SULLIVAN & CROMWELL LLP

S&C memo

March 16, 2023

New California Privacy Requirements Effective in 2023

California Privacy Rights Act of 2020 Enters Into Force

SUMMARY

The amendments to the California Consumer Privacy Act ("CCPA") enacted pursuant to the California Privacy Rights Act ("CPRA"), a statewide ballot initiative passed in November 2020 by California voters, became effective January 1, 2023.[1] The CPRA establishes two new consumer privacy rights, imposes additional restrictions on how businesses are permitted to share personal information with service providers, contractors and third parties, expands the scope of businesses subject to the CCPA (imposing obligations on businesses that "share" personal information) and establishes the California Privacy Protection Agency ("CPPA") to implement and enforce the CCPA.

Although a majority of the CPRA's provisions entered into force on January 1, 2023, many of the new obligations imposed by the CPRA include a 12-month look-back that give consumers the right to request that businesses provide applicable information from as early as January 2022. Additionally, the CPPA announced on February 3, 2023 that it approved certain regulations required by the CPRA, which will become effective in April 2023. Although enforcement of the new obligations imposed on businesses by the CPRA will not begin until July 1, 2023, the CCPA's pre-existing provisions remain in effect and enforceable until that date.[2] Businesses should be mindful of their new obligations under the CCPA and how their existing obligations may apply to employment and business-to-business related data that are no longer subject to exemptions, especially in light of the California Attorney General's first enforcement action brought under the CCPA in 2022 against Sephora and its subsequent settlement, as well as the recent enforcement case examples published by the California Attorney General.

In addition to the CPRA, four other state privacy laws are becoming effective in 2023: the Colorado Privacy Act,[3] the Connecticut Data Privacy Act,[4] the Utah Consumer Privacy Act,[5] and the Virginia Consumer Data

Protection Act.[6] In light of these new laws, businesses will need to review and update their privacy programs, including their website and employee privacy notices, data subject rights procedures, data processing agreements, and data security policies and procedures.

BACKGROUND

The CCPA became the nation's first statewide comprehensive privacy law in June 2018. Unsatisfied with certain aspects of the CCPA, Alastair Mactaggart, a driving force behind the CCPA's enactment, proposed a new statewide ballot initiative—the CPRA.[7] The CPRA passed comfortably and the CPPA was then established to implement and enforce the CCPA. On April 21, 2022, rulemaking authority under the CCPA formally transferred from the California Attorney General to the CPPA, though the Attorney General retains civil enforcement authority.[8]

In May 2022, the CPPA released its first draft of proposed regulations governing compliance with the CCPA as amended by the CPRA.[9] On July 8, 2022, the CPPA issued a Notice of Proposed Action, triggering a 45-day comment period on the draft of proposed regulations[10] and, after releasing two subsequent drafts and holding three days of board meetings, the CPPA published a final version of the regulations on February 3, 2023 (the "CPRA Regulations"), which are expected to become effective in April 2023.[11] The CPRA Regulations do not address the entirety of the regulations required to be enacted pursuant to the CPRA, however, and as a result the CPPA will need to address the CPRA's requirements for risk assessments, cybersecurity audits, and automated decision-making in future rulemakings. On February 10, 2023, the CPPA issued an invitation for preliminary comments on proposed rulemaking for these additional topics, with comments due on March 27, 2023. Given the impact of the delayed regulations on California businesses, the CPPA has indicated that it may consider the amount of time between the effective date of the CCPA and the CPRA Regulations and alleged violations thereof, as well as a business's' good-faith efforts to comply, when enforcing the CCPA.

I. KEY UPDATES TO THE CCPA BY THE CPRA

A. INCLUSION OF EMPLOYMENT AND B2B DATA

Previously under the CCPA, businesses were exempt from complying with certain obligations with respect to personal information ("PI") collected in the employment context or in the context of a business "providing or receiving a product or service to or from" another business ("B2B").[12] However, these exemptions expired on January 1, 2023 and the CPRA did not further extend such exemptions.

The expanded applicability of the CCPA to PI collected in the employment or B2B contexts is expected to widely impact many businesses who satisfy the revenue threshold and have California employees, contractors, job applicants, vendors or business contacts from whom they collect PI. Most notably, these

businesses are required to respond to requests from the employees, contractors, job applicants, vendors or business contacts who exercise their rights with respect to their PI.

