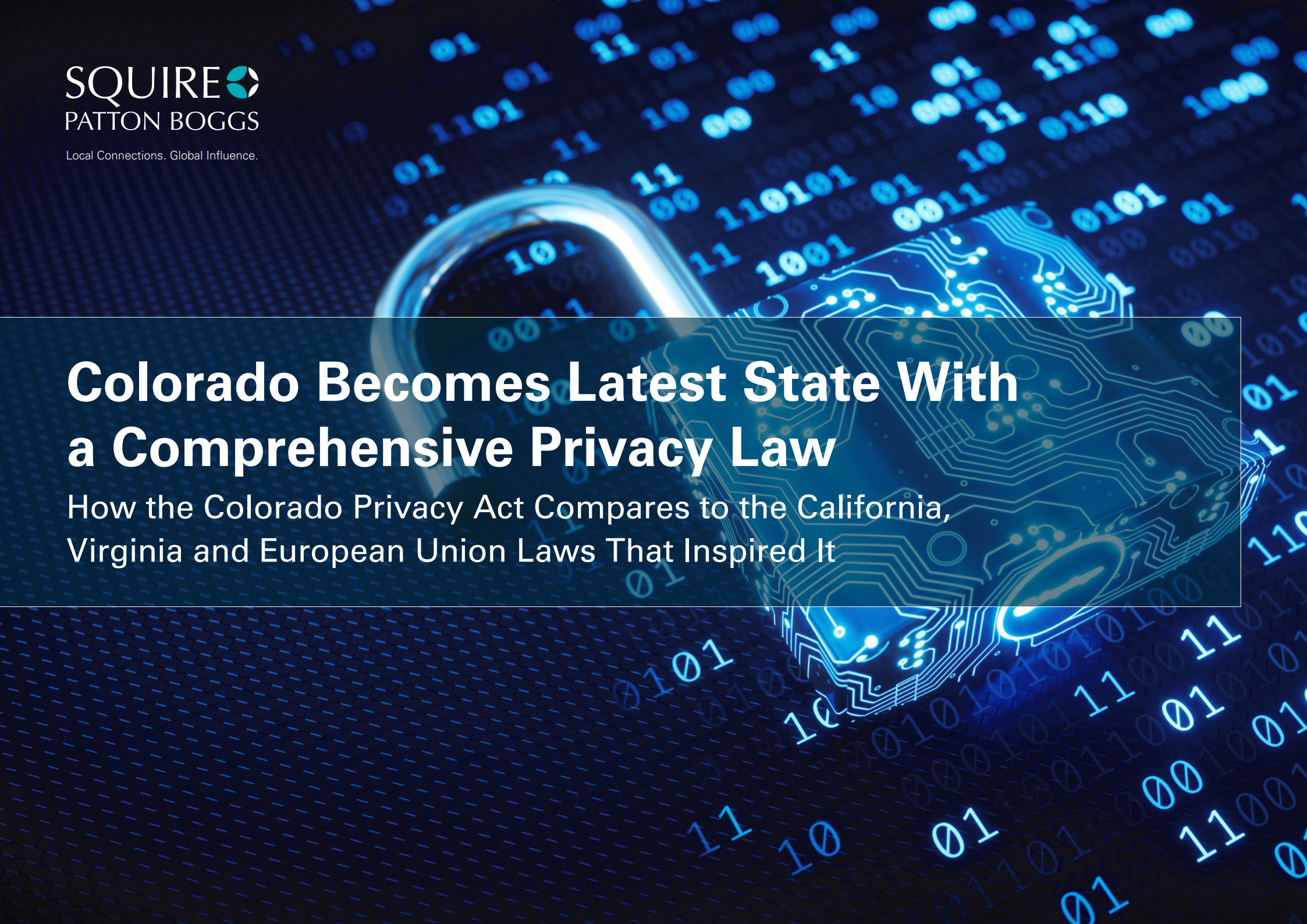
SQUIRE PATTON BOGGS

Local Connections. Global Influence.



Colorado Becomes Latest State With a Comprehensive Privacy Law

How the Colorado Privacy Act Compares to the California, Virginia and European Union Laws That Inspired It

