LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

THURSDAY, MAY 26, 2022

PERSPECTIVE

CPRA Series: Part V - Litigation and Enforcement

Introduction

As discussed in the previous installments of our series on the California Privacy Rights Act of 2020 (CPRA or the Act), the CPRA is leading the charge in how many regulators and companies address privacy, creating new consumer rights and imposing new obligations on businesses covered by the Act. Along with these new rights and obligations come new enforcement mechanisms – including the creation of the California Privacy Protection Agency (the Agency) – the first regulatory agency in the United States dedicated to consumer privacy issues – and the expansion of private enforcement through litigation. Although the CPRA's substantive provisions go into effect on Jan. 1, 2023, the Act contains a "lookback" provision to Jan. 1, 2022, which means that companies must be prepared for potential enforcement activity for the decisions they are making today.

In this fifth and final installment of our series on the CPRA, we provide an overview of expected enforcement activity, both by the Agency as well as through private enforcement. We also provide compliance guidance to businesses that will be governed by the CPRA.

CPRA Enforcement by the Agency

Shared Enforcement Authority with California Attorney General

Created to regulate consumer data privacy and enforce state privacy laws, the Agency's five-member board was appointed on March 17, 2021, and Ashkan Soltani was selected as the Agency's first Executive Director on October 4, 2021.

The Agency has the authority to investigate possible violations of the CPRA upon the sworn complaint of any person or on its own initiative, and to bring an administrative action to enforce violations. However, this authority is discretionary, and the Agency may choose not to investigate a complaint. In addition, the Agency is charged with cooperating with other privacy enforcement agencies, including those in other states, territories and countries.

Although the Agency has the power to "[a]dminister, implement, and enforce" the Act "through administrative actions," the California Attorney General retains civil enforcement powers, and can seek an injunction and/or penalties in a civil action. While enforcement authority is shared, the Agency is expected to take the lead on administrative enforcement once the agency has achieved enforcement readiness and final regulations are adopted. Under the Act, enforcement is set to begin July 1, 2023, and will apply to violations occurring on or after that date. Until that time, the Attorney General is expected to continue enforcement under the existing CCPA regulations. With the resources of both agencies in action, we anticipate robust enforcement of the CPRA and a potential increase in regulatory enforcement actions and more intense scrutiny of business practices.

Elimination of Cure Period

The CPRA eliminates the 30-day cure period that currently applies to CCPA enforcement by the Attorney General, and instead grants both the Attorney General and the Agency discretion whether to offer a cure period. The Act identifies several factors that the Agency "may" consider in deciding whether to permit a cure period, including the business's lack of intent to violate the Act as well as voluntary efforts undertaken by the business to cure the violation. The CPRA authorizes the Agency to impose fines ranging from $2,500 to $7,500 per violation (the same as the CCPA) regardless of any opportunity for cure, subject to the enforcement process set out in the Act.

Litigation and Enforcement	CCPA (2020)	CPRA (2023)
Private Right of Action for Violations of the Act	No	No
Private Right of Action for Data Breaches	Yes	Yes
Data Breach Cure Period	Yes	Yes
AG Enforcement Action	Yes	Yes
Enforcement Cure Period	Yes	Discretionary
Agency Enforcement Action	No	Yes
Agency Cure Period	N/A	Discretionary, notice of probable cause hearing required
Effective Date	January 1, 2020	January 1, 2023
Enforcement Date	July 1, 2020	July 1, 2023
Look-back Date	Jan. 1, 2019	Jan. 1, 2022
Retroactive	No	No
Requirement to Adopt Implementing Regulations	Yes	Yes
Rulemaking Subject to Open Meetings Act	No	Yes
Number of Mandates for Creation of Regulations	7	22
Number of Pages of Final Regulations	23	TBD

Procedure for Administrative Enforcement

The CPRA provides that administrative enforcement by the Agency will use a "probable cause" standard, and that the service of the probable cause notice constitutes the commencement of the administrative action. Entities alleged to have violated the Act must be given at least 30 days' notice, be provided with a summary of the evidence, and be informed of their right to be present and have counsel at any proceeding held by the Agency. The Agency has the power to obtain subpoenas in aid of any enforcement proceeding. Administrative actions under

the CPRA generally must be commenced within five years of the violation, although the Act provides exceptions to this limitation in the event of fraudulent concealment of information or in the case of delay in responding to a subpoena issued in the course of such proceeding. The Act further provides for judicial review of Agency enforcement decisions "in an action brought by an interested party to the complaint or administrative fine" under an abuse of discretion standard.

Penalties

If, after a hearing, the Agency determines that a violation has occurred, the Agency can issue a cease and desist order as well as impose a fine of up to $2,500 for each violation or up to $7,500 for each intentional violation or for violations involving the personal information of a minor consumer.

In a civil action by the Attorney General, the available penalties are the same. In a civil action, the Act provides that the "court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty."

