How Calif. Privacy Rights Act Could Shape Privacy Landscape

By **Lauren Kitces and Lydia de la Torre** (June 30, 2020)

Lauren Kitces

Lydia de la Torre

The California Privacy Rights Act, or CPRA, entered the privacy arena as an unexpected surprise in September of 2019. At that time organizations and legal professionals were already busy interpreting and implementing the California Consumer Privacy Act, or CCPA, which had not yet gone into effect.

The CPRA was proposed by the same group behind the enactment of the CCPA, Californians for Consumer Privacy, and presented as a ballot measure that would introduce significant amendments to the CCPA. These amendments would rework the current CCPA language, and add in a plethora of new requirements and concepts.

On June 24, the CPRA was certified as having collected the required number of valid signatures for ballot initiative in California, which guarantees that it will appear on the Nov. 3 ballot. It is now up to the California voters decide whether the measure will be enacted. If it is passed, it will become a permanent baseline for California privacy law, increase the already demanding requirements of the CCPA, and potentially redefine informational privacy for the entire U.S.

The CPRA as a Permanent Baseline for California Privacy Law

As permitted by the California Constitution, Section 25 of the CPRA allows for amendments to the CPRA by the Legislature, but only "provided that such amendments are consistent with and further the purpose and intent of this Act." In practice, this means that any amendment to the CPRA by the California Legislature will be subject to scrutiny by the proponents and other activist, who can challenge it in court if they believe that it leads to an erosion of the rights of California residents or otherwise limits the obligations imposed by the CPRA on businesses.

Due to these restriction, should the CPRA be passed it will de facto become a permanent baseline for California privacy law. Thereafter, the only effective paths to lessen its requirements will be a new California ballot initiative, a federal law preempting the CPRA, or a constitutional challenge (most likely on the bases of a violation of freedom of speech or the dormant commerce clause).

The CPRA's Demanding Requirements

The CPRA redefines the privacy landscape, and goes well beyond the requirements imposed by the CCPA. The changes in the CPRA will push entities to take such actions as being even stricter with their uses of personal information, offering additional rights to consumers, and treating sensitive personal information (as defined in the CPRA) differently than the remainder of personal information.

The following are some of the changes that are new to the area of U.S. privacy, or that will otherwise likely have an enduring impact.

New Rights

The CCPA created four main consumer rights: (1) the right to know, (2) the right to delete, (3) the right to opt out of sale and (4) the right to not be discriminated against for exercising the first three of these rights.

The CPRA adds several important new rights to the lineup. These include allowing consumers to direct businesses to limit the use of sensitive personal information (as defined in the CPRA) and to request updates to inaccurate personal information. As with the CCPA, new rights will be expanded by necessary regulations, which will likely mean even more details and requirements than those enumerated in the CPRA.

Purpose and Storage Limitations

The CCPA does not include strict use and retention restrictions for personal information. The CPRA will change this by imposing limitations on the ability to collect, use, retain and share personal information of California consumers. Such activities "shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

This change moves California in the direction of the EU's General Data Protection Regulation and its predecessor (the Data Protection Directive), which includes purpose limitation as a core principle of lawful data processing.

The CPRA also requires businesses to more clearly disclose their use and retention practices, not retain personal information for compliance with the CPRA that they otherwise would not have retained in the ordinary course of business, and imposes additional restrictions on service providers and contractors.

Businesses will be required to include their retention time frames per category of personal information that they process in their privacy notices or, in the alternative, explain the criteria they use to determine the retention time frames. Personal information will only be permitted to be retained for as long as is reasonably necessary for the disclosed purposes.

Applicability Beyond Consumers: Privacy Rights for All California Residents

Both the CCPA and the CPRA apply not only to traditional consumers who receive goods and services from an entity, but also to all residents of California (e.g., employees, contractors, individuals that act in their capacity as business representatives, etc.) However, the applicability of the CCPA beyond traditional consumers is limited by two temporary carveouts: one for personnel and applicant personal information, and a second one for business-to-business communications. These exemptions are designed to sunset Jan. 1, 2021, but could be extended temporally or permanently by the California Legislature. (In fact, a bill currently under consideration in the California Legislature would extend the carveouts for one more year.)

The CPRA also includes both personnel/applicant and business-to-business communication exemptions, but these would both expire on Jan. 1, 2023. As discussed above, the CPRA can only be amended to further the purposes of the law, namely to protect the privacy rights of Californians. Therefore, the California Legislature will not be able to extend the exemptions beyond Jan. 1, 2023, as that would prevent those individuals from having a full

realization of their privacy rights.

Once the carveouts expire, this will open the door to employees exercising CPRA rights (including a full right of access) and significantly increase compliance obligations for organizations that operate mainly in the business-to-business space.