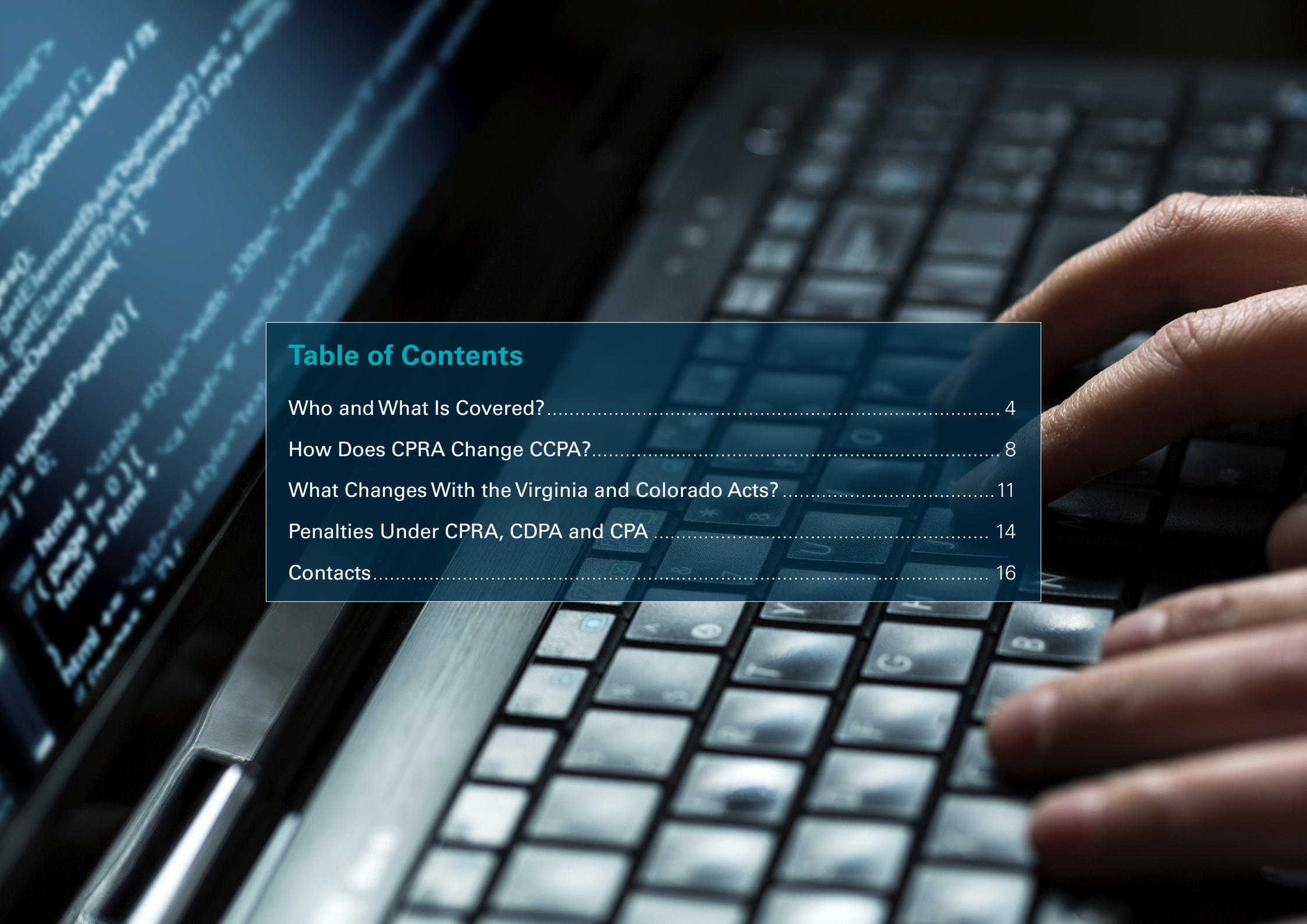


Table of Contents

On June 8, 2021, the Colorado legislature passed SB 21-190, known as the Colorado Privacy Act (CPA or CO Act), which the governor signed into law on July 7, 2021.

The CO Act is a mishmash of concepts from other jurisdictions. It is in large part modeled on the March 2021 Virginia Consumer Data Protection Act (CDPA), but with California influences, such as a broader definition of "sale" and requiring companies to look for and honor global privacy signals. Both the California consumer privacy regime, and even more so the CDPA, were inspired by Europe's General Data Protection Regulation (GDPR), but depart from it in many material ways. If the California law was consumer privacy 1.0 for the US, and Virginia 2.0, it seems that Colorado hopes to be the 3.0 (or maybe v 2.1) model for the rest of the nation. Indeed, in the act's declaration of purpose, the Colorado legislature found:

- "States across the United States are looking to this [law] and similar models to enact state-based data privacy requirements and to exercise the leadership that is lacking at the national level"
- "By enacting this [law] Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue innovate"

In the pages that follow, we break down the similarities and differences of the three US state consumer privacy regimes. A more detailed analysis and workstreams for assessing and establishing compliance readiness, as well as detailed project plans and compliance checklists, are available to clients. Please contact the author for further information.

Overview

Changes in US consumer privacy law passed in late 2020, and to date in 2021 will require most US businesses to make material changes to their data privacy compliance and information governance programs by January 1, 2023 (July 1, 2023, in the case of Colorado).

The California Privacy Rights Act (CPRA or Title) 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, and further legislative extensions are unlikely since the CPRA prohibits legislative amendments that do not "enhance" privacy, though there could ultimately be somewhat different rules for these non-consumer data subjects. More information on the CPRA is available.

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 PI under the CCPA/CPRA) of its residents generally, but excluding data subjects outside of an individual or household context and does not include persons acting in an employment or B-to-B context, provided, however, that HR data used outside of HR purposes could be within the scope of consumer rights. Like the CCPA/CPRA, certain already regulated data, such as protected healthcare information, is also carved out of the new Virginia law. Set to go into effect on January 1, 2023, the CDPA (or the VA Act) is in many ways similar to the CPRA, but it also shares some additional concepts inspired by the EU's GDPR. However, it is sufficiently dissimilar to each of those laws that a business developing a strategy for compliance with the VA Act will not be able to rely solely on its CPRA and/or GDPR compliance efforts in complying with the act.
More information on the CDPA is available.