B. AGREEMENTS WITH SERVICE PROVIDERS OR CONTRACTORS

The CPRA Regulations set forth specific requirements for agreements between businesses and service providers or contractors to which the businesses disclose PI. Although the CPRA Regulations do not provide model clauses, they do specify that these contracts must:

- Prohibit the service provider or contractor from selling or sharing PI;
- Identify the specific Business Purpose(s) for which the service provider or contractor is processing PI and specify that the business is disclosing the PI to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract;
- Prohibit the service provider or contractor from retaining, using, or disclosing the PI for any purposes other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA or its implementing regulations;
- Prohibit the service provider or contractor from retaining, using, or disclosing the PI for any commercial purpose other than the Business Purpose(s) specified in the contract, unless expressly permitted by the CCPA or its implementing regulations;
- Prohibit the service provider or contractor from retaining, using, or disclosing the PI outside its direct business relationship with the business, unless expressly permitted by the CCPA or its implementing regulations;
- Require the service provider or contractor to comply with all applicable sections of the CCPA and the accompanied regulations, including providing the same level of privacy protection as required of businesses;
- Grant the businesses the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the PI in a manner consistent with the business's obligations under the CCPA and its implementing regulations;
- Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and its implementing regulations;
- Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of PI; and
- Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.[13]

Although the CPRA Regulations do not hold businesses liable for noncompliance by downstream service providers or contractors, businesses are required to include terms in contracts with such service providers or contracts granting the business the right to take reasonable and appropriate steps to ensure compliance by the service providers or contractors with the CCPA.[14] This may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.[15] Because the CPRA Regulations require a service provider to notify the business if it can no longer meet its CCPA obligations, the contract

should also grant the business rights, upon notice, to take reasonable and appropriate steps to remediate unauthorized use of PI, which may include additional attestation or documentation from a service provider verifying deletion of PI.[16]

Further, if a service provider or contractor subcontracts with another person in providing services to the business, the service provider or contractor is required to pass the foregoing obligations through to such subcontractor.[17]

C. NEW REQUIREMENTS FOR "SHARING" PERSONAL INFORMATION

The CPRA updates the scope of businesses subject to the CCPA to include organizations that do business in California and "share" the PI of 100,000 or more consumers or households or derive 50% or more of their annual revenues from "sharing" consumers' PI.[18] "Sharing" is defined under the CPRA as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to a third party for cross-contextual behavioral advertising, whether or not for monetary or other valuable consideration, including when no money is exchanged.[19]

Previously under the CCPA, "sharing" was not a defined term and the CCPA focused on businesses in California that "sold" PI. Under the CCPA, a "sale" of PI is defined as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means PI to another business or third party for monetary or other valuable consideration.[20] The key difference between the definitions of "sale" and "sharing" is the consideration requirement. As a practical matter, although sharing PI for cross-contextual behavioral advertising only becomes a sale if the consideration requirement is satisfied, the CCPA now treats the two activities similarly. For example, companies that engage in either activity must place a "Do Not Sell or Share My Personal Information" link on their website.[21]

D. EXPANDED CATEGORIES OF RIGHTS

The CCPA previously enumerated five categories of data privacy rights granted to consumers with respect to their PI: (1) the "right to know"; (2) the "right to access"; (3) the "right to deletion"; (4) the "right to opt out"; and (5) the "right to equal service."[22]

The CPRA amends the CCPA by creating two additional rights: (1) the right to correct inaccurate PI; and (2) the right to limit use and disclosure of sensitive PI.

1. Right to Correct Inaccurate Personal Information

Under the CCPA as amended by the CPRA, businesses are required to (i) disclose to consumers information about their right to correct in the business' privacy policy; (ii) provide consumers with a means

to request a correction; and (iii) use "commercially reasonable efforts" to correct inaccurate PI upon receiving such a request from a verifiable consumer.[23]

