to qualify a new privacy law for the November 2020 ballot. If it receives a majority at the general election, businesses around the world will have to comply with the California Privacy Rights Act of 2020 (CPRA) effective January 1, 2023 and disclose their information processing practices since January 1, 2022. CPRA would expand the California Consumer Privacy Act of 2018 (CCPA), a law that was also originally introduced as a ballot initiative but ultimately enacted by the California Legislature.

Consumer Privacy Rights Act: Key Provisions

Piece of the action: Businesses face significant penalties under CCPA that, once paid, are to be deposited in a Consumer Privacy Fund earmarked to offset government enforcement costs. CPRA contemplates that non-profit organizations would receive 3% of proceeds from such penalties to promote and protect consumer privacy (See active initiative 19-0021A1 at https://oag.ca.gov/initiatives/active-measures (https://oag.ca.gov/initiatives/active-measures) p. 39 proposing Cal. Civ. Code). The proponent of the ballot measure is the Board Chair and Founder of Californians for Consumer Privacy, a Section 501(c)(4) social welfare organization according to www.caprivacy.org (http://www.caprivacy.org).

Yet another agency: Voters rarely demand that states expand existing bureaucracies, leave alone create new authorities. But, CPRA would do just this and mandate the creation of a California Privacy Protection Agency (CPPA) to enforce CPRA against businesses with fines and cease-and-desist orders. The new agency would also assume from the California Attorney General the mandate to issue regulations on an expanded list of topics without further input from voters or the legislature. These topics include establishing restrictions on health-related research (CPRA, §1798.185(a)(19)(C)(ii); more generally see pp. 46-51, Cal. Civ. Code §1798.199.10-95), which could clash with present-time and future health and safety priorities.

CPRA contemplates a number of statutory safeguards to protect the prescribed mission of the new agency from influence by consumers, businesses or other government agencies, to drive independent and single-purpose-focused data processing regulation. The agency is incentivized to impose penalties on businesses to secure funding and growth for itself via the Consumer Privacy Fund.

Error corrections and new mistakes: CPRA corrects a number of remaining clerical errors in CCPA and recognizes trade secret rights of businesses as a limitation on data access rights of consumers. The proponents of CPRA framed the statute as an amendment and restatement of CCPA. This approach is preferable over a new stand-alone statute. With amendments, drafters tend to remain more mindful of existing law and avoid creating inconsistencies and duplications, as CCPA did with respect to other California and federal privacy laws. Unfortunately, CPRA also duplicates requirements and fails to repeal existing laws that would largely become obsolete if the broader CPRA takes effect. Whether or not CPRA passes, the California Legislature should urgently work on streamlining California privacy laws, which have become unbearably complex and convoluted (Regarding trade secrets, see Cal. Civ. Code §1798.100(h). For error corrections, see, e.g., Cal. Civ. Code §1798.110(c)(1) and (5). For duplication, see, e.g., the proposed new Cal. Civ. Code §1798.100(f) and the existing Cal. Civ. Code §1798.81.5(b) or the definitions of "contractor" and "service provider" in Cal. Civ. Code §1798.140, which are similar and unnecessarily complex. Regarding the need to repeal and streamline existing law, see https://iapp.org/news/a/an-open-letter-to-the-california-legislature-on-updating-the-ccpa/?mod=article_inline (https://iapp.org/news/a/an-open-letter-to-the-california-legislature-on-updating-the-ccpa/?mod=article_inline) and www.wsj.com/articles/privacy-experts-expect-amendments-to-clarify-restrict-california-law-11556535600 (http://www.wsj.com/articles/privacy-experts-expect-amendments-to-clarify-restrict-california-law-11556535600)).

Tighter restrictions on information sharing*:* Effective January 1, 2023, businesses would have to comply with various new or changed requirements regarding information collected after January 1, 2022. For example, a business that receives a deletion request would have to not only comply itself and instruct its service providers, but also notify other businesses to whom it sold or with whom it shared information to also delete the information (Cal. Civ. Code §1798.105(c)(1)). Unlike currently, the business would not be permitted to continue to use the information for internal purposes compatible with the context in which the consumer provided the information (Cal. Civ. Code §1798.105(d)(9)). Businesses would have to add prescribed clauses to contracts with service providers and contractors (Cal. Civ. Code §1798.100(d)), which many businesses will loathe having to re-open again after updating contracts for GDPR by May 2018 and for CCPA by January 2020. Service providers may also want to re-open existing agreements, as they would be required by statute to assist their customers (Cal. Civ. Code §1798.105(c)(3); §1798.130(a)(3)(A)), which would inevitably create additional compliance costs.

