SQUIRE PATTON BOGGS

Are You July-1-READY?

2023 Privacy Laws and Regulations Call for Revisiting Your 2022 End-of-Year Compliance Efforts

US – June 2023

As of July 1, four states' privacy laws will be effective and enforceable – the California Consumer Privacy Act as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA), effective since January 1, becomes enforceable on that date; the Virginia Consumer Data Protection Act (VCDPA) has been effective and enforceable since January 1; and, on July 1, the Colorado Privacy Act (CPA) and Connecticut Data Privacy Act (CTDPA) are both effective and enforceable.

There are a number of compliance obligations that overlap among these laws where prior compliance efforts for the original CCPA in 2020, and in relation to its updates for January 1 of this year, will suffice for compliance with the other, non-California laws. This said, Colorado's regulations, promulgated on March 15, 2023, materially deviate from the CCPA in a number of consequential areas in a way that likely requires companies to revisit their January 2023 privacy notices and practices. Now is also a good time to address CPRA, CPA, CTDPA and VCDPA compliance posture generally. While some businesses plan to wait until their end-of-year review and update process, when they can also assess the many additional state laws that have or will pass this year, delaying compliance until then risks enforcement actions, particularly by California and Colorado regulators (interestingly, Connecticut's Attorney General recently released an FAQ).

This top-level summary of key considerations outlines the issues we are finding that clients have often overlooked in their January 2023 updates.

Privacy Policy Content Requirements

Of all of the state consumer privacy laws on the books, the CCPA and CPA are the most prescriptive as they relate to the content that must be in privacy policies and notices at collection. Here, while the two laws provide some overlap, there are a number of requirements found in the CPA rules that would not be satisfied by the disclosures found in a California-compliant privacy policy and/or notice at collection. Below, we list the most relevant of the CPA's enumerated privacy notice content requirements and analyze whether a CCPA-compliant privacy notice would suffice to meet such requirements.

1. **"[A] comprehensive description of the controller's online and offline personal data processing purposes, including, but not limited to the following, linked in a way that gives consumers a meaningful understanding of how each category of personal data will be used when they provide that personal data to the controller for a specified purpose"** – This effectively requires listing the processing purposes that apply to each category of personal data/personal information.
   - This includes, among other things reflective of the CCPA, "[w]hether the Personal Data provided for a specific purpose will be sold or used for Targeted Advertising or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer[,]" which is likely not covered by California notices.
   - It should be noted that Colorado does not require the same level of detail by subcategory of sensitive data that the CCPA required as of January 1. However, many businesses decided to delay adding that detail until July 1 in order to better diligence practices and to also see how competitors addressed the disclosures.
2. **If a controller's processing activity involves the processing of personal data for the purpose of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, disclosures are required by Section 9.03 of the CPA rules** – This likely is not covered by most CCPA notices.
   - Under the CPA, there are very detailed and voluminous – seven in total – disclosure requirements for controllers that process personal data for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, including (1) the decisions subject to profiling; (2) the categories of personal data that were or will be processed as part of the profiling in furtherance of decisions that produce legal or other similarly significant effects; (3) a non-technical, plain language explanation of the logic used in the profiling process; (4) a non-technical, plain language explanation of how profiling is used in the decision-making process, including the role of any human involvement; (5) if the system has been evaluated for accuracy, fairness or bias, including the impact of the use of sensitive data, and the outcome of any such evaluation; (6) the benefits and potential consequences of the decision based on the profiling; and (7) information about how a consumer may exercise the right to opt out of the processing of personal data concerning the consumer for profiling in furtherance of decisions that produce legal or other similarly significant effects.
   - As of now, without CPRA regulations on profiling and automated decision-making, there are not (yet) specific privacy policy disclosures required in relation to such concepts.

3. **A list of the data rights available** – This will be met by existing disclosures, assuming that the privacy notice already addresses the new CPRA and VCDPA rights that became effective on January 1, 2023.