The Act also makes provision for the dual enforcement authority of the Agency and the Attorney General. For example, the Attorney General can ask the Agency to stay administrative actions or investigations to permit the Attorney General to proceed with its own investigations and/or civil actions. Under the CPRA, the Agency must defer to such requests and "may not limit the authority of the Attorney General" to enforce the Act. Additionally, the Attorney General cannot file a civil action against a person for the same violation that has been the subject of an administrative penalty, and the Act also provides that "[a] business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation."

Retroactivity

As discussed in our previous installments, the CPRA's substantive requirements are effective Jan. 1, 2023, and enforcement of its provisions may begin at that time. However, CPRA includes a "lookback" provision which makes its provisions applicable to information collected on or after Jan. 1, 2022. There is good news for businesses that are already compliant with the CCPA and a warning for those still waiting to get into compliance.

Agency Funding and Enforcement Impact

The Agency will begin work with an annual budget of $10 million, which is nearly twice what the AG's office budgeted for enforcement of the CCPA. As a result, the Agency will have more dedicated employees to pursue more businesses for alleged violations and is expected to employ 34 staff members and attorneys to carry out its mission. These resources are in addition to those already deployed by the Attorney General's office.

Additionally, the Act provides for the creation of a Consumer Privacy Fund that will provide most funding for the Agency moving forward. The Consumer Privacy Fund will be funded by recoveries under the CPRA in enforcement actions. The majority of fines deposited into the Consumer Privacy Fund will be used to offset costs incurred by the Attorney General and the courts for enforcement actions, invested for the benefit of California taxpayers, to support the Agency, and the remainder will be used for grants to promote education and non-profit initiatives to increase visibility and awareness about privacy related issues. Therefore, the Agency is incentivized to vigorously enforce provisions of the CPRA. It is unclear whether the Agency or Attorney General expect recoveries to exceed the annual budget. Regardless, businesses should assume that regulators will be looking to offset the expense to California taxpayers with recoveries under the Act and be prepared for enforcement to begin after July 2023.

Private right of action

Like the CCPA, no private right of action exists under the CPRA for alleged violations of the Act. However, the CPRA expands upon the private claim that already existed under the CCPA for data breaches – i.e., where a consumer's "nonencrypted and nonredacted personal information… is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's 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."

The CPRA's private right of action provision incorporates the definition of "personal information" used by the CCPA, which means "[a]n individual's first name or first initial and the individual's last name in combination with" a number of data elements identified in the Act, "when either the name or the data elements are not encrypted or redacted." These data elements include Social Security number, driver's license, passport, or other unique government identification number, account number or credit or debit card number in combination with any required password or code to access the account, medical, health or genetic data, or unique biometric data. However, the CPRA also expands on the CCPA's definition of personal information by including an "email address in combination with a password or security question and answer that would permit access to the account" in the list of personal information whose breach gives rise to a cause of action. We expect that this expansion of the definition of personal information will result in increased consumer litigation following data breaches.

Consumers who prove entitlement to recovery may recover damages between $100 and $750 per consumer per incident, or actual damages, whichever is greater, and may obtain injunctive or declaratory relief. The Act provides that in assessing the amount of statutory damages, the court shall consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Before instituting a private action, CPRA requires consumers to provide a business with a 30-day written notice of the alleged violation. If the business cures the violation and provides the consumer with an "express written statement" to that effect, the consumer cannot sue. However, this notice requirement and cure period is only applicable if the consumer is seeking statutory damages, not if the consumer is only seeking actual pecuniary damages. Additionally, the Act makes clear that "[t]he implementation and maintenance of reasonable security procedures and practices… following a breach does not constitute a cure with respect to that breach." And, businesses may also be subject to litigation if they fail to abide by any "express written statement" provided to a consumer.

The civil action provision of CPRA is effective Jan. 1, 2023.

Impact of pending rulemaking

Under the CPRA, the Agency assumes responsibility for rulemaking activity from the Attorney General. Moving forward, the Agency will then have sole responsibility for promulgating, revising, and implementing regulations interpreting both the CCPA and CPRA.

Much like the rulemaking process under the CCPA, the CPRA requires that the Board:

- Begin the informal rulemaking process;
- Receive public comments on proposed rules/regulations;
- Modify the regulations and rulemaking package to account for public comment;
- Prepare the final rulemaking package;
- Send the rulemaking package to the Office of Administrative Law for review and approval;
- The Secretary of State must adopt the regulations.

Unlike the rulemaking process under the CCPA, however, the Agency must comply with California's Bagley-Keene Open Meeting Act, which requires the board to conduct its meetings and make all decisions in public. Transparency comes at the expense of efficiency. As a result, and as the Agency has already suggested, it is unlikely that the Agency will have final regulations approved by the July 1, 2022 deadline.

Subcommittees are permitted to meet in private so long as only two board members are present and they only work to advise the Board. The Agency consists of three subcommittees that will advise the Board in the following areas:

- Regulations: Provide guidance on planning and priorities for the rulemaking process.
- Public Awareness and Guidance: Ensure consumer visibility and guidance for consumers and business with respect to CPRA requirements.
- Administration: Manage administrative issues involved in the creation of the Agency (e.g. staffing and internal policy).

