ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

NOVEMBER 4, 2020

Planning for the California Privacy Rights Act

***by* Michael Young *and* Jim Harvey**

Yesterday, California voters approved a ballot initiative called the California Privacy Rights Act of 2020 (CPRA). Arguably the most comprehensive U.S. state privacy law, the law establishes a new enforcement and regulatory authority and will result in further expansive privacy regulation.

Essential Steps to Compliance

While there is no "one size fits all" compliance plan, there are steps businesses handling information related to California residents, households, or devices can take to help ensure compliance.

1. **Expressly Confirm Data Retention Practices.** The CPRA requires that businesses may only retain personal information as "necessary and proportionate" for processing. Businesses must identify and provide notice of the specific retention periods for the categories of personal information collected. Businesses should systematically review data retention practices for personal information and consider measures to minimize that retention to ensure compliance with these new standards. For large or complex enterprises that do not currently maintain an active data retention program, this review will likely require a significant effort.

2. **Review Use of Sensitive Information.** The CPRA defines a new category of personal information, "sensitive personal information," including information such as Social Security number, financial account, precise geolocation data, racial and ethnic orientation, labor union affiliation, and genetic, biometric, and health data. Businesses must either restrict their use of sensitive personal information or else provide consumers notice of their right to request such processing restrictions. Permitted use of sensitive personal information includes use as "necessary to perform the services or provide the goods," as "reasonably expected by an average consumer who requests such goods or services," and for certain limited additional purposes, including using information to ensure security and integrity, short-term transient use, and maintaining service quality. Businesses will need to catalog, evaluate, and potentially modify their use of sensitive personal information to ensure compliance with these new standards.

3. **Review and Revise Initial Notices.** The CPRA expands notice obligations "at or before the point of collection" of personal information. Those initial notices must now describe the categories of sensitive personal information collected, the purpose for such collection, and whether such information is sold or shared. In addition, initial notices must identify retention periods for each category of information the business collects. Businesses will need to review and update their initial notices to reflect this new content mandated under the CPRA.

4. **Update Homepage Links.** Businesses that use sensitive personal information beyond the narrow purposes expressly permitted by the CPRA must include a link on their homepage offering consumers a right to limit the use of sensitive personal information.[1] In addition, the CPRA changes the wording for "do not sell" links to the phrase "Do Not Sell *or Share* My Personal Information." In light of these requirements, businesses must update their homepages to: (1) disclose the new right to limit processing of sensitive personal information; and (2) update the existing wording of "do not sell" links. Alternatively, businesses may choose to provide a "single, clearly-labeled link" that "easily allows" these consumer choices from the homepage, though the statute does not clearly identify what wording might satisfy the requirement to be "clearly-labeled" and "easily allow" consumer choice.

5. **Review Data Sharing with (Digital) Marketing Providers.** The CPRA expands existing "do not sell" rights to provide consumers a new right to opt out of having their personal information shared with third parties for cross-contextual behavioral advertising.[2] As a result, businesses will need to identify marketing providers that personal information may be shared with (even if such sharing is not technically a "sale") and identify ways to restrict the provision of personal information to such providers in response to the new consumer right. In addition, the CPRA will likely challenge the ability of some digital advertising networks to characterize themselves as "service providers" acting on behalf of publishers or advertisers. Digital advertising relationships between advertisers, publishers, and advertising networks need to be examined to ensure accurate characterization of each party's role (and appropriate allocations of responsibility).

6. **Update (or Create) Rights-Response Procedures.** The CPRA also expands data deletion rights and provides consumers with a new right of data correction. Pursuant to the new correction right, businesses must "use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer." The CPRA also expands data deletion obligations throughout the supply chain in response to a verifiable consumer deletion request: (1) the *business* that interacts with the consumer must delete personal information and direct entities the information has been shared with to delete the information; (2) the business's *service providers* must delete personal information; and (3) those

---

1 Note that "homepage" is a defined term under the CPRA that means an "introductory page of an internet website" but also any webpage "where personal information is collected" and, in the case of a mobile application, the application's download page or a link from within the application.

2 "Cross-context behavioral advertising" means:

> The targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

service providers must direct *their suppliers* in turn to delete such information. Businesses will need to comprehensively review and update rights-response procedures to adapt to these new consumer opt-out rights. B2B service providers will also need to create new processes to operationalize the data deletion obligations the CPRA now imposes on them.

7. **Update Section 130 Website Notice.** The CPRA also requires businesses to explain consumer rights within their website privacy notice in addition to the initial notice and homepage links. These notices will need to reflect the new CPRA right of correction. Consumers now also have the express right to understand the purposes for which the business has disclosed information for cross-context behavioral advertising and the categories of third parties such disclosures were made to. Thus, existing online website privacy notices (or related disclosures of California privacy rights) must be reviewed and updated to reflect rights under the CPRA.

8. **Update (Customer/Vendor) Contracts.** The CPRA requires that businesses include specific terms in contracts with their vendors that process personal information of California residents, including terms (1) requiring compliance with law; (2) enabling the business to "take reasonable and appropriate steps" to ensure proper use of such information (including a right to stop processing); and (3) requiring the service provider to provide notice if it determines it cannot meet obligations under the CPRA. In addition, contracts with vendors that act as service providers must prohibit the vendor from combining personal information received from the business with other personal information. ("Service provider" is a significant legal designation under the CPRA that permits businesses to avoid regulated sales of data.) Businesses should update their vendor contracts to reflect these requirements. Businesses that provide services to other businesses may want to preempt customer contractual demands by proposing their own terms for customers, designed to help satisfy the CPRA requirement.

