SQUIRE
PATTON BOGGS

Local Connections. Global Influence.

CPRA/CDPA/CPA Unpacked

Develop a Preparedness Plan Now

September 2021

Understanding and Preparing For New State Privacy Laws

The California Privacy Rights Act (CPRA) is a comprehensive rework of California's paradigm-shifting 2018 consumer protection law (the California Consumer Privacy Act or CCPA) that was enacted through a ballot initiative on November 3, 2020, and will go into full effect on January 1, 2023. It amends the CCPA in several material ways to, among other things, eliminate the existing carve-outs for data collected from job applicants, employees and contractors, and for data of persons representing another business in connection with a business-to-business (B-to-B) transaction or communication. Those carve-outs expire on January 1, 2023. Further legislative extensions are unlikely, as the CPRA prohibits legislative amendments that do not "enhance" privacy, though there could ultimately be somewhat different rules for these non-consumer data subjects. The CPRA retains a number of existing carve-outs for data covered by other state and federal privacy laws, such as protected healthcare information.

As a reminder, on July 1, 2020, the AG began enforcement of the CCPA and has reportedly launched more than 200 investigations. On July 19, 2021, the AG published 27 summaries of concluded enforcement actions, providing important guidance on third-party cookies, digital advertising, global privacy controls and financial incentive rules as applied to loyalty programs and sufficiency of notices and consumer rights responses.

On March 2, 2021, the Virginia governor signed into law a new consumer protection law becoming the second state in the US to enact a holistic data privacy law that regulates the collection, use and disclosure of "personal data" (broadly defined to include most information that would be personal information under the CCPA/CPRA) of its residents generally, but excluding data subjects outside of an individual or household context (i.e., does not include persons acting in an employment or B-to-B context). Like the CCPA/CPRA, certain already regulated data, such as protected healthcare information, is carved out of the new Virginia law.

Set to go into effect on January 1, 2023, the Virginia Consumer Data Protection Act (CDPA) is, in many ways, similar to the CPRA, but it also shares some additional concepts inspired by the EU's General Data Privacy Regulation (GDPR). However, it is sufficiently dissimilar to each of those laws that a business developing a compliance strategy for compliance with the CDPA will not be able to rely solely on its CPRA and/or GDPR compliance efforts in complying with the act.

On June 8, 2021, the Colorado legislature passed SB 21-190, known as the Colorado Privacy Act (CPA), which the governor signed into law on July 7, 2021. The CPA is, in large part, modeled on the CDPA, but with CCPA/CPRA influences, such as a broader definition of "sale" and requiring companies to look for and honor global privacy signals. It uses the categories of controller and processor as do the CDPA and the GDPR.

As a reminder, Nevada enacted a much more limited law regarding the sale (for cash consideration) of certain data collected online, effective October 1, 2019 (the PICICA), which was amended in 2021 to also cover sales by data brokers and to add a data broker registration requirement (California and Vermont also have data broker registration laws). Other states and the federal government are considering new consumer privacy laws. The regulatory requirements are evolving, so a privacy compliance program will need to be flexible enough to evolve with changes to law.

The infographics that follow summarize and compare these laws at a very high level. Detailed guidance materials are available.

Scope of Coverage

The following chart demonstrates the similarities and differences of the current US consumer privacy laws of general application, and compares them to the GDPR:

Consumer Right	PICICA	CCPA	CPRA	CDPA	GDPR	CPA
Right to access	✗	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	✗	Implied	Implied	✓	✓	✓
Right to data portability	✗	✓	✓	✓	✓	✓
Right to delete ~	✗	✓	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	✗	✗	✓	✓	✓	✓
Notice and transparency requirements	✓	✓	✓	✓	✓	✓
Right to opt-out of sales	✓[1]	✓[5]	✓[5]	✓[4]	✓[2]	✓[5]
Right to opt-out of targeted advertising (CO and VA)/cross-context behavioral advertising sharing (CA)	✗	✗[3]	✓	✓	✓	✓
Right to object to or opt-out of automated decision-making ~ ~	✗	✗	✓	✓	✓	✓
Opt-in or opt-out for processing of "sensitive" personal data? "Sensitive" is defined differently under CPRA, CDPA and CPA	✗	✗	Opt-out[6]	Opt-in	Opt-in[7]	Opt-in[6]
Right to object to/restrict processing generally	✗	✗	✗	✗	✓	✗
Right to non-discrimination	✗	✓	✓	Limited	Implied	Limited
Purpose/use/retention limitations	✗	Implied	✓	✓	✓	✓
Applies to both consumers and in HR and B-to-B contacts	✗	+	++	✗	✓	✗
Privacy and security impact assessments sometimes required	✗	✗	✓	✓	✓	✓
Obligation to maintain reasonable security	✗	✓	✓	✓	✓	✓