2. Right to Limit Use and Disclosure of Sensitive Personal Information

Sensitive Personal Information ("SPI") is a subset of PI newly defined by the CPRA. The definition of SPI includes data elements included in California's breach notification law as well as those that are considered "special categories" of personal data under other privacy and data protection laws such as the European Union's General Data Protection Regulation ("GDPR"). SPI includes PI that reveals: (1) a consumer's Social Security, driver's license, state identification card, or passport number; (2) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (3) a consumer's precise geolocation; (4) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (5) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; or (6) a consumer's genetic data.[24] SPI also includes (1) the processing of biometric information for the purpose of uniquely identifying a consumer; (2) PI collected and analyzed concerning a consumer's health; and (3) PI collected and analyzed concerning a consumer's sex life or sexual orientation.[25]

The CCPA as amended by the CPRA requires businesses to include separate disclosures for the categories of SPI collected, the purpose of collection, and whether such SPI is sold or shared.[26] The CCPA now also provide consumers a new right to limit use and disclosure of SPI. A business must offer that right unless the collection, use or disclosure of SPI is reasonably necessary and proportionate:

- To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services;
- To prevent, detect, and investigate security incidents that compromise PI;
- To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions;
- To ensure the physical safety of natural persons;
- For short-term and transient use, provided that the PI is not disclosed to another third party and is not used for target advertising outside the consumer's current interaction with the business;
- To perform services on behalf of the business;
- To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business; or
- To collect or process SPI where such collection or processing is not for the purpose of inferring characteristics about a consumer.[27]

E. OTHER OBLIGATIONS OF BUSINESSES, SERVICE PROVIDERS AND CONTRACTORS

1. Audits and Risk Assessments

The CCPA as amended by the CPRA requires businesses to perform cybersecurity audits on an annual basis if the business's processing of PI presents a significant risk to consumers' privacy or security. The CPRA Regulations do not include specific provisions spelling out the parameters of an annual cybersecurity audit, but the CPRA suggests that, in determining whether the processing may result in significant risk to the security of PI, both (1) the size and complexity of the business and (2) the nature and scope of processing activities should be considered.[28]

The CCPA now also requires businesses to submit to the CPPA regular risk assessments with respect to their processing of PI that presents significant risk to consumers' privacy or security, including whether the processing involves SPI, and identifying and weighing the benefits resulting from such processing against the potential risks to the rights of the consumer associated with that processing. The goal of this requirement is to restrict or prohibit the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing.[29]

In its December 2022 meeting, the CPPA issued sample questions for a preliminary rulemaking in 2023 that address risk assessments, cybersecurity audits and automated decision-making. On February 10, 2023, the CPPA issued an invitation for comments on the topics of cybersecurity audits, risk assessments, and automated decision-making, which have not been addressed in the CPRA Regulations.[30]

2. Data Minimization Obligation

Under the CCPA as amended by the CPRA, businesses are now required to comply with the principle of data minimization. Similar to the GDPR,[31] businesses collecting and storing PI that does not serve a business use will be subject to a penalty. A business's collection, use, retention and sharing of PI must be reasonably necessary and proportionate to either the purposes for which it was collected or another disclosed purpose compatible with the context in which the PI was collected.[32]

3. Opt-Out Preference Signals

An "opt-out preference signal" is a signal sent by a platform, technology, or mechanism, on behalf of the consumer, that clearly communicates the consumer's choice to opt out of the sale and sharing of PI.[33] One example is Global Privacy Control, a technical specification for transmitting universal opt-out signals. Through browser settings or extensions, Global Privacy Control signals allow consumers to make an opt-out request that applies to all websites able to process the signal rather than the consumer needing to make an opt-out request on each website.[34] Under the CPRA Regulations, businesses are required to process any opt-out preference signal, such as a Global Privacy Control, as a valid opt-out request, even if it already posts "Do Not Sell My Personal Information" and "Limit the Use of My Sensitive Personal Information" links.[35] Businesses that do not post such links are further required to process opt-out preference signals in

a frictionless manner, which means not charging a fee, not changing the consumer's experience with the product or service offered by the business, and not displaying a notification, pop up, text, graphic, video, or any interstitial content in response to the opt-out preference signal.[36]

4. CPPA Audit Authority

The CCPA provides the CPPA with the authority to audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA, including those without a California presence.[37] The CPPA may conduct an audit (1) to investigate a possible violation; (2) if the business' collection of processing of PI presents a significant risk to consumer privacy or security; or (3) if the business has a history of noncompliance with the CCPA or any other privacy protection law.[38] These audits may be announced or unannounced,[39] and a business's failure to cooperate during the audit may result in enforcement actions against that business.[40]