The CO Act is in large part modeled on the VA Act, 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 does the VA Act and the GDPR.
More information on the CPA is available.

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 (CA and VT also have data broker registration laws). Other states and the federal government are considering new consumer privacy laws. In addition, the National Conference of Commissioners on Uniform State Laws, in an effort to try to harmonize state privacy laws, has been working on a model bill, known as the Uniform Personal Data Protection Act (UPDPA), an April 23, 2021 revision of which is currently in a public comment period. The UPDPA proposes the controller/processor distinction that comes from GDPR and was not adopted by California. Rather than laying out various opt-ins and opt-outs, it permits processing that is consistent with the ordinary expectations of data subjects or that is likely to substantially benefit them. All other processing requires consent, and certain types of processing are outright prohibited. Another interesting aspect of the proposal is the ability for the state to grant safe harbor for industry development of voluntary consensus standards. Time will tell if the UPDPA proposals influence new states' legislation or federal legislation.

A Comparison

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

Consumer Right	PICICA	CCPA	CPRA	CDPA	GDPR	CPA	UPDPA
Right to access	×	✓	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	×	Implied	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	✓*	✓*****	✓*****	✓****	✓**	✓*****	Possibly†††
Right to opt-out of targeted advertising (CO and VA)/cross-context behavioral advertising sharing (CA)	×	×***	✓	✓	✓	✓	×
Right to object to or opt-out of automated decision-making	×	×	✓	✓	✓	✓	Possibly†††
Opt-in or opt-out for processing of "sensitive" personal data? "Sensitive" is defined differently under CPRA, CDPA and CPA	×	×	Opt-out†	Opt-in	Opt-in††	Opt-in†	Possibly†††
Right to object to/restrict processing generally	×	×	×	×	✓	×	×
Right to non-discrimination	×	✓	✓	Limited	Implied	Limited	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	×	✓	✓	✓	✓	✓	×

* 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.

** 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.

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

**** Cash consideration required; online and offline data covered.

***** Any consideration required; online and offline data covered.

† 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.

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

††† The UDPA does not require consent for processing that is consistent with the ordinary expectations of data subjects or that is likely to substantially benefit them. All other processing requires consent, and certain types of processing are outright prohibited.

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

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

+++ HR data excluded, but B-to-B included.

Accordingly, covered businesses will need to be prepared to honor new data subject rights well beyond what is currently required by the CCPA and the PICICA. In addition, the CPRA, CDPA and CPA have strict purpose, proportionality and minimization obligations, and the CPRA requires the disclosure of retention periods (or, if not then "possible," how that period will be determined), by category of data, at the point of collection. As a result, covered businesses will need to develop very detailed retention schedules that include purposes of processing and are tied to categories of data and a defensible destruction program. This goes well beyond what public companies must have in the way of retention programs and schedules under the Sarbanes-Oxley Act and SEC regulations, though these are a good starting point. Further, since the Title requires such retention schedules be available for consumers to review at the points of data collection, it will be readily apparent to the AG and CalPPA, the new privacy protection agency created by the CPRA, by merely sweeping website privacy notices, which companies have insufficient retention schedules.

- For more information on what is covered and exempted under each of the three states' laws.
- For details on how CPRA changes CCPA.
- For more information on how CDPA and CPA differ from CCPA/CPRA, and each other.
- For a summary of how these laws will be enforced and the penalties for non-compliance.

Recommendations

Below are high-level recommendations for adapting your current data privacy program for CPRA, CDPA and CPA compliance, and to help prepare for other potential new consumer privacy laws that may follow:

1	Create or update data inventories or maps and develop and deploy data management capabilities
2	Address personnel data and B-to-B communications
3	Conduct privacy impact assessments of data activities, including website and mobile app audits
4	Update privacy policy(ies)
5	Update or implement a vendor and data recipient management program
6	Develop and implement a consumer request procedure
7	Shore-up data security and breach preparedness
8	Implement Privacy-by-Design
9	Assess compliance and gaps, and prepare 2022 notices and a 2023 preparedness plan
10	Implement reporting, recordkeeping and training

We recommend that you undertake a CCPA compliance review and CPRA/CDPA/CPA gap analysis in the third quarter of this year as part of preparing your January 1, 2022 California privacy notice update, and then complete the CPRA/CDPA/CPA compliance workflows during 2022. Sufficient budget for these 2022 activities should be sought. The goal should be to have a program in place that can easily be tweaked to address additional state or federal laws that may pass between now and January 1, 2023, and one strategic decision you will have to make is if you want to apply rights on a state-by-state basis or afford all data subjects the highest level of rights, and only distinguish where harmonization is just not possible or there is a business imperative for applying lesser rights where possible. 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. Further, doing so will further help prepare for additional consumer privacy laws likely to follow, at the state or federal level, and will provide the added benefit of better understanding data assets and how they can be commercially exploited in a legal and consumer-friendly manner.