[1] Website and online service operators are required to offer an "opt-out," but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

[2] Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

[3] However, certain data disclosures inherent in this type of advertising are arguably a "sale," subject to opt-out rights.

[4] Cash consideration required; online and offline data covered.

[5] Any consideration required; online and offline data covered.

[6] Under the CPRA, consumers' opt-out rights do not apply to processing sensitive personal information for certain limited purposes. The purpose limitations to controller and processor obligations in the CPA would seem to apply to both personal data and sensitive data.

[7] Under the GDPR, processing sensitive personal information is allowed with explicit consumer consent, or where it is otherwise justified under another recognized lawful basis.

+ Yes, but most provisions suspended until January 1, 2022.

++ Yes, but most provisions suspended until January 1, 2023.

~ In California, deletion obligations are limited to PI collected from the consumer, but in Virginia and Colorado, it is any PI about the consumer.

~ ~ Colorado and Virginia only regulate automated decision-making if it results in legal or similarly significant impacts on the consumer, whereas California leaves open the scope of the right for rulemaking.

Exclusions

The CPRA, CDPA and CPA include exclusions, some differing from CCPA and each other, as illustrated below:

Exclusions	CCPA	CPRA	CDPA	CPA
Employee/HR data	Now superseded by CPRA	Mostly exempt until 1/1/23.	Exempt (CPPA/CPRA-style definition).	Exempt, but only in so far as maintained as an employment record.
B-to-B contact/ communications data	Now superseded by CPRA	Mostly exempt until 1/1/23.	Specifically exempt + data subjects are only consumers in so far as they act in an individual or household capacity.	Data subjects are only consumers in so far as they act in an individual or household capacity.
Publicly available	Exempts lawfully available government public records data.	Expands CCPA definition to also include lawfully obtained truthful information of public concern, information made available by another person not under a disclosure restriction, information from the mass media and information the consumer publicly makes available.	The same as CPRA.	Exempts lawfully available public records data and personal data the controller reasonably believes the consumer made available to the general public.
De-identified	Exempt.	Exempt.	Exempt.	Exempt.
Household data	Not exempt.	Exempt from right to delete, right to correct and right to access (Sections .105, .106, .110 and .115).	Not exempt.	Not exempt.
Aggregate	Exempt (different definition than de-identified).	Exempt (different definition than de-identified).	Not exempt, unless meets the definition and requirements for de-identified.	Not exempt, unless meets the definition and requirements for de-identified.
Government entities	Exempt as a business or service provider but could be a third party or exempt third party.	Exempt as a business, but could be a service provider, contractor or third party.	Any Virginia state or local government agency or body and institutions of higher learning, as defined, are exempt.	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processors are any person processing on behalf of a controller.
Non-profits	Exempt as a business and service provider, but could be an exempt third party.	Exempt as a business, but could be a service provider, contactor or third party.	Exempts certain types of non-profit organizations (corporations organized under the Virginia Nonstock Corporation Act and organizations exempt from taxation under §§501(c)(3), 501(c)(6) and 501(c)(12) of the Internal Revenue Code).	Controllers are only regulated if they conduct business in, or produce or deliver commercial goods or services to, CO and meet the processing thresholds. Processor is any person processing on behalf of a controller.