II. ENFORCEMENT ACTIONS AND OUTLOOK

Although the CPRA grants the CPPA full administrative power, authority, and jurisdiction to implement and enforce the CCPA, the Attorney General still retains enforcement powers and the CPPA may not limit the authority of the Attorney General to enforce the CCPA.[41]

Enforcement of the CCPA's new obligations added under the CPRA will not begin until July 1, 2023, and enforcement will apply only to violations occurring on or after that date. The CCPA's existing provisions remain in effect and enforceable until that date.[42]

A. REMOVAL OF 30-DAY NOTICE AND CURE PERIOD EXCEPT FOR SECURITY INCIDENTS

The CCPA previously included a 30-day "cure period" following notice of non-compliance from the California Attorney General during which a business had the opportunity to cure the alleged non-compliance without penalty.[43] The CPRA eliminates the 30-day notice and cure period but provides that the CPPA may decide not to investigate a complaint or may choose to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide time to cure, the CPPA may consider (1) the lack of intent by the business to violate the CCPA and (2) the voluntary efforts undertaken by the business to cure the alleged violation prior to being notified by the agency of the complaint.[44]

B. SEPHORA SETTLEMENT

In August 2022, California Attorney General Rob Bonta announced a settlement with Sephora, Inc. (Sephora), its first official enforcement action involving alleged violations of the CCPA. The Attorney General alleged that Sephora failed to (1) disclose to consumers that it was selling their PI and (2) process user requests to opt out of such sales via user-enabled global privacy controls in violation of the CCPA, and that it did not cure these violations within the 30-day period previously allowed by the CCPA.[45] The

California Attorney General's action also alleged violations of California's Unfair Competition Law by Sephora for unfairly depriving California consumers of their statutorily granted opt-out rights.[46]

The allegation against Sephora focused on Sephora's use of third-party tracking software on its website and in its mobile application to monitor consumers as they shop. This practice is common among online retailers, and, in Sephora's case, the third parties were able to create profiles about consumers by tracking their location, the devices used, the items put in their "shopping cart," and other identifiers. These consumer profiles ostensibly allowed Sephora to more effectively target potential customers.

Unlike other U.S. state privacy laws such as those in Virginia or Utah, an exchange of data may constitute a "sale" under the CCPA without monetary consideration, and a business may "sell" PI under the CCPA by disclosing such information to third-party ad networks or tracking software. The California Attorney General alleged that Sephora's arrangement with third parties to install tracking software which enabled them to create consumer profiles constituted a "sale" of consumer information under the CCPA for which Sephora was obliged to provide notice to consumers of the sale and allow consumers to opt out of the sale of their information. Sephora failed to take either of those actions.[47]

The settlement requires Sephora to pay $1.2 million in penalties and comply with important injunctive terms. Sephora must:

- Clarify its online disclosures and privacy policy to include an affirmative representation that it sells PI;
- Provide mechanisms for consumers to opt out of the sale of PI, including via the Global Privacy Control;
- Conform its service provider agreements to the CCPA's requirements; and
- Provide reports to the Attorney General relating to its sale of PI, the status of its service provider relationships, and its efforts to honor Global Privacy Control.[48]

C. CASE EXAMPLES AND INVESTIGATIVE SWEEPS

In 2022, the California Attorney General published 13 new enforcement case examples brought under the CCPA.[49] The case examples address non-compliance related to failures to honor consumer opt-out requests or provide request methods, non-compliant privacy policies or notices, and erroneous treatment of requests to know or delete.[50] In January 2023, the California Attorney General conducted an investigative sweep of mobile applications to evaluate their compliance with CCPA requirements. The sweep focused on popular applications in the retail, travel and food service industries that allegedly did not fulfil consumer opt out requests or failed to provide a mechanism to consumers to opt-out of the sale of their PI. The sweep also focused on businesses that failed to honor consumer requests submitted by authorized agents rather than consumers themselves.[51] Under these case examples, in response to notices received from the California Attorney General, businesses cured the alleged violations, including by updating service provider contracts, implementing technology to honor Global Privacy Control signals, posting or revising applicable

notices, revising online interfaces, implementing required data subject request methods, adding opt-out links, training staff, redesigning loyalty programs and refining data subject request response processes, as applicable.