Who and What Is Covered?

Companies will need to reassess their scope of coverage, as the CPRA, CDPA and CPA have material differences in this regard from the CCPA.

The CPRA applies to a wide range of businesses that handle Californians' personal information (PI), obligating them to comply with a host of new requirements governing their collection, use and sharing of PI. Most businesses need to update the disclosures in their privacy notices, establish processes for responding to new consumer rights requests and potentially updating those that relate to existing rights, observe restrictions on data sharing and monetization practices, and revisit relationships and contracts with vendors that handle PI on their behalf and third parties with which they share PI. The CPRA impacts many businesses and business activities not previously subject to privacy regulations in the US, regardless of whether the business is located in California or not. The CPRA applies to for-profit entities "doing business" in the state that control PI and meet one of the three thresholds below (a Business):

- Have a gross annual revenue in excess of US$25 million
- Annually buy, sell or "share" for cross-context behavioral advertising purposes PI of 100,000 or more California consumers or households [this is a material change from the CCPA, which was 50,000 and included "devices" and without limiting the count to Californians]
- Derive 50% or more of their annual revenues from selling or "sharing" for cross-context behavioral advertising California consumers' PI

The CPRA also treats as a Business, regardless of whether it meets one of those thresholds, any entity with whom a Business "shares" PI that (1) controls, or is controlled by, a Business that meets the above criteria, and (2) shares common branding with that Business. Certain joint ventures, partnerships and persons that voluntarily self-certify adherence are also a Business subject to the CPRA, and applicable joint ventures and partnerships must be treated as separate Businesses from their members. The CCPA applied certain conditions to service providers and third parties, regardless of revenues or processing volume, and the CPRA increases these obligations (and brings non-profit service providers into scope), though it still requires less than is required of a Business acting as the data controller. (Some third parties will also be a Business.) There are certain limited exceptions designed not to conflict with other laws, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act (financial institutions) and HIPAA (healthcare), detailed in the chart below.

The VA Act applies to natural or legal persons that act as "controllers" and "processors" (defined in a manner that tracks to the GDPR) provided that:

- They conduct business in the state of Virginia or produce products or services that are targeted to Virginia residents
- In a calendar year, either (i) control or process the personal data of at least 100,000 Virginia residents; or (ii) control or process the personal data of at least 25,000 Virginia residents and derive at least 50% of their gross revenues from the "sale" (as defined in the act) of personal data

The CO Act tracks the VA Act excepting that a business will be covered if it derives any revenue from the sale of personal data and it controls or processes the personal data of at least 25,000 Colorado residents.

Unlike the CCPA/CPRA, the VA Act and the CO Act do not include a gross revenue component for determining applicability; instead, they focus on the number of consumers whose personal data is controlled or processed, and on the selling of personal data. Therefore, even very large businesses doing business in Virginia and Colorado may not be subject to the acts if they do not meet one of two volume-based thresholds described above.

PICICA applies to most operators of online services and data brokers, but excludes certain operators of online services that are not a primary source of revenue and have fewer than 20,000 unique visitors a year.

The CO Act and the VA Act includes exclusions, some differing from CCPA/CPRA and each other, as illustrated below:

Exclusions	CCPA	CPRA	CDPA	CPA
Employee/HR data	Mostly exempt until 1/1/22.	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	Mostly exempt until 1/1/22.	Mostly exempt until 1/1/23.	Specifically exempt + data subjects are only consumers insofar as they act in an individual or household capacity.	Data subjects are only consumers insofar 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.	Tracks 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 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 of 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 any institution of higher learning, as defined, is 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.

Exclusions	CCPA	CPRA	CDPA	CPA
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.
GLBA/financial institutions	Exempts personal information "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 "personal data collected, processed, sold, or disclosed in compliance with the" FFCA.	Exempts financial institutions subject to the GLBA, and their affiliates, plus GLBA-regulated data.
FCRA/credit report	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 VA Act 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 + PD "regulated by" FERPA.	Exempts PD that is "regulated by" FERPA.
DPPA/driver's license	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 PD that is "collected, processed sold, or disclosed … pursuant to" DPPA, if such activity "is regulated by that law."

Exclusions	CCPA	CPRA	CDPA	CPA
Vehicles	Exempts vehicle information and ownership information retained or shared between manufacturers and dealer 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 potentially – see government and non-profits above.	Not specifically exempt, but potentially – see government and non-profits above.	Not specifically exempt, but potentially – 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.

Note that unlike the CCPA and CPRA, the VA Act and the CO Act provide for certain entity-level exemptions. This means that a financial institution subject to the GLBA (and in CO their affiliates) is exempt even if it holds personal data that is not directly regulated by the GLBA. Under the CCPA/CPRA, financial institutions likely will have PI that is both covered and exempt under the act. The VA Act does the same for a covered entity or business associate under HIPAA, whereas the CO Act applies exemption to certain HIPAA-regulated and other regulated healthcare information, though with more detailed carve-outs than CCPA/CPRA.