Exclusions	CCPA	CPRA	CDPA	CPA
GLBA/financial institutions	Exempts PI collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), but does not exempt security or breach liability.	Changes "pursuant to" GLBA to "subject to," and adds the Federal Farm Credit Act (FFCA).	Exempts financial institutions subject to the GLBA, plus GLBA-regulated data and "PD collected, processed, sold, or disclosed in compliance with the" FFCA.	Financial institutions subject to the GLBA, and their affiliates, plus GLBA-regulated data.
FCRA/credit reporting	Exempts certain activities of consumer reporting agencies and users of consumer reports, each subject to compliance with the Fair Credit Reporting Act (FCRA).	Expands CCPA exemption to include certain furnishing of data for consumer reports.	Exemption largely tracks CCPA.	Exemption largely tracks CPRA.
HIPAA/health	Exempts medical information governed by the CA Confidentiality of Medical Information Act (CMIA) and protected health information under the Health Insurance Portability and Accounting Act (HIPAA) and CMIA providers and HIPAA, covered entities to the extent they protect patient data as required by CMIA and HIPAA, and certain clinical trial data.	Expands CCPA exemption to include certain biometric research.	Exempts covered entities and business associates, as those terms are defined by the Health Insurance Portability and Accountability Act (HIPAA) + protected health information, as defined under HIPAA, and certain other types of health-related information.	Exempts protected health information, as defined under HIPAA, and certain other types of health-related information, more detailed than under the CDPA or CCPA/CPRA.
COPPA/children	Not exempt.	"CPRA shall not be deemed to conflict with obligations under the Children's Online Privacy Protection Act (COPPA)."	Exempts controllers and processors that comply with the verified parental consent requirements of COPPA.	Exempts personal data that is "regulated by" COPPA (i.e., personal information collected from a child under 13 online).
FERPA/ educational	Not exempt.	Not exempt but certain exemptions regarding access to student records under the state Educational Code or to opt-in use for production of physical items such as yearbooks.	Exempts institutions of higher learning as defined by state law + personal data "regulated by" FERPA.	Exempts personal data that is "regulated by" FERPA.

Exclusions	CCPA	CPRA	CDPA	CPA
DPPA/drivers information	Exempts PI "collected, processed, sold, or disclosed pursuant the Driver's Privacy Protection Act" (DPPA).	Same as CCPA.	Exempts personal data that is "collected, processed sold, or disclosed … in compliance with the" DPPA.	Exempts personal data that is "collected, processed sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealers regarding motor vehicle repair and warranty use and no other purpose. Note, not all motorized vehicles meet the definition of motor vehicle.	Same as CCPA.	No specific exemption.	No specific exemption.
Air carriers	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Not exempt (but preemption savings clause).	Exempt (as defined in 49 U.S.C. Sec.40101 and 41713).
SEC-regulated	Not exempt.	Not exempt.	Not exempt.	Exempts SEC-registered "national securities associations."
Public utilities	Not specifically exempt, but see government and non-profits above.	Not specifically exempt, but see government and non-profits above.	Not specifically exempt, but see government and non-profits above.	Exempts customer data maintained by certain public utilities if "not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law."
Activates protected by free speech/1st Amendment or other Constitutional rights	Exempt.	Exempt.	Exempt.	Exempt.

Recommendations

Below are high-level recommendations for adapting your current privacy program for CPRA, CDPA and CPA compliance, and to help prepare for other potential new consumer privacy laws that may follow, along with a summary of workstreams to enable you to do so. A more detailed 40-page version of the workstreams for use with project management is available for a fixed fee.

1. Assess Compliance and Gaps, and Prepare a 2023 Preparedness Plan

Workstream 1: Preliminary Scoping and Information Gathering [Q4 2021]

- Conduct a readiness assessment and gap analysis based on existing privacy compliance materials developed for CCPA compliance (e.g., data maps, internal policies, external privacy policy, rights requests procedures, contracts, training, etc.) and practices (e.g., consumer rights response program, cookie consent management platform, etc.).
- Develop a detailed work plan listing all required/optional tasks to allocate roles and responsibilities and a way to track the status and completion of each task. We have tools available at a fixed fee to enable you to do this. Develop a budget tied to the project plan and obtain approval.

2. Create or Update Data Inventories or Maps and Develop and Deploy Data Management Capabilities

Workstream 2: Data Mapping [Q4 2021 and Throughout 2022]

- Update/develop data map(s) to identify how the following categories of PI[1] are collected, used, transferred or disclosed, and for what purposes:
  - Sensitive PI
  - B-to-B contact PI
  - Employee/contractor PI
- Identify categories of PI that may be totally or partially exempt from the CPRA, CPA or CDPA, such as PI regulated by the FCRA, GLBA and HIPAA, and certain educational data.
- Determine the reasonably necessary retention period, and the processing purposes, for all PI.

