Skadden

Privacy & Cybersecurity Update

California Attorney General Announces Settlement With Sephora Under the CCPA

The California attorney general and Sephora, Inc. settled the first action brought by the state under the California Consumer Privacy Act (CCPA), highlighting the need for businesses to conduct data transfers lawfully and honor consumer opt-out requests where required by law.

On August 24, 2022, California Attorney General Rob Bonta announced a settlement with Sephora, Inc. (Sephora), resolving allegations that the company violated the CCPA by failing to honor consumer requests made via Global Privacy Control (GPC) and by failing to comply with certain required disclosures and opt-out processes in relation to the sale of personal information through the use of website analytics.[1] This lawsuit and settlement are the first to be brought by the state government under the CCPA.

Background

Mr. Bonta's office first notified Sephora that it may be in violation of the CCPA in June 2021. The attorney general then sued the company on August 23, 2022, alleging violations of the CCPA, with the complaint[2] alleging that (1) Sephora was not responding to GPC and (2) Sephora's use of trackers (*e.g.*, cookies and pixels) to send personal information to third parties, including data analytics companies and advertising networks, constituted a sale under the CCPA, and that Sephora failed to comply with the CCPA's consumer disclosure and opt-out requirements relating to the sale of personal information. GPC refers to the technical specifications for the transmission of a universal opt-out signal, which allows for browser-level user-enabled requests to signal privacy preferences.

With respect to the GPC, the attorney general's office stated in the CCPA FAQs that covered businesses that sell personal information must honor GPC signals as valid consumer requests to stop the sale of personal information. The complaint noted that "Sephora's website was not configured to detect or process any global privacy control signals" and that, as a result, Sephora was in violation of the CCPA by disregarding

[1] The details of the attorney general's settlement can be found here.

[2] The state of California's complaint against Sephora can be found here.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

consumers who communicated to the company in such manner, making clear that the attorney general views honoring GPC as a requisite for CCPA compliance.

With respect to sales of personal information, the attorney general focused on Sephora's provision of consumer data to third parties, including advertising networks, business partners and data analytics providers, and concluded that this constituted a "sale" under the CCPA, in light of the broad definition of "sale" that covers an exchange of personal information for anything of value. Sephora's relationship with certain third parties satisfied this definition because such information was exchanged for free or discounted services. Since the company did not have a valid service provider contract in place with such third parties — a step that would have qualified the information exchanges as exceptions to the "sale" definition — these exchanges were defined as sales under the law. Sephora's sale of personal information consequently triggered numerous compliance obligations, requiring the company to take steps such as notifying consumers about the categories of personal information sold or shared in the preceding 12 months, posting a "Do Not Sell My Personal Information" link on its website and mobile application, and refraining from selling the data of consumers who opted out of such a sale (including via the GPC). Rather, Sephora had stated in its privacy policy that it did not sell personal information, failed to include a "Do Not Sell My Personal Information" link and sold the information of consumers who exercised their opt-out right via the GPC.

The Settlement

Pursuant to the settlement agreement[3], Sephora agreed to pay a $1.2 million fine and adopt specified compliance measures, including the following:

- clarify its online disclosures to consumers to include an affirmative representation that it sells the personal information of consumers;
- process consumer requests to opt out signaled via GPCs; and
- for the next two years, implement and maintain a program to monitor compliance with opt-out requests and review its data transfers to ensure they are legal, as well as conduct an annual review of its website and mobile applications to determine the entities with which personal information is made available (and provide regular updates to the government on these efforts).

[3] The details of the settlement agreement can be found here.

Key Takeaways

This settlement makes clear that companies need to be mindful of how they collect and use personal information from website and mobile application users to ensure that company policies and practices accurately reflect such collection and usage. It may be prudent for businesses that are subject to the CCPA to conduct a review of their data practices, including (1) confirming whether their website(s) and mobile application(s) honor GPC signals and (2) executing service provider contracts to avoid data transfers to analytics providers that would qualify as a sale (or otherwise take appropriate measures to ensure that sales of personal information are conducted in accordance with law). Companies that fail to do so may risk an enforcement action, as the California attorney general steps up enforcement efforts and the impending implementation of the California Privacy Rights Act (CPRA) on January 1, 2023, eliminates the existing 30-day cure period following a notice alleging violation(s) of the CCPA. In the future, we also may see other states that have implemented data privacy legislation that has similar provisions as the CCPA (*e.g.*, the Colorado Privacy Act and the Connecticut Data Privacy Act) adopt similar requirements to those articulated by California's action against Sephora, thus requiring more widespread adoption of the aforementioned practices.