Like the CCPA and CPRA definition of personal information, "de-identified" data is not treated as personal data under the CDPA or CPA, but all four have differing standards as to what must be done to qualify data as de-identified. This will require attention when providing vendors and others with the ability to use de-identified data. Each of the CCPA, CPRA, CDPA and CPA also exclude "publicly available" data, but again the definitions differ somewhat.

How Does CPRA Change CCPA?

The CPRA will introduce a host of new consumer rights and corresponding Business requirements. We highlight some of the key changes below:

New Principles:

- **Data minimization/purpose limitation** – The CPRA requires the collection, use, retention and sharing of personal information to be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed…." While data minimization is generally considered best practice in the US, this concept had not been broadly codified prior to the CPRA. The CPRA also reinforces that personal information cannot be used in a manner that is "incompatible with the disclosed purpose for which the personal information was collected" without providing the consumer with notice.
- **Storage limitation** – Also, whereas the CCPA was silent on retention, the CPRA prohibits storing personal information for longer than is "reasonably necessary" for the purpose disclosed at the time of collection, and that this period be disclosed, by category of PI, at collection (or if it is not then "possible" to determine the reasonably necessary period then to explain how that will be later determined).

These new principles will make detailed data inventories, including purposes of processing, essential and necessitate far more detailed retention and defensible destruction programs and schedules necessary than even what is now required of public companies. For many companies, this will be a time- and resource-consuming task, which can be aided through the use of one of several SaaS/PaaS tools.

- **New "sensitive personal information" category** – The CPRA creates a new category of "sensitive personal information," which is subject to specific additional restrictions. Sensitive personal information is broadly defined to include, among other things, some government-issued IDs; certain financial, genetic, biometric and health information; precise geolocation; race and ethnicity; religion; union membership; content of certain communications; and information about sex life or sexual orientation.
- **New Rights**:
  - **Restrict the use and disclosure of sensitive personal information** – The CPRA provides consumers with the right, at any time, to direct a business to limit its use and disclosure of sensitive personal information to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services…" In order to allow consumers to exercise this right, businesses will be required to display a link on their internet homepage(s).
  - **Ability to correct personal information** – The CPRA grants consumers a new right to correct inaccurate personal information.
  - **Opt-out of "sharing"** – The CCPA definition of "sale" is widely debated, with many arguing it already includes various aspects of sharing related to online advertising. The CPRA settles the debate insofar as it adds another opt-out for sharing in relation to cross-context behavioral advertising (CCBA). The CPRA defines "sharing" as the transferring or making available of "a consumer's personal information by the business to a third party for cross-context behavioral advertising" and CCBA as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctively-branded websites, application or services, other than the business, distinctively branded website, application or service with which the consumer intentionally interacts."
  - **Automated decision-making** – The CPRA requires the adoption of new regulations "governing access and opt-out rights with respect to a business's use of automated decision-making technology, including profiling…."

- **Expanded right to access** – The right of access is expanded under the CPRA by deleting the existing 12-month look-back limitation of the CCPA with regard to both the obligation to provide access to specific pieces of PI and the obligation to disclose the categories of PI shared or sold. In practice, however, due to the way the CPRA goes into effect, businesses will have to provide access to any information "collected" (as defined in the CPRA) on or after January 1, 2022, unless providing such access proves "impossible or would involve a disproportionate effort" (a threshold that will be defined by regulation).
- **New Obligations**:
  - **Contracting with vendors** – The CPRA imposes new obligations on "service providers" and "contractors." Among other things, a written contract is needed that requires the data to be used for business purposes and prohibits the "selling" or "sharing" of the PI. It is recommended for the contract to, among other things, (1) limit the vendor's ability to combine the PI with other information, (2) require notification to the Business when engaging subcontractors, and (3) mandate that obligations be flowed down to any engaged subcontractors. Given that vendor relationships often last many years and the failure to qualify a vendor as a service provider or contractor could trigger a "sale," updating vendor agreements sooner rather than later is recommended. The CPRA also adds more vendor monitoring and remediation obligations necessitating a robust vendor management program.
  - **Reasonable security** – The CPRA requires businesses to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosures." This express obligation does not exist under the CCPA but has already been codified under California law (Civ. Code Sec. 1798.81.5(a)) for certain types of personal information and implied by the CCPA's private right of action for certain security incidents where failure to maintain reasonable security led to the breach.
  - **Privacy impact assessments and cybersecurity audit requirements for high-risk activities** – The CPRA requires the issuance of regulations regarding mandatory risk assessments and cybersecurity audits for high-risk activities. The risk assessments will have to be submitted to the CalPPA, a new data authority created by the CPRA, on a "regular basis." The concept of a "regular basis" is not defined in the CPRA and is likely to be expanded upon in the implementing regulations. Although not required for lower-risk processing, the purpose, proportionality and retention obligations make assessments practically necessary for all processing.
- **Regulatory audits** – The CalPPA will have the right to audit entities for compliance with the CPRA. This ability is very loosely addressed in the CPRA text, and we expect that the regulations will provide details around these practices.