3. Update Privacy Policy(ies) and Remediate Practices

Workstream 3: Annual Privacy Policy Update and Program Audit [Q4 2021]

4. Refine Your Consumer Request Procedure

Workstream 4: Consumer Rights [2022]

- Modify processes for responding to requests to exercise existing CCPA consumer rights to address new CPRA, CPA and CDPA requirements (e.g., to reflect the longer look-back period for the right to access). In addition, you will need to expand existing rights processes to apply to B-to-B contact PI and applicant/employee/contractor PI for rights requests from California residents.

5. Implement Privacy-by-Design and Data Governance

Workstream 5: Privacy Impact Assessments and Cybersecurity Audits [2022]

- CPRA requires businesses that engage in high-risk processing activities to perform impact assessments that must be filed with the California Privacy Protection Agency. Similarly, the CDPA and CPA require a controller to conduct a data protection assessment of certain processing activities, including targeted advertising, the sale of PI, the processing of sensitive PI and any other processing activities that present a heightened risk of harm to consumers.
- Consider a privacy impact assessment program for all PI processing, to help meet purpose, proportionality, data minimization, retention and other requirements and reduce risks.

6. Update or Implement a Vendor and Data Recipient Management Program

Workstream 6: Vendor/Supplier Contracts [Q4 2021 and Throughout 2022]

- Review and, as necessary, amend/execute (upstream and downstream) contracts to ensure compliance with the CPRA, CPA and CDPA (mainly prohibiting secondary uses, allowing for audits and requiring assistance honoring consumer rights) and to avoid transfers of PI being considered a "sale" and to address expanded deletion requirements.
- Identify any (upstream and downstream) contracts that involve the processing of "de-identified" data to include new contract terms required by the CPRA, CPA and CDPA.

[1] PI means personal information under the CCPA/CPRA and/or personal data under the CDPA and/or CPA.

7. Update Policies

Workstream 7: Review/Develop/Update Policies [2022]

- Update/develop policies to support CPRA, CPA and CDPA compliance, including:
  - Privacy policy(ies) and notices (internal and external)
  - Consumer rights procedures
  - Privacy impact assessments
  - Audit functions
  - Data retention policies and schedules
  - Record-keeping requirements

8. Implement Reporting, Recordkeeping and Training

Workstream 8: Administration and Training [2022]

- Update training materials for personnel with specific responsibilities for handling consumer requests or compliance to reflect new CPRA, CPA and CDPA requirements. Consider broader training, especially regarding privacy impact assessments and privacy-by-design and security.
- Confirm that record-keeping and reporting meet the requirements of the final regulations, and any new rulemaking as promulgated throughout 2022.

9. Shore-up Data Security and Breach Preparedness

Workstream 9: Other Compliance (Optional But Recommended) [2022]

- Review and update a written information security program plan, including incident response plan, acceptable use policy, cookie management and vendor security program.
- Conduct privacy compliance and security breach preparedness (i.e., "tabletop") exercises.

10. Project Audit and Go-Live [Q4 2022]

Workstream 10: Final Compliance Check and Remediation

- Use a project tracker and compliance checklist to confirm that the responsible persons have signed off on the completion of each task. We have developed such a tool and provide it to clients for a fixed fee.
- Beta test and QA check the new notices and consumer rights tools before going-live.

Businesses will benefit from immediately taking steps to develop and implement a CPRA/CDPA/CPA preparedness plan and to thereafter continue to improve compliance on a risk-based basis. Doing so will further help a business prepare for additional consumer privacy laws likely to follow, at the state or federal levels, and will provide the added benefit of better understanding its data and how that can be commercially exploited in a legal and consumer-friendly manner.

Our US Consumer Privacy Preparedness Taskforce

Ann LaFrance
Senior Partner, New York
E ann.lafrance@squirepb.com

Alan Friel
Partner, Los Angeles
E alan.friel@squirepb.com

Elliot Golding
Partner, Washington DC
E elliot.golding@squirepb.com

Kyle Fath
Of Counsel, Los Angeles
E kyle.fath@squirepb.com

Glenn Brown
Of Counsel, Atlanta
E glenn.brown@squirepb.com

Kyle Dull
Senior Associate, New York

Niloufar Massachi
Associate, Los Angeles

Gicel Tomimbang
Associate, Los Angeles