4. **A description of the methods through which a consumer may submit requests to exercise data rights, including, effective as of July 1, 2024, an explanation of how requests to opt out using universal opt-out mechanisms will be processed** – Meeting the CPRA's requirements in this regard that apply to OOPS likely will suffice. CPRA rights, especially regarding sensitive data, differ from the other states (opt-out rather than opt-in).

5. **Rights of appeal** – Disclosures regarding how consumers can appeal a controller's decision relating to consumer rights requests, as well as how to contact the Colorado AG if the consumer's appeal is defined. Under California law, consumers do not have the right to appeal, but, if an appeal right is offered, it must be explained. Virginia and Connecticut have appeals provisions.

Loyalty and Incentive Programs

Due to material differences between the CCPA and CPA's definitions and requirements in this area, many businesses complying with the CCPA's financial incentive and nondiscrimination requirements will have to shift their approach in order to also comply with Colorado law. In some instances, businesses may be forced to choose between taking a completely divergent approach as to Coloradans – such as applying a different user experience (UX) – or to applying certain of Colorado's more strict requirements to all users. California has concepts of financial incentives (FI) and price or service differences (POSD), and permits price or service discrimination based on exercise or nonexercise of CCPA rights only if the value of the benefit is reasonably related to the value of the data, and sets forth acceptable data valuation methodologies. Colorado similarly prohibits rights-based discrimination:

"Based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service.

However, it excepts bona fide loyalty programs (BFLP), defined as "[a] loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program, such that the primary purpose of Processing Personal Data through the program is solely to provide Bona Fide Loyalty Program Benefits to participating Consumers." "Bona Fide Loyalty Program Benefit" means "an offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program. Such benefits may be provided directly by a Controller or through a Bona Fide Loyalty Program Partner." "Bona Fide Loyalty Program Partner" means "a Third Party that provides Bona Fide Loyalty Program Benefits to Consumers through a Controller's Bona Fide Loyalty Program, either alone or in partnership with the Controller."

A number of regulatory requirements apply to BLFPs, which do not apply to California FIs or POSDs:

- **Secondary use for sale or targeted advertising** – In Colorado, use of personal data collected in relation to a BFLP for sale or targeted advertising is a per se secondary use for which separate consent is necessary, and explicitly cannot be required for BFLP participation. This is a significant divergence from California's requirements, and prevailing practice in the US, that will require businesses to implement GDPR-like consent to utilize data collected in relation to a BFLP for targeted advertising (such as for email addresses for custom audience campaigns) or sale. There is an exception to this rule if the sale or targeted advertising is related to sharing with a "bona fide loyalty program partner."
- Colorado's BFLP disclosure must include the following information that is not required to be in a CCPA FI notice:
  - The categories of personal data or sensitive data collected through the BFLP that will be sold or processed for targeted advertising, if any.
  - Categories of third parties that will receive the consumer's personal data and sensitive data, provided in the level of detail described in the CPA rules, including whether personal data will be provided to data brokers.
  - A list of any BFLP partners, and the BFLP benefits provided by each partner
  - If a controller claims that a consumer's decision to delete personal data makes it impossible to provide a BFLP benefit, then the controller must provide an explanation of why the deletion of personal data makes it impossible to provide a bona fide loyalty program benefit.
  - If a controller claims that a consumer's sensitive data is required for a BFLP benefit, then the controller must provide an explanation of why the sensitive data is required for a BFLP Benefit.

In summary, complying with both the CCPA and the CPA in respect of loyalty programs may require significant changes for some businesses currently complying with only the CCPA.

Opt-out Rights – Sale, Sharing and Targeted Advertising

The CCPA and CPA define "sale" similarly in that they do not require exchange of monetary consideration for a sale to have taken place. However, one significant difference between the CCPA and CPA (and the other non-California state laws) relates to their targeted advertising opt-outs. The CCPA's opt-out right extends to "sharing" personal information with third parties for purposes of cross-context behavioral advertising. The CPA's opt-out right, on the other hand, extends more broadly to "processing of personal data… for purposes of targeted advertising." Therefore, in response to a targeted advertising opt-out, controllers must cease not only disclosures of personal data to third parties for such purposes, but also internal processing for such purposes. Virginia and Connecticut align with Colorado in this regard.