New Enforcement Agency

The CPRA creates a new state agency, the California Privacy Protection Agency, or CalPPA, that will be vested with full administrative power, authority, and jurisdiction to implement and enforce the CPRA. The initial task for CPRA regulations will rest with the California attorney general (who currently handles the CCPA and its regulations), but will then transition to CalPPA on the later of June 1, 2021, or six months after CalPPA tells the California AG that it's ready to take over.

CalPPA will initially be funded by $5 million for 2020-2021, and then $10 million each subsequent year. There is an ability for additional funds to be allocated, and they will also be able to use funds from the Consumer Privacy Fund (which is currently in existence and will be replenished through penalties deposited that arise from violations of the CCPA — and if passed, the CPRA).

CalPPA will be administered by a five-member board. There will be a chair and one other member appointed by the governor, and three additional members respectively appointed by the attorney general, Senate rules committee, and speaker of the Assembly. No member may serve more than eight consecutive years.

The stated goal of CalPPA is not only to enforce the CPRA and its regulations, but also to educate Californians on privacy rights and provide insight on complying with the CPRA to in-scope entities.

The presence of a dedicated privacy agency will potentially allow for much greater attention to be paid to the rights of consumers and compliance efforts of in-scope entities.

Heightened Oversight

Entities whose processing of personal information presents a "significant risk" to a consumer's privacy or security will be required to submit regular risk assessments to CalPPA. They also will be subject to auditing activities by CalPPA. These requirements are to be primarily shaped by the yet to be drafted CPRA regulations.

Along the same lines, businesses will have the legal right to monitor service providers and the newly created category of contractors. This monitoring includes, but is not limited to, manual and automated review processes, assessments, audits, and annual technical and operational testing.

In another requirement that heralds back to the GDPR, service providers and contractors will have to notify businesses of additional entities they engage to help them provide services to the business. These entities will also require contracts.

This will require a detailed understanding of vendor relationships. Many entities struggled to cleanly capture this information when preparing to comply with the GDPR. If that process wasn't performed for U.S. processing of personal information, it likely will be a significant undertaking for many entities should the CPRA pass.

Redefining Informational Privacy in the U.S.

The heightened requirements of the CPRA will undoubtedly fuel increased interest in the passage of a federal privacy law and, potentially, privacy laws in states other than California.

Historically, federal and state privacy laws have been sectoral in nature, with the CCPA introducing the first broad privacy law into effect. The CPRA follows the trend started by CCPA, and it is likely that future state and federal privacy efforts will follow the more comprehensive CPRA approach.

At the state level, jurisdictions beyond California may introduce laws that mirror the CPRA. This would allow entities that have already invested in CPRA compliance to leverage those efforts across multiple jurisdictions. In fact, many medium and large entities have chosen to apply the individual rights afforded to California consumers to all those in the U.S. due to the complexities of proving residency and untangling Californian personal information from the remainder.

Any such state laws will undoubtedly impact new entities, and increase the number of regulators that can enforce the laws, as well as the potential fines.

If states move toward varied requirements that do not align with each other, Congress may be pressured to create a single U.S. standard. However, that pressure may or may not result in actual legislation because similar subjects (such as data breach laws) have remained inconsistently regulated at the state level for years despite industry requests for a single federal standard.

In any event, the key points of discussion for federal privacy laws will be to what extent federal law should preempt state laws and what should be the enforcement mechanisms. The vast majority of recent federal proposals would preempt state laws, which has resulted in stern opposition from the California delegation that sees federal privacy law as potentially subverting the rights and requirements currently in its state laws.

Considering that many entities are spending at least six-figure sums to come into compliance with the CCPA, and even more will be required by the CPRA should it pass, any federal privacy law will likely face strong arguments to align with preexisting compliance standards. Additionally, California will then be working on another new set of regulations and the assembly of CalPPA, neither of which will be small undertakings. To overturn all of this effort from the state of California and entities alike will potentially be harshly received.

And Now, We Wait

All polling assessing support for the CPRA predates COVID-19, and therefore isn't very reliable. That said, the support it received early in the year was significant.

The uses of personal information during the pandemic may increase consumer awareness and care for the privacy of their personal information. Conversely, the cost of CalPPA and the compliance costs that will impact sized entities in California may act as deterrents.

No matter what happens on Election Day, the time leading up to that will be uncertain as entities in-scope of the CCPA try to determine how to best proceed in their privacy compliance efforts as they wait to learn the fate of the CPRA.

We won't know until Nov. 3, but if it passes, CPRA will leave an impression on privacy law that will likely always remain.

Lauren Kitces is an associate and Lydia de la Torre is of counsel at Squire Patton Boggs LLP.