As a reminder, the CCPA already grants California residents the right to request that a business:

- Disclose the categories and, in a transportable format, the specific pieces of PI it has collected about the consumer in the preceding 12 months
- Disclose the categories of sources from which the PI is collected
- Disclose the business or commercial purpose for which it collected or sold the PI
- Disclose the categories of third parties with whom the Business shares PI
- Disclose the categories of PI that the Business sold in the preceding 12 months and, for each category identified, the categories of third parties to which it sold that particular category of PI
- Disclose the categories of PI that the Business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of PI
- Delete any PI the Business collected directly from the consumer, subject to certain exceptions
- Not "sell" (broadly defined, and not requiring any monetary consideration for the disclosure) the consumer's PI (the "Do Not Sell" or "DNS" opt-out) [the exceptions to "sell" are disclosures at the direction of the consumer; to qualified service providers subject to contractual restrictions; to facilitate the opt-out; and as part of M&A transactions, subject to use restrictions]

Businesses typically must respond to CPRA rights requests within 45 days of receipt (but the DNS opt-out right is currently "as soon as feasibly possible, but no later than 15 business days," with a clawback for any disclosures made after the notice was received) and must provide certain easily accessible, cost-free methods for exercising these rights. The CPRA adds a requirement that service providers and contractors delete PI upon notice by a Business that has received a deletion request, and that Businesses pass deletion requests on to third parties. However, curiously, it does not add a corresponding obligation for third parties to act on such a notice from a Business. For all but the DNS right, currently businesses need only respond to a "verifiable consumer request," defined as a request made by or on behalf of a consumer that the business can reasonably verify. Under CPRA, such verification standards will also be applied to the right of correction, but not, unless added by the regulations, to the new rights to opt-out of data "sharing" for cross-context behavioral advertising, use of sensitive information or profiling. Existing regulations provide details on both rights' exercise mechanics and clarify the requirements for verification of consumers making requests, but it is expected that they will be updated and changes are possible.

The CPRA adds several new elements to the required disclosures that must be included in an enterprise-wide privacy notice. In addition to the information that must be included under the CPRA and other California privacy laws, online privacy policies and any California-specific notice must:

- Explain not only all existing CCPA rights, but also new consumers' rights under the CPRA and how to exercise them, and designated methods for submitting requests.
- Identify the length of time that a business intends to retain each category of PI, including sensitive PI, or if that is not possible, the criteria used to determine that period. Note that given different data elements within one of the enumerated categories of PI may have different retention periods, greater granularity may be required. It may essentially be necessary to post a link to a comprehensive retention schedule that includes PI categories tied to CCPA/CPRA business and commercial purposes.

As a reminder, the CCPA already requires that online privacy policies and any California-specific notice must:

- Describe the process the Business will use to verify a consumer request.
- Identify the categories of PI the Business has collected about consumers in the preceding 12 months.
- Identify the categories of sources from which the PI is collected.
- Identify the business or commercial purpose for which the PI is collected, used, disclosed and sold.
- Identify the categories of PI a Business has disclosed for a business purpose or sold to third parties in the preceding 12 months, and for each category of PI identified provide the categories of third parties to whom the information was disclosed or sold.
- Identify the categories of third parties with whom PI is shared.
- State whether or not the Business has knowledge that it sells the PI of minors under 16 years of age.
- State whether or not the Business sells PI and, if so, provide a link to a "Do Not Sell My Personal Information" web-based opt-out tool.
- Explain the right not to be discriminated against by differential prices or services based on the exercise or non-exercise of CCPA rights, subject to reasonable differences based on the value of the data and/or reasonable financial incentives for the data. The final regulations have detailed valuation disclosure requirements.
- Describe any opt-in financial incentives for providing data or not exercising rights and the right-to-terminate consent. The final regulations define financial incentives very broadly and provide for very detailed notice requirements at subscription and in the privacy policy.
- Provide instructions on how an authorized agent can make a request on a consumer's behalf.

Under the current regulations, Businesses that do not collect PI directly from consumers are not required to provide pre-collection notice, so long as they do not sell the consumer's PI. However, registered data brokers are permitted to sell PI that they did not collect directly from the consumer.

The final regulations provide for honoring global privacy controls (a similar concept has been added by the CPRA, and which Colorado has copied) and require certain recordkeeping, published statistics of high volume processing, and training.

Finally, both the CCPA and the CPRA subject companies that fail to undertake reasonable measures to ensure the security of PI to potential liability.

What Changes With the Virginia and Colorado Acts?

Just when you thought you had your arms wrapped around the CCPA/CPRA (and if you have not sorted out how CPRA changes CCPA), Virginia and Colorado complicate things.

The VA and CO acts provide residents with rights that largely align to the CPRA (right of access, correction, deletion, and opt-out of targeted advertising, sale and "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"), but each require opt-in to certain non-exempt processing of sensitive data (see chart below for exemptions that apply to CDPA/CPA consumer rights). However, the Colorado Act has broader exemptions to all controller and processor obligations than does Virginia, such as internal operations reasonably aligned with the expectations of the consumer based on the existing relationship, and this would seem to apply to sensitive data, as well as personal data generally. The Colorado definition of sale is closer to California (any consideration) than Virginia (only monetary consideration), and the definitions of cross-context behavioral advertising (CA) and targeted advertising (CO and VA have identical definitions) are materially different. While the CO and VA definitions of targeted advertising are the same, the opt-out applies only to controllers in VA, but as of January 1, 2024, opt-outs may be made also directly to a processor, as can opt-outs of sale. Colorado follows the lead of the CCPA and CPRA, calling for the development of standards for universal opt-out signals or settings consumers can apply broadly. Virginia does not.