Sensitive Data – Opt-out vs. Opt-in

The CPA, along with the VCDPA and CTDPA, requires GDPR-like consent for any processing of sensitive data, while the CCPA has the "right to limit," which is akin to a right to opt out of the processing of use and disclosure beyond certain limited purposes that are enumerated in the regulations. While the CPA and the other non-California state laws do not address it explicitly, those laws also require controllers to allow, and heed, revocation of consent by a consumer. The rights, however, are qualified. Businesses should closely consider the broad exemptions and exceptions in those laws as they operationalize consent (and revocation of consent) with respect to sensitive data. For example, there is a broad exemption in the CPA and some of the other non-California state laws that would permit a controller to continue processing sensitive data following the revocation of consent to provide a product or service requested by the consumer.

The definition of sensitive data in the CPA (and the other non-California states) differs materially in a handful of respects from the CCPA's definition of sensitive personal information (PI). For example:

- Precise geolocation data is sensitive PI under the CCPA and sensitive data under the VCDPA, but it is not sensitive data under the CPA nor the CTDPA. Like many other material differences in the various state laws, businesses must decide to set high-watermark standards, or apply rights differently depending upon state.
- The scope of health data categorized as sensitive PI/data varies to some degree between the laws as well. For example, the CCPA defines the term as PI "concerning a consumer's health," while the CPA and CTDPA refers to data "revealing … a mental or physical health condition or diagnosis"; the VCDPA refers to data "revealing mental or physical health diagnosis" (much narrower); and the UCPA refers to data that reveals "information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional."

The CPA's rules devote a significant amount of time to business's obligations with respect to "sensitive data inferences," defined as "inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status." Also, under the CPA, businesses may be exempt from obtaining consent for processing sensitive data inferences if they meet certain criteria that seem difficult to meet for most industries. Such criteria include deleting the inferences within 24 hours, and not transferring, selling, or sharing the inferences to processors, affiliates or third parties.

Global Privacy Control/Opt-out Preference Signal/Universal Opt-out Mechanism

The CPRA and CPA are generally aligned in respect of how businesses must address global privacy control (GPC) signals, which are signals that communicate a consumer's choice to opt out of the sale, sharing, and/or processing of PI for targeted advertising (as those concepts are set forth in their respective laws), and, in California, limit sensitive personal information processing. As if we do not have enough acronyms, however, the two laws do differ in terms of GPC nomenclature – the CPRA uses "opt-out preference signals" (OOPS), while the CPA's version is referred to as "Universal Opt-Out Mechanisms" or (UOOMs). Second, the CPRA statutory updates regarding OOPS became effective on January 1, while the regulations on OOPS became effective as of March 29, 2023, and will be enforceable on July 1. Colorado's UOOM requirements do not take effect until July 1, 2024. Connecticut's law has opt-out preference signal requirements as well, but they do not go into effect until January 2025.

Scope of application – Both the CPRA and CPA require businesses to apply GPC signals to both "online" data, like cookie IDs and IP addresses collected on or about a browser or device, and, if known, any consumer profile or account information associated with the browser or device ("offline data"). For example, the CPRA provides specific examples in Section 7025(c)(7) that require businesses to apply GPC to offline data if a consumer has logged in to their account with the business while the GPC signal is activated on the business's website, and to apply a GPC signal to online data on a different device/browser after the consumer has logged in on that different device/browser (the latter likely requiring integrations between the business's internal systems and its consent management platforms that do not generally exist). It is unclear whether the CPA's "if known" scope of application (see Rule 5.08(A)(1)) would extend to these examples provided in the CPRA. The CPRA's requirements certainly provide challenges for business' compliance due to technical limitations of many companies that do not in fact tie online and offline data together in their systems, and in view of technical limitations of prevailing consent management platforms that do not provide these types of capabilities in their standard offerings.