Return to Table of Contents

California Enacts Privacy Law Aimed at Protecting Children Under 18 Years Old

California Gov. Gavin Newsom signed the California Age-Appropriate Design Code Act into law on September 15, 2022, implementing wide-ranging requirements on businesses that offer online services, products or features that are likely to be accessed by children under the age of 18.

Gov. Newsom signed the California Age-Appropriate Design Code Act (A.B. 2273) into law after its prior passage in the California legislature in August 2022.[4] The Design Code Act, which is scheduled to take effect on July 1, 2024, is designed to work in tandem with the CCPA, as amended by the CPRA, and is modeled after the U.K.'s Age Appropriate Design Code (the U.K. Privacy Code). Notably, the Design Code Act defines the "children" it intends to protect as individuals under the age of 18, which stands in stark contrast to the significantly narrower cutoff of 13 years old that is set forth under the federal Children's Online Privacy Act (COPPA).

[4] The text of the California Age-Appropriate Design Code Act can be accessed here.

Covered Businesses, Services and Products

The Design Code Act will apply to businesses (as defined by the CCPA) that provide online services, products or features (OSPFs) that are likely to be accessed by children.

Businesses that are subject to the CCPA — and therefore the Child Privacy Act as well — are for-profit organizations that conduct business in California (even if not based in California) and satisfy any of the following:[5]

i. the business has annual gross revenue of more than $25 million (regardless of whether generated in California or from California residents);

ii. the business, alone or in combination, annually buys, sells or shares the personal information of 100,000 or more California consumers or households; or

iii. the business derives at least 50% of its annual revenue from selling or sharing personal information of California consumers.

Under the Design Code Act, an OSPF is likely to be accessed by children if it is reasonable to expect that such OSPF would be accessed by children, based on the extent to which the following statutory indicators apply:

i. The OSPF is directed to "children" as defined by COPPA.

ii. The OSPF is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

iii. The OSPF contains advertisements marketed to children.

iv. The OSPF is substantially similar or the same as a separate OSPF subject to clause (ii).

v. The OSPF has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music and celebrities who appeal to children.

vi. A significant amount of the audience of the OSPF is determined, based on internal company research, to be children.

The standard under the Design Code Act for whether an OSPF is likely to be accessed by children is much broader than the comparable standard under COPPA, which is only applicable to operators of websites or services when such website or service is directed to children or the operator has actual knowledge that it is collecting personal information from children. Importantly, the Design Code Act expressly provides that OSPFs exclude broadband internet access services, telecommunications services and — unlike the U.K. Privacy Code — delivery or use of physical products. Further, certain information and entities are exempt from the Design Code Act, including health care providers, entities governed by HIPAA and medical information subject to California's Confidentiality of Medical Information Act.

Compliance Requirements

The Design Code Act imposes certain affirmative obligations on, and prohibits certain activities by, covered businesses providing OSPFs that are likely to be accessed by children. The affirmative obligations include:

- **Data Protection Impact Assessment.** Each covered business must complete a data protection impact assessment (DPIA) (meeting the requirements set forth in the Design Code Act) prior to offering any new OSPF to the public. For currently offered OSPFs, and new OSPFs that will be offered before the Design Code Act goes into effect, DPIAs must be completed by July 1, 2024, (if such OSPF will continue to be offered at that time). Key points to be covered by each DPIA include the purpose of the OSPF, the anticipated uses of children's personal information and the risks of material detriment to the children resulting from the data collection. With respect to each identified risk of material detriment, the business must create a timed plan to mitigate or eliminate the risk before the OSPF is accessed by children. Each business must review and update their DPIAs biennially, and upon request from the California attorney general, must provide a list of all the business's DPIAs within three business days and copies of any requested DPIA within five business days (though such copies would be exempt from public disclosure).
- **Child Age Estimates.** Each covered business must estimate the ages of child users (to facilitate compliance with the Design Code Act) with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or, instead, the business can uniformly apply the privacy and data protections afforded to children under the Design Code Act to all users of the applicable OSPFs. Personal information collected to estimate ages or age ranges may only be used, and may only be retained for as long is necessary, to estimate ages or age ranges.
- **Privacy Defaults and Policies.** Each covered business must set default privacy settings for children using each OSPF to be a "high level"[6] of privacy, unless the business can demonstrate a

[5] The three-prong test for a covered business under the CCPA reflects the CCPA as amended by the CPRA, which will go into effect on January 1, 2023, (and will therefore be in effect when the Design Code Act becomes effective on July 1, 2024).