Many businesses would also have to revise the link required by CCPA for every web and mobile site to "Do Not Sell ***or Share*** My Personal Information" and add a link with the words "Limit the Use of My Sensitive Personal Information" or a combined link addressing both topics (Cal. Civ. Code §1798.135(a)(1)-(3)). If more states and countries follow this approach with their own prescriptive link and text requirements, consumers will have to search much harder for valuable information on the Internet between the many conspicuous links and warnings required by law. The CPRA's additional restrictions on information sharing would probably capture only a few more types of information exchanges given the counter-intuitively broad current definition of "selling" in CCPA (any disclosure for any valuable consideration), and the counter-intuitively narrow new definition of "sharing" in CPRA (any disclosure for cross-context behavioral advertising whether or not for consideration) (Cal. Civ. Code §1798.135(a)(1), §1798.140(ah)). Some businesses may become less concerned about the adverse brand impact of warnings that they are selling personal information with a "Do Not Sell My Personal Information" link if more businesses have to place more of these types of warnings on their online properties, which consumers can be expected to notice less and less.

Businesses would have to provide more details in "at collection notices" (Cal. Civ. Code §1798.100(a)) which would make such notices longer and more difficult to read and comprehend. The CPRA would define "advertising" to include inducing a consumer to obtain employment, and expand restrictions on information sharing for hiring purposes and job

advertisements (Cal. Civ. Code §1798.140(a)). These types of restrictions seem counter-productive in light of current unemployment statistics.

CPRA maintains and tweaks various complex and wordy exceptions, exemptions and delayed implementation dates, including for employee and business representative data that should never have been – and probably were not originally considered or intended to be – covered by a 'consumer' privacy law (Cal. Civ. Code §1798.145).

Data Minimization, Corrections, Sensitive Information Opt-in. CPRA adds data minimization requirements and data retention limits. These have been a fundamental principle of European Union and Canadian data protection laws but largely absent from U.S. laws due to greater regard for freedom of speech and information in the United States (Cal. Civ. Code §1798.100(c); Determann, Adequacy of data protection in the USA: myths and facts, International Data Privacy Law 2016; doi: 10.1093/idpl/ipw011). California residents would receive a right to demand that businesses correct inaccurate information concerning them (Cal. Civ. Code §1798.106).

Businesses would have to comply with directions and objections from California residents regarding the use and disclosure of sensitive personal information, defined by CPRA to include credit card numbers, religion and various other categories from existing California security breach notification laws and Art. 9(1) of the EU General Data Protection Regulation (Cal. Civ. Code §1798.121, §1798.140(ae)).

Deja Vu All Over Again?

CCPA, the law that the CPRA ballot initiative seeks to amend, emanated itself from a ballot initiative promoted by the same group.

On May 3, 2018, Californians for Consumer Privacy announced that they had gathered enough signatures for their CCPA initiative. Less than two months later, after an unusually rushed legislative process, the California Legislature passed a compromise version of the CCPA that could be amended by simple majority going forward (whereas the CCPA version proposed by the ballot initiative would have required a 70 percent majority vote for any amendments). June 28, 2018 was the last day on which the CCPA ballot initiative could be withdrawn and the day on which Governor Jerry Brown signed the CCPA into law.

On May 4, 2020, Californians for Consumer Privacy announced that they gathered enough signatures for their CPRA initiative. This time around, the Legislature may feel less pressure to rush through compromise legislation, because CPRA would expressly permit the California Legislature to amend CPRA by simple majority. Also, CPRA would prevail over any conflicting legislation that the California Legislation enacts after January 2020.

Moving Target

Businesses face a rapidly moving target: The California Legislature enacted CCPA after an unusually short legislative process on June 28, 2018 to take effect on January 1, 2020 with requirements to disclose data processing practices after January 1, 2019. CCPA was already amended twice, in September 2018 and October 2019. Dozens of bills to further amend CCPA have been floating in Sacramento. Meanwhile, the California Attorney General published draft regulations on October 10, 2019 (based on the then-current, but since-amended version of CCPA) and significantly revised drafts on February 10 and March 11, 2020. Even though the regulations are still not final by May 18, 2020, the California Attorney General has confirmed that enforcement will on start July 1, 2020.