Consent after GPC opt-out – Each law also explicitly states that businesses shall not interpret the absence of a previously utilized GPC signal for a particular consumer as consent to opt back in.

Conflicts with consumers' other choices – The CPA's rules and CPRA's regs would both seemingly permit a business to present, to a new and/or unknown website visitor, a pop-up or interstitial in response to a GPC signal (e.g., similar to what some online publishers do in response to a pop-up blocker), asking for consent to sale and sharing, and processing for targeted advertising. As to known consumers, however, the CPRA regulations provide specific requirement that need to be addressed.

Description of GPC practices in privacy policy – Both the CPRA and CPA require businesses to explain how GPC signals will be processed. The CPA is more general, while the CPRA provides that this means businesses must provide a description of "whether the signal applies to the device, browser, consumer account and/or offline sales, and in what circumstances[,]" and if it addresses GPC in a "frictionless" manner or not. Complying with the CPRA's requirements would appear to suffice for Colorado's disclosure requirements.

Authentication – For businesses that are applying or plan to apply GPC/OOPS/UOOM signals to state residents based on the location using features of their consent management platforms, that would appear to be a reasonable practice under both the CCPA and CPA.

Display re: honoring GPC signal – Both states make it optional for businesses to display whether they have honored a GPC signal.

List of approved UOOMs – The CPA rules provide that the Colorado Department of Law must maintain a public list of UOOMs that have been recognized to meet the standards of the CPA, and the initial list must be released no later than January 1, 2024, and thereafter updated periodically.

We have already seen California enforcement actions, including one with a significant civil penalty settlement, related to failure to apply GPC under the less complex CCPA mandate. The more fulsome CPA and CPRA requirements are likely to be an area of enforcement, especially since failure to comply is easily discernable with simple website analysis tools.

Profiling and Automated Decision-making

At least as it stands while we wait for the CPPA to promulgate regs on these issues, the CPA provides for very detailed and prescriptive rules and requirements on the issue of profiling and automated decision-making (ADM). For a detailed look at ADM and profiling issues under GDPR, and how the CPPA may be approaching regulations, please see our post on that topic.

In particular, the CPA rules set forth a detailed compliance framework for specific requirements for profiling, including specific requirements pertaining to consent, transparency and data protection assessment. The CPA affords consumers the right to opt out of profiling that is either "solely automated" or "human reviewed" automated processing, but permits controllers to decline honoring opt-out requests where the profiling is properly characterized as "human involved" automated processing.

While it is yet to be seen what will be the full extent of requirements and limitations imposed on profiling and ADM technology by the CPPA under the CPRA, it is reasonable to posit that there may be substantial nuances between its requirements and those of the CPA that companies will need to understand to ensure compliance with both laws.

Data Practice Assessments

Referred to as "data protection assessments" under the CPA and "risk assessments" under the CCPA, data due diligence/privacy-by-design assessments are another area where the CPA rules set forth significant detail and on which we are awaiting California risk assessment regulations from the CPPA, including regarding annual security audits and whether assessments will be subject to regulatory filing.

The CPA sets forth extensive, prescriptive rules and requirements on performing assessments, which entail (among others) the following:

- Assessments must involve key stakeholders and all relevant internal personnel from across all lines of business and operations, as well as any external entities whose involvement is necessary to evaluate applicable data protection risks presented by the business's processing activities.
- Assessments must evaluate, at a minimum, 13 discrete issues that pertain to the nature, purpose, scope, and risks associated with the processing of personal data.
- Controllers must update their assessments whenever risk levels associated with processing activity materially changes.