Although similar, the rights provided by the VA Act and CO Act, and the corresponding obligations and limitations, are not identical to what is provided by the CCPA/CPRA and separate legal analysis will be required to identify the correct legal scope under the laws of each jurisdiction or to create the highest level of harmonization. For example, we include a chart below comparing the exceptions to the rights to delete under the CPRA and the exceptions to the limitations on controller processing under the CO Act and VA Act.

Exceptions to Deletion	CCPA	CPRA	CDPA	CPA
To comply with federal, state or local laws, rules or regulations	✓	✓	✓	✓
To comply with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by federal, state, local or other governmental authorities	✓	✓	✓	✓
To cooperate with law-enforcement agencies concerning conduct or activity that are reasonably and in good faith believed to violate federal, state or local laws, rules or regulations	✓	✓	✓	✓
To investigate, establish, exercise, prepare for or defend legal claims	Implied	Implied	✓	✓
To provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract	✓	✓	✓	✓
To prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report or prosecute those responsible for any such action	✓	See next below	✓	✓
To help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes	See above	✓	See above	See above
To engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws	✓*	✓*	✓**	✓***
To assist another controller, processor or third party with any of the obligations under the privacy law in question	×	×	✓	✓
To debug to identify and repair errors that impair existing intended functionality	✓	✓	✓	✓

Exceptions to Deletion	CCPA	CPRA	CDPA	CPA
To exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law	✓	✓	✓	✓
To comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code	✓	✓	×	×
To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business	✓	✓	✓	✓
To conduct internal research to improve, repair or develop products, services or technology	Implied	Implied	Implied	✓
To otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information	✓	×	×	×
To conduct the vital interest of a consumer or another individual	Implied	×	×	✓

* The CCPA and CPRA provide that the exception is available only if (a) deletion of the information is likely to render impossible or seriously impair the ability to complete such research; and (b) the consumer has provided informed consent.

** The CDPA requires that the research be approved, monitored and governed by an institutional review board, or similar independent oversight entities, that determine whether (i) the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

*** CPA limits to public health purposes subject to security and confidentiality obligations.

Notably, the VA Act and the CO Act give consumers the right to appeal a controller's refusal of a request before the entity that denied it and requires businesses to set up a process to address those appeals. Upon an appeal, a controller must (within 60 days for VA and 45 days (extendable by another 60) for CO) inform the consumer in writing of its response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also provide Virginia consumers with an online mechanism (if available) or another method through which the consumer can submit a complaint to the Virginia Attorney General, and inform Colorado consumers of the ability to bring complaints to the attention of the Colorado Attorney General.

In addition to providing consumers with the rights described above, the CO Act and VA Act impose certain obligations on controllers, including:

- **Data minimization and proportionality** – The VA Act provides that controllers must limit the collection of personal data to that which is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed." The Colorado Act lists permitted processing activities, but limits them to what is "necessary, reasonable and proportionate to the specific [permitted] purposes." The CPRA and the GDPR also impose a similar data minimization obligation.
- **Limitations on use** – The VA Act provides that unless a controller obtains a consumer's consent, it must not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes that the controller has disclosed to the consumer. Colorado reaches a similar result by limiting permitted purposes. Both acts require controllers to obtain a consumer's consent in order to process sensitive data (as defined), subject to certain exceptions. Although this is a more burdensome obligation than the obligations imposed on "sensitive personal information" under the CPRA, the Colorado and Virginia definitions of "sensitive data" are significantly more limited.
- **Reasonable data security** – The Colorado and Virginia acts require controllers to establish and maintain reasonable administrative, technical and physical data security practices that are appropriate to the volume and nature of the personal data maintained by the controller. The GDPR and the CCPA/CPRA have similar requirements.
- **Data protection assessments** – The Colorado and Virginia acts require controllers to undertake data protection assessments of certain types of high-risk processing activities. The acts specify the matters such assessments must address. The VA Act does not specify how often controllers are required to conduct these assessments or for how long they must be retained. The CO Act provides more detail on how to conduct assessments. Upon request, a controller must provide copies of such assessments to the Virginia or Colorado Attorney General, but the CO Act deems them to be confidential and subject to attorney-client or work product privilege, and exempt from the public records act.