The text of the CCPA is long and complex, with more than 10,000 words and many counter-intuitive definitions, including "consumer" defined to mean any resident, "selling" defined to mean any sharing for any valuable consideration, and "homepage" to mean any web page. The draft regulations of the Attorney General are even more wordy and complex. When businesses read the requirement in the draft CCPA regulations, multiple times repeated verbatim (See, e.g., § 999.306(a)(2)(a)), that they shall "[u]se plain, straightforward language and avoid technical or legal jargon" in their privacy notices, they might perceive this a cynical rendition of "do as we say, not as we do."

The CPRA is even longer and more complex than the CCPA, and the list of topics its regulations are supposed to address is more than twice as long as that in the CCPA. If the CPRA is passed in its current form this November, one can expect businesses to continue to have to deal with shifting compliance targets for the foreseeable future.

Impact on Businesses

The California Department of Justice commissioned and published an impact assessment that estimated the total cost of initial compliance with the CCPA at approximately $55 billion, equivalent to approximately 1.8% of California Gross State Product in 2018 (Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations at 19 (Aug. 2019), www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf). This estimate does not take into account the many legislative changes and drawn-out rulemaking process, which companies have to monitor, nor does it factor in the potential additional burdens that CPRA would add.

In 2019, businesses were already subjected to dozens of class action lawsuits that referred to CCPA despite the fact that CCPA expressly disclaims rights of private action and did not even take effect until January 1, 2020. Since then, even more suits have been filed, some based on incidents alleged by plaintiffs to have occurred before the CCPA's effective date. CPRA does not try to remedy or worsen this situation; it does not repeal or add rights of private action.

In March 2020, when California started shutting down in response to the coronavirus pandemic and many businesses started fighting for survival, a few associations asked for an extension regarding CCPA enforcement; the California Attorney General rejected the requests and privacy advocates expressed disappointment that businesses even asked for an extension (Joe Duball, *California Attorney General's Office: No Delay on CCPA Enforcement Amid COVID-19*, IAPP (Mar. 24, 2020)).

Larger technology companies will likely find it easier to comply with CCPA and CPRA than most other businesses. Some of the largest tech companies can handle the coronavirus crisis quite well. Some see more opportunities than challenges. Also, larger, well-established businesses have relatively mature privacy compliance programs and depend less on data sharing and advertising than smaller and newer companies. Restrictions on advertising and information sharing generally favor established companies and cement their market powers.

What To Do Now?

First of all, businesses need to do their best to comply with CCPA as the July 1, 2020 enforcement start-date approaches. Companies that have been taking a "wait and see" approach and hoping for Federal legislation, an extension from the California Attorney General, or other miracles have been falling further behind and have become exposed to risks of compliance challenges and lawsuits. Businesses that comply with CCPA will be better prepared for CPRA, GDPR and new laws in Brazil, India and possibly other states and countries (See Lothar Determann and Chetan Gupta, India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act, 37 Berkeley Journal of International Law 481, https://ssrn.com/abstract=3244203 (https://ssrn.com/abstract=3244203)).

Second, companies that expect the CPRA to pass in one form or another should consider upgrading their CCPA compliance measures to address CPRA requirements where this does not require major economic sacrifices, for example, with respect to vendor contract renewals and upgrades.

Third, in their spare time, businesses should carefully assess the potential impact of CPRA on their operations and business models. If they determine a significant impact, they should consider changing plans, relocating and speaking up to help inform voters.

CCPA and CPRA are following a European approach of rigid data processing regulation that may have limited business successes in the old country: After 50 years of restrictive data protection laws, European citizens are mostly using information technologies made in the United States and increasingly in China. Consumers in Europe make the same trade-offs concerning privacy as Internet users in the United States and elsewhere do. Few European businesses are leading in the IT sector. Data-driven innovation is unable to thrive where businesses are by default prohibited from processing personal information and required to minimize data collection, restrict data use, limit data retention periods and respond to data subject requests for deletion, portability and copies free of charge.

Soon it may be up to California voters to follow or reverse course. Since the coronavirus pandemic broke out, many voters have reset priorities and may opt for more information and **healthy data protection (https://ssrn.com/abstract=3357990)** just as European governments are considering exceptions for contact-tracing apps.

Lothar Determann, *partner at Baker McKenzie, Palo Alto, and author of California Privacy Law – Practical Guide and Commentary (3d Ed. 2018) thanks Jonathan Tam for valuable input and edits, but takes sole responsibility for personal opinions expressed in this article.*