As noted above, the first difference relates to fact that the CPA requires assessments to be conducted prior to any sensitive data processing activities, while the CPRA contains no similar requirement, instead punting all risk assessment details to the CPPA for rule making. In addition, the CPA also requires assessments to be performed under a range of other circumstances beyond sensitive data processing, including profiling, processing personal data for the purpose of targeted advertising, the sale of personal data and other high-risk activities. More than that, the CPA rules set forth extensive prescriptive content requirements for assessments, as well as fairly detailed timing requirements, such as mandatory reviewing and updating of assessments "as often as appropriate considering the type, amount and sensitivity of the data at issue."

Further, the Colorado attorney general (AG) maintains the authority to request that a controller provide the AG with a copy of its assessments, subject to certain confidentiality protections.

Conversely, the CPPA has yet to issue its final regulations on assessment requirements pertaining to the CPRA, giving it broad authority, including to require filing of assessments with the CPPA. The CPPA has stated that its ongoing rulemaking is looking at the CPA rules and guidance from the European Data Protection Board (EDPB) in crafting California's assessment requirements. Technically, assessments are currently required under the CPRA, and, as that becomes enforceable on July 1, there are no standards to apply. Virginia has required assessments since January 1, 2023, and Connecticut will do so as of July 1. However, the Virginia and Connecticut laws lack any details on how they should be conducted. Unless and until the CPPA sets differing requirements, the CPA requirements should satisfy the other states, though adding EDPB recommendations may be prudent.

For additional insights, strategic advice and recommended best practices for complying with new consumer privacy laws' assessment requirements, be sure to check out Privacy World's detailed assessment guidance. We have developed CPA and EDPB assessment guidance and templates, which are compatible with OneTrust and other information governance platforms.

Data Minimization

In addition, the CCPA and CPA also differ on the nature and extent of data minimization obligations imposed on businesses.

In this respect, both the CCPA and CPA have provisions that require companies to implement data minimization as part of their data processing activities and compliance programs. Importantly, however, the CPA contains additional, focused rules regarding the retention of biometric identifiers, photographs, and audio or voice recordings – requiring controllers to review, at least annually, whether continued retention and storage of these types of data are necessary, adequate or relevant for the controller's stated processing purpose. California requires disclosure of retention periods, by data category, in the notice at collection, which could be given by reference to a retention statement in the privacy notice. The CPA rules also have detailed requirements regarding so-called "secondary uses," most notably requiring separate, express consent.

HR and B-to-B Data

Because HR data and data reflecting B-to-B contacts and communications came into full scope under the CPRA on January 1, 2023, it is necessary to expand the scope of your privacy program to account for those data sets. HR data is largely exempt under the VCDPA, UCPA and CTPA, and employment records are exempt under the CPA. The VCDPA exempts B-to-B contacts and communications, and Virginia, Colorado, Utah and Connecticut only treat data subjects as consumers when they act in an individual or household capacity, effectively exempting both HR and B-to-B data. It will be a time-consuming effort that will require adaptation of existing policies and procedures, particularly with regard to personnel data, to address the expanded scope in California. Also, more rigor should be applied in responding to HR data subject access requests, as they are likely made in anticipation of litigation, and to take into account the rights of other data subjects, trade secrets and privileged information that are more likely to be implicated than is the case with traditional consumer data. Privacy World has more information on how to prepare for HR requests.

Takeaways and Recommendations

The CPRA, CPA and CTDPA join the VCDPA as fully enforceable on July 1, 2023. The CPRA rulemaking is still ongoing, with the last set of rules promulgated on March 29, with more to come later this year. The CPA rules were finalized on March 15. Businesses that delayed addressing some or all of their new 2023 obligations until July 1 need to turn back to that now if they have not already done so. Those that updated their notice and practices in January 2023 with the aim to be compliant throughout 2023 almost certainly need to address the regulations that have since been developed and should revisit their compliance posture accordingly. For more information, contact the authors or your relationship partner at the firm.

Contacts

Kyle R. Fath
Partner, Los Angeles
T +1 213 689 6582
E kyle.fath@squirepb.com

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

David J. Oberly
Senior Associate, Cincinnati
T +1 513 361 1252
E david.oberly@squirepb.com