The CPRA includes a mandate for the development of new or additional regulations in 22 specifically enumerated areas. In contrast, the CCPA only included seven mandates which resulted in 23 pages of CCPA regulations. Under the CPRA, the Agency is directed to develop new rulemaking regarding issues such as establishing definitions under the CPRA, ensuring consistency with federal and state privacy laws, developing rules related to consumer exercise of privacy rights, setting civil penalties, harmonizing the CPRA with other laws and regulations, and clarifying the scope of Agency's authority. We anticipate that regulations promulgated by the Agency will be significantly more voluminous than those promulgated by the Attorney General under the CCPA.

The Agency has already begun initial informal rulemaking, with the public comment period held from Sept. 21, 2021 through Nov. 8, 2021. Preliminary public comments are available on the Agency's website, here. The initial rulemaking process sheds some light on the regulatory priorities with respect to the following topics:

- Definitions: how terms and concepts should be defined, including

but not limited to the definitions of personal information, sensitive personal information, de-identified information, geolocation, and dark patterns.

• Identification of significant privacy and security risk: identifying processes and practices that pose significant privacy and security risks (and which processes and practices will require annual security auditing and risk assessment reporting under the CPRA).

• Automated Decision-making: what information is necessary for businesses to share about automated decision-making processes employed by the business.

• Agency Audits: the scope of Agency's authority to audit a businesses' compliance with CPRA and applicable privacy laws and regulations.

• Consumer Rights: defining the rights added under the CPRA, such as the right to correct, right to opt out of sharing, and the right to limit the use of sensitive personal information.

• Consumer Requests: understanding the challenges businesses may encounter when responding to consumer requests for data collected by the business for time periods longer than the CCPA's requirement for access to data for the preceding 12-months.

As of the writing of this series, the Agency has not commenced formal rulemaking. The Agency's final deadline to promulgate regulations is currently July 1, 2022, which will allow companies time to comply before the CPRA goes into effect on Jan. 1, 2023. However, the Agency has already indicated that final regulations likely will not be ready until the fourth quarter of 2022. Enforcement of the CPRA will begin July 1, 2023, but the Agency may need to exercise discretion to allow sufficient time for businesses to interpret and respond to the final regulations.

Litigation and Enforcement: Comparison of Key Provisions

While the CCPA forms the foundation of California's privacy protection framework, the CPRA continues to evolve that framework and significantly amends the CCPA to strengthen consumer privacy protections and regulate the technology industry. Some of the notable similarities and differences between the CCPA and CPRA are highlighted in the table, below, to illustrate the evolution of California's privacy law enforcement efforts.

Conclusion

Throughout this Series we have discussed the many changes between the CCPA and CPRA to provide covered businesses with tools to evaluate compliance and plan for a different privacy landscape beginning January 2023. It is important for businesses to take note of these changes and plan accordingly because compliance with the CPRA currently required by the look-back period.

On July 1, 2023, the Agency will begin enforcement activities and we anticipate an immediate increase in regulatory oversight. Plaintiffs' attorneys are equally eager to bring litigation under the expanded private right of action. Companies should consider the following actions to mitigate regulatory and litigation risk:

• Conduct a CPRA compliance gap analysis to understand what efforts are still required to bring the company in line with the CPRA.

• Ensure that company management and the board are aligned to support CPRA compliance objectives and that key stakeholders are accountable for meeting compliance deadlines.

• Create a "crown jewels" inventory of data collected from consumers. Ensure that the "crown jewels" (e.g., financial information, personally identifiable information and all categories of "sensitive personal information") are carefully mapped and the company understands data flows of consumer information.

• Prepare for annual risk assessments by ensuring that cyber security measures are effective, and that data is adequately protected.

• Make sure that the company is engaging in data minimization practices and that data retention requirements are closely followed and documented.

• Audit and revise internal policies, procedures and practices to align with CPRA requirements.

• Conduct an audit of third-party agreements to ensure compliance and alignment with the CPRA. Make sure that any agreements with data processors are in writing, set forth the instructions for processing data, and describe the types of data shared. Also ensure that contracts prohibit vendors from sharing, using, or aggregating personal information outside the business purpose for the relationship.

• Maintain a list of third-party vendors and partners with whom consumer information is shared, including what information is shared and for what purpose. Also ensure that third-parties are aware of the company's data retention policy and agree to a cadence for data destruction that aligns with the CPRA's data minimization and retention requirements.

• Update publicly facing privacy policies on the company website.

• Ensure the company website contains information about how a consumer can exercise his/her privacy rights and confirm that the business has a documented and effective pro

Ron Raether, James Koenig *and* **Kamran Salour** *are partners;* **Sadia Mirza,** *and* **Graham Dean** *are associates and* **Edgar Vargas** *is an attorney at Troutman Pepper Hamilton Sanders LLP.*