9. **"Reasonable" Information Security.** While implicit in the current California Consumer Privacy Act, the CPRA *expressly* requires businesses to "implement reasonable security procedures and practices" to "protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." Businesses should maintain a comprehensive information security program that protects personal information of California consumers, households, or devices.[3]

Effective Date and Impact on Current Law

The CPRA amends and extends the California Consumer Privacy Act (CCPA), which itself only took effect on January 1, 2020. The previously enacted (and currently effective) CCPA remains in effect until replaced by the additional or amending provisions of the CPRA.[4] Most provisions of the CPRA that impose direct requirements

---

[3] While the CPRA does not itself provide much definition for what "reasonable" information security requires, note that the California attorney general previously identified 20 controls from the Center for Internet Security's Critical Security Controls as an appropriate "minimum" level of information security: "The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." In addition, businesses should consider how the concept of "reasonable" security may be informed in their particular contexts by evolving regulatory and commercial practices.

[4] However, note that the CPRA provides that "upon passage" it prevails over any "conflicting" legislation enacted since January 1, 2020. It is unclear what (if any) particular provisions of California law could be impacted by this provision.

on business will take effect on January 1, 2023, although provisions relating to the establishment of a new privacy regulator will take effect much more quickly.

Most businesses subject to the current CCPA will remain subject to the CPRA. In some cases, the CPRA expands the scope of regulated "businesses" to include (1) certain joint ventures that may have been previously unregulated (particularly, joint ventures "composed of businesses in which each business has at least a 40 percent interest"); and (2) businesses that voluntarily submit to the CPRA through a certification to the newly created regulator, the California Privacy Protection Agency. Small businesses that annually buy, sell, or share the personal information of fewer than 100,000 California consumers or households may not qualify as regulated businesses under the CPRA unless meeting some further condition, such as voluntary certification or ownership by a larger, regulated business.

New California Enforcement Authority: The California Privacy Protection Agency

In addition to imposing obligations on businesses directly, the CPRA also creates a new privacy regulator and enforcement authority, the California Privacy Protection Agency (CPPA). Provisions creating the CPPA have quick effect (just five days) after the California secretary of state certifies the vote approving the ballot measure. Under these provisions, $5 million of funding is immediately allocated within the current 2020–2021 fiscal year for the establishment of the new privacy regulator, with $10 million a year guaranteed in subsequent years.

Once formed, the CPPA will face the immediately effective mandate to "administer, implement, and enforce through administrative actions" provisions of the California code containing the existing CCPA, as amended by the CPRA. Notwithstanding this immediately effective general mandate, some critical enforcement procedures and powers of the CPPA will not be effective until January 1, 2023, such as the provision providing the CPPA with express authority to conduct independent investigations. It is unclear how the CPPA will interpret its own enforcement authority and power before January 1, 2023 in light of these provisions. Until clarified further by the CPPA itself, businesses could technically face enforcement by the new agency as soon as the agency is operational.

In addition to creating the CPPA, the CPRA in general does not limit the authority of the state attorney general to continue enforcing California privacy law. In fact, parts of the new law contemplate that the attorney general and the CPPA will each have independent authority to separately enforce California privacy laws.[5]

Additional Regulations

In addition to statutory requirements reflected directly in the text, the CPRA requires the adoption of expansive new regulations that will further impact businesses. The CPPA will assume regulatory authority from the attorney general on the earlier of July 1, 2021 or six months after it provides notice to the attorney general that it is prepared to begin rulemaking. Regulations under the CPRA must be adopted by July 1, 2022. However, it is unclear whether these regulations will be effective on that date (or shortly thereafter) or

---

[5] Provisions such as 1798.199.90(c)(d) and 1798.199.100 aim to establish principles and procedures governing potential enforcement conflicts between the attorney general and the CPPA. The potential for such enforcement conflicts appears to underline the intent of the law that both agencies will have enforcement authority.

on January 1, 2023, when most CPRA provisions become effective. (Of course, it would make little sense for regulations to become effective before the effectiveness of the statutory provisions they aim to implement.)

In any case, the CPRA mandates the adoption of broad regulations in particular areas, including:

- Prohibiting "deceptive or harassing conduct," and requiring additional consumer notice explaining how the consumer may be impacted by exercising opt-out rights.
- Handling consumer data correction requests.
- Restricting service providers' permitted use and combination of personal information obtained from different sources.
- Defining "intentional interactions" with consumers (a critical concept for businesses that may rely on consumer authorizations or direction to avoid a technical data sale under the law).
- Requiring annual "cybersecurity audits" and submission of "risk assessments" to the CPPA when information processing poses a "significant risk" to consumers' privacy or security (noting that the quoted phrases are not defined in the statute).
- Empowering the CPPA to conduct audits without a court order, warrant, or subpoena.
- Further restricting the use of sensitive personal information.
- Expanding the CPPA to insurance companies.[6]

Until regulations are finalized, it will of course be difficult for businesses to plan effectively in these areas. Nevertheless, the potential for comprehensive additional regulation (potentially effective on short notice) underlines the need for businesses to maintain robust compliance and data governance practices generally.

---

[6] The CPPA is required to study whether existing insurance regulations provide greater protections to consumers than the CPRA. After completing that review, the CPPA "shall adopt" a regulation that applies provisions of the CPRA to insurance companies, with the goal of imposing on insurers any CPRA provisions that are determined to be "more protective" of consumers than existing insurance law.

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Elizabeth Broadway Brown
404.881.4688
liz.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Kimberly K. Chemerinsky
213.576.1079
kim.chemerinsky@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Maki DePalo
404.881.4280
maki.depalo@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Wim Nauwelaerts
+32.2.550.3709
202.239.3709
wim.nauwelaerts@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333