STATE OF CALIFORNIA Gavin Newsom, Governor

CALIFORNIA PRIVACY PROTECTION AGENCY
2101 Arena Blvd
Sacramento, CA 95834
www.cppa.ca.gov

Written Testimony of Maureen Mahoney
Deputy Director of Policy & Legislation, California Privacy Protection Agency

Comments on HB 807 (Online and Biometric Data Privacy)
Maryland House Economic Matters Committee

Chair Wilson, Vice Chair Crosby, and Members of the House Economic Matters Committee, the California Privacy Protection Agency[1] (CPPA or Agency) thanks you for the opportunity to submit written comments on HB 807 (Online and Biometric Data Privacy). Our originating statute, the California Consumer Privacy Act (CCPA), directs the Agency to work with other entities with jurisdiction over privacy laws to "ensure consistent application of privacy protections."[2] We are proud that states are leading the way on legislation to protect consumers' privacy and data security. As of 2023, four states have adopted, and over half the states have considered, omnibus consumer privacy laws.[3]

The Agency is encouraged that HB 807 shares similarities with California's approach. For example, HB 807, like the CCPA, not only provides consumers with the right to access, delete, correct, and stop the sale of information to third parties, with additional protections for sensitive data, but is intended to be easy for consumers to use. This reflects the concerns outlined in the California law's findings, which pointed out the "asymmetry of information [that] makes it difficult for consumers to understand what they are exchanging[.]"[4]

Background

California has a long history of privacy and data protection legislation. In 1972, California voters established the right of privacy in the California Constitution, amending it to include privacy as one of Californians' "inalienable" rights.[5] In 2002, California became the first state to pass a data breach notification requirement, and in 2003, became the first state to require businesses to post privacy policies outlining their data use practices. In 2018, it became the first state in the nation to adopt a comprehensive commercial privacy law, the California Consumer Privacy Act. That measure went into effect on January 1, 2020, and the Attorney General began enforcing it on July 1, 2020.[6]

In November 2020, California voters ratified Proposition 24, the California Privacy Rights Act, which amends and expands the CCPA, including by creating the first authority with full administrative powers focused on privacy and data protection in the