[6] The Design Code Act does not provide a standard for, or examples of, a "high level" of privacy. However, the act states a general intent of the California legislature that covered businesses can look to the U.K. Privacy Code for guidance. Applicable U.K. guidance for high levels of privacy includes, as an example, default privacy settings that prevent children's personal information from being visible or accessible to other users of the OSPF unless the settings are affirmatively changed to permit such data sharing.

compelling reason that a different default setting is in the best interests of children. Privacy policies must be made available prominently and must be drafted concisely, including by using clear language suited to the age of children likely to access the applicable OSPF, and must actually be enforced by the business.

- **Tracking.** If the OSPF allows a child's parent, guardian or any other consumer to monitor such child's online activity or track the child's location, the OSPF must include an obvious signal to such child when being monitored or tracked.
- **Privacy Tools.** Each covered business must provide prominent, accessible and responsive tools to help children, or their parents or guardians (if applicable), exercise privacy rights and report concerns.

The prohibited activities under the Design Code Act include:

- **Use of Personal Information.** Covered businesses may not use the personal information of children in any way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health or well-being of any child. In addition, businesses cannot collect, sell, share or retain any personal information that is not necessary to provide an OSPF with which a child is actively or knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing or retaining the personal information is in the best interests of children who are likely to access the OSPF. Similarly, if the end user of an OSPF is a child, the business providing such OSPF may not use personal information for any reason other than the reason for which the personal information was collected, unless the business can demonstrate a compelling need that other uses of the personal information is in the best interests of children.
- **Profiling.** Covered business are prohibited from profiling children (*i.e.*, automated processing of personal information to evaluate certain aspects of a natural person or their life) by default unless the business has appropriate safeguards in place to protect the children, and either (a) profiling is necessary to provide the applicable OSPF and the profiled child is actively and knowingly engaged in such process, or (b) the business can demonstrate a compelling reason that profiling is in the best interests of children.
- **Geolocation Information.** Covered businesses may not collect, sell or share any precise geolocation information of children by default unless the collection of precise geolocation information is strictly necessary (and only for such time that such geolocation information is strictly necessary) for the business to provide the applicable OSPF. Precise geolocation information of a child may never be collected without an obvious sign to the child of the collection activity for the duration of such collection activity.
- **Dark Patterns.** Covered businesses are prohibited from using dark patterns to lead or encourage children to provide personal information (beyond what is reasonably expected for the business to provide the applicable OSPF), forego privacy protections or take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health or well-being.

Enforcement

There is no private right of action for violations of the Design Code Act. The California attorney general may bring civil actions against businesses that violate the act, which can result in an injunction and civil penalties of up to $2,500 per affected child for each negligent violation and up to $7,500 per affected child for each intentional violation. If a covered business is in substantial compliance with the Design Code Act, before initiating an action for a violation, the attorney general must provide notice to the business of such a violation and allow the business a 90-day period to cure the violation and implement sufficient measures to prevent future violations, in which case the business will not be liable for any civil penalties for such cured violations.

Key Takeaways

The Design Code Act represents a significant expansion of the number of businesses offering online products or services subject to California privacy law compared to the CCPA, and further represents a heightened level of regulatory compliance compared to the CCPA and COPPA. All businesses, regardless of whether currently subject to California privacy law, should consider reassessing their current and anticipated operations and offerings of products and services to determine whether they are currently, or will be, subject to the Design Code Act, and potentially take necessary actions to reduce risk exposure for violations of the law once it goes into effect on July 1, 2024.

Return to Table of Contents

California Privacy Protection Agency Advances CPRA Rulemaking Process

On August 25, 2022, the formal comment period for the draft regulations implementing the CPRA ended with the conclusion of a public hearing period held by the California Privacy Protection Agency (CPPA).