III. IMPLICATIONS

The CPRA Regulations and the failure of the California legislature to extend the CCPA's original exemptions for employment and B2B data will have a profound impact on companies doing business in California. These businesses are required to update privacy notices, contracts and internal policies and procedures. The proliferation of new requirements imposed by the CPRA, especially the data minimization requirement, increases the likelihood that a business could be liable for violating the CCPA. Companies should heed the lessons from the California Attorney General's enforcement action and case examples and apply them to their business practices in collecting, using and disclosing PI.

* * *

ENDNOTES

1 California Privacy Right Act of 2020 ("CPRA"), CAL. SECRETARY OF STATE, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last accessed January 10, 2023).

2 Cal. Civ. Code § 1798.185.

3 *See* 2021 Colo. S.B. 21-190.

4 *See* 2022 Bill Text CT S.B. 6.

5 *See* Utah Code Ann. Title 13, Ch. 61.

6 *See* Va. Code Ann. § 59.1-Ch. 53.

7 California Privacy Right Act of 2020 ("CPRA"), CAL. SECRETARY OF STATE, https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last accessed January 10, 2023).

8 Cal. Civ. Code § 1798.199.90.

9 *See* Text of Proposed Regulations, CALIFORNIA PRIVACY PROTECTION AGENCY, https://cppa.ca.gov/meetings/materials/20220608_item3.pdf (last accessed January 10, 2023).

10 *See* Notice of Proposed Rulemaking, CALIFORNIA PRIVACY PROTECTION AGENCY, https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf (last accessed January 10, 2023).

11 *See* Final Regulations Text, CALIFORNIA PRIVACY PROTECTION AGENCY, https://cppa.ca.gov/meetings/materials/20230203_item4_text.pdf (last accessed February 20, 2023) ("Final Regulations Text").

12 *See* AB-25 California Consumer Privacy Act of 2018.

13 Final Regulations Text, Section 7051 (a).

14 *Id.*

15 *Id.*

16 *Id*.

17 *Id.* at 7051 (b).

18 Cal. Civ. Code § 1798.140(v).

19 Cal. Civ. Code § 1798.140(ah).

20 Cal. Civ. Code § 1798.140(t) (2018).

21 Cal. Civ. Code § 1798.135(a).

22 *See* Cal. Civ. Code § 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125 (2018).

23 Cal. Civ. Code § 1798.106(c).

24 Cal. Civ. Code § 1798.140(ae)(1).

25 Cal. Civ. Code § 1798.140(ae)(2).

26 Cal. Civ. Code § 1798.100(a)(2).

27 Final Regulations Text, Section 7027 (m).

28 Cal. Civ. Code § 1798.185(a)(15).

29 Cal. Civ. Code § 1798.185(a)(15).

30 *See* Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, CALIFORNIA PRIVACY PROTECTION AGENCY,

ENDNOTES (CONTINUED)

https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf (last accessed Feb. 21, 2023)

31 *See* Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation), Article 5(1)(c).

32 Cal. Civ. Code §1798.100(c).

33 Final Regulations Text, Section 7001 (u).

34 *See* Global Privacy Control, https://globalprivacycontrol.org/ (last accessed Jan. 9, 2023)

35 Final Regulations Text, Section 7025.

36 *Id*.

37 *Id.* at 7304 (a).

38 *Id.* at 7304 (b).

39 *Id*. at 7304 (c).

40 *Id*. at 7304 (d).

41 Cal. Civ. Code § 1798.199.90.

42 Cal. Civ. Code § 1798.185.

43 Cal. Civ. Code § 1798.155(b) (2018).

44 Cal. Civ. Code § 1798.199.45(a).

45 *See* California Attorney General, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement (last accessed Jan. 9, 2023).

46 *Id.*

47 California Attorney General, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement (last accessed Jan. 9, 2023).

48 *Id*.

49 *See* California Attorney General, *CCPA Enforcement Case Examples*, https://oag.ca.gov/privacy/ccpa/enforcement (last accessed Jan. 9, 2023).

50 *Id.*

51 See California Attorney General, *Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act*, https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications%E2%80%99 (last accessed Feb. 7, 2023).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.