- **Contracts with processors** – Both the VA Act and the CO Act require that a controller's contract with a processor clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. They also include specific terms that must be included in such contracts relating to the processor's use and disclosure of personal data. An odd result of the VA Act including applicability thresholds for processors is that a controller would not seem to be required to include any of these terms in contracts with small vendors that do not meet the thresholds described above in "Applicability of the Act." This is not the case with the CO Act, which applies the applicability thresholds only to controllers. As is recommended for the CPRA, given that vendor agreements can last for many years, moving to CDPA/CPA-compliant processor agreements should be done sooner rather than later. Like the CPRA, there are processor monitoring and remediation obligations for controllers that practically will require robust vendor management programs.
- **Anti-discrimination** – The Colorado and Virginia acts, using identical language, prohibit controllers from processing personal data in violation of anti-discrimination laws. The VA Act goes on to prohibit discriminating against consumers for exercising their rights under the act. However, both the VA Act and the CO Act avoid some of the interpretational challenges created by the CCPA's anti-discrimination prohibition by carving out price or service discrimination based on exercise of rights, without the need to justify the reasonableness as do CCPA/CPRA. In addition, neither have requirements for offering "financial incentives." Both make clear that there are to be no limits on typical opt-in loyalty and rewards programs offered by retailers.
- **Privacy notice** – The CO Act and the VA Act require controllers to provide a privacy notice to consumers that includes certain specified disclosures, but unlike CCPA and CPRA, these acts do not address when the controller must provide the notice or the means of delivery, and are less granular about what must be in the notice. While descriptions of categories of personal data and types of purposes are required, these acts do not enumerate specific categories of data or purposes to be used.

Compared to controllers, processors have relatively few obligations under the Colorado and Virginia acts. The following are their primary obligations:

- **Following the instructions of the controller** – The act requires processors to adhere to the instructions of a controller and to assist it in the matters described below.
- **Assistance to controllers** – Processors must assist controllers with responding to consumers' rights requests, with meeting the controller's obligations relating to the security of personal data and giving notice of a security breach, and with the processor's creation of the data protection assessments described above.

Penalties Under CPRA, CDPA and CPA

Violations of the CPRA are subject to enforcement by the CalPPA, a new data protection authority created by CPRA, and/or the Attorney General's office, with the law requiring that these agencies coordinate their actions.

Both agencies can seek civil penalties of US$2,500 for each violation or US$7,500 for each intentional violation or violations involving the data of minors. Violations may be potentially calculated based on each applicable piece of data or consumer and, thus, exposure could be substantial. The existing requirement in the CCPA to provide notice of violation and give a 30-day cure period before bringing an enforcement action is eliminated by the CPRA, but the law permits the agencies to consider good faith cooperation efforts by the Business when calculating the fine, and prosecutorial discretion is not limited. Further, CalPPA actions are subject to a probable cause hearing prior to commencement of an administrative enforcement proceeding. Enforcement of the CPRA is delayed until July 1, 2023.

The requirements for the existing limited private right of action, with the potential of statutory damages, for consumers following certain types of security incident attributable to a Business' failure to maintain reasonable security does not substantially change under the CPRA, except the CPRA clarifies that post-breach remediation of unreasonable security vulnerabilities does not satisfy the 30-day cure to prevent statutory damages. There is not otherwise a private right of action under the CPRA, but the CPRA opens the possibility of enforcement by California administrative agencies other than the AG and the CalPPA, and it is conceivable that an incomplete or inaccurate response to a consumer request might also give rise to an independent deception claim, and the plaintiff's lawyers are expected to otherwise test the scope of the limitation on private consumer and class action relief.

There is no private right of action for violations of the CO Act or the VA Act; the Virginia Attorney General has exclusive enforcement authority, and in Colorado Districts Attorney have jurisdiction in addition to the Attorney General. The VA Attorney General may seek injunctive relief and civil penalties of US$7,500 per violation. In Colorado, injunctive relief and civil penalties under the Colorado Consumer Protection Act, which provides for civil penalties of US$500 per violation, actual damages, or three times actual damages if bad faith is shown. However, like the CCPA (but unlike the CPRA), the VA Attorney General must provide a controller or processor with 30 days' written notice of any violation of the act, specifying the provisions that the Attorney General alleges have been violated, and in Colorado if a cure is "deemed possible," notice and a 60-day opportunity cure must be given. In Virginia, a controller or processor can avoid statutory damages if, within this 30-day cure period, it cures the noticed violation and provides the Attorney General with an express written statement that the alleged violations have been cured and that no further violations will occur.

The Colorado and Virginia acts provide that a controller or processor that complies with the act in disclosing personal data does not violate the act if the third party, controller or processor that receives such personal data violates the act (assuming the disclosing party had no actual knowledge that the recipient intended to violate the act). Likewise, a third party, controller or processor receiving personal data does not violate the act due to the disclosing party's violations of the act. The CCPA and CPRA have similar "safe harbors" for businesses and qualified service providers and contractors.

Contacts

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Ann J. LaFrance
Senior Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Glenn A. Brown
Of Counsel, Atlanta
T +1 678 272 3235
E glenn.brown@squirepb.com

Niloufar Massachi
Associate, Los Angeles
T +1 213 689 6580
E Niloufar.massachi@squirepb.com

Kyle Fath
Of Counsel, New York
T +1 212 872 9863
E kyle.fath@squirepb.com

Kyle R. Dull
Senior Associate, New York
T +1 212 872 9867
E kyle.dull@squirepb.com

Elliot Golding
Partner, Washington DC
T +1 202 457 6407
E Elliot.golding@squirepb.com

SQUIRE PATTON BOGGS

squirepattonboggs.com

41780/07/21