Background

The CPPA concluded a public hearing period that was held to solicit comments on draft regulations to the CPRA on August

25, 2022.[7] The draft regulations, issued in a notice of proposed rulemaking by the CPPA on July 8, 2022, further define and expand upon the CPRA's statutory provisions. Since the statutory deadline of July 1, 2022, to adopt final regulations has already passed, the CPPA may soon issue final regulations for the CPRA. The CPPA and the California attorney general are authorized to enforce the final regulations against business operating in California starting on July 1, 2023.

Key Provisions of the CPRA Draft Implementing Regulations

The CPRA implementing regulations are intended to (1) update the existing CCPA regulations to harmonize them with the CPRA; (2) operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and (3) reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand. Some of the most significant features of the CPRA draft regulations are discussed below.

- **Consumer Rights.** Consumers have new rights to limit the use of sensitive personal information, correct personal information and opt out of data sharing, in each case, to the extent that a "disproportionate effort" is not required for a business to comply with the relevant consumer request. However, businesses should note that a claim of disproportionate effort cannot be based on a failure to create adequate processes and procedures to respond to a consumer request.
- **Notice Requirements.** Businesses must comply with new notice requirements designed to allow users to make informed decisions about exercising their rights. For example, privacy notices must specify the length of time the business intends to retain each category of personal information collected, including categories of sensitive personal information. Additionally, businesses that sell or share personal information collected through a connected device (*e.g.*, smart TVs or smartwatches), or in augmented reality (AR) or virtual reality (VR), must provide notice in a manner than ensures that the consumer will encounter the notice while using the connected device or engaged in the AR or VR environment.
- **Requirements for the Collection and Use of Personal Information.** Businesses' collection and use of personal information must be "reasonably necessary and proportionate" to the business purpose. To evaluate reasonableness and proportionality, the CPRA mandates an objective "reasonable person" standard based on assumed expectations of the average consumer.
- **Consumer Consent Requirements.** Businesses must avoid manipulative language and cannot make opting out more complicated than consenting, thereby providing consumers with "symmetry of choice." Additionally, withdrawing consent must be as simple as providing it in the first instance. These requirements align with the CPRA's definition[8] of consent, which states that "agreement obtained through use of dark patterns does not constitute consent."
- **Third Party Requirements.** Businesses must publish privacy policies that include notification of any third-party data collection and identify such third parties. A third party that receives a consumer request to delete personal information or opt-out of the sharing or sale of personal information — forwarded to such third party from the business that originally provided or collected the consumer's personal information — must comply with the consumer's request. Additionally, any agreements between a business and a third-party service provider must meet a variety of requirements, including stating, with specificity, the purpose for disclosing consumer personal information.
- **Enforcement Mechanisms.** The CPPA may conduct announced or unannounced audits to investigate potential violations, protect consumer privacy or security, or examine the practices of entities with a track record of noncompliance with CCPA or other privacy laws. The CPPA is empowered to accept individual complaints sworn under penalty of perjury or initiate its own investigations (which could lead to private proceedings).

The Subject Matter of the Final CPRA Implementing Regulations

Businesses operating in California should note that the CPRA draft implementing regulations are subject to revision before the CPRA becomes effective on January 1, 2023, or enforcement begins on July 1, 2023. Notably, in its pre-rulemaking invitation[9] for comments, the CPPA highlighted eight specific topics of interest, two of which are currently not addressed in the draft regulations: (1) "Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses"; and (2) "Automated Decisionmaking." There is a reasonable likelihood that the final regulations may address these two topics and other new topics as well. Further, the CPPA may revise the draft regulations to incorporate the feedback it received during the now-concluded formal comment period.

[7] See the CPPA website at for further detail on the CCPA and CPRA. The California Code of Regulations, Title 11, Division 6, Chapter 1, which are available here.

[8] Under the CPRA, dark patterns are defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

[9] Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, Proceeding No. 01-21.

Key Takeaways

The draft CPRA implementing regulations provide California consumers with new rights and impose new requirements on businesses operating in the state with respect to the notice, collection and use of personal information, and obtaining consumer consent. The regulations also will standardize interactions between businesses collecting consumer personal information and third parties. Although the CPRA implementing regulations are not yet final, businesses subject to the CPRA that are determining what a compliance program will likely require should review these regulations carefully, since there is a reasonable likelihood the final regulations will mirror this draft. As noted, the new privacy obligations imposed by the CPRA will be enforced by the CPPA and the California attorney general starting July 1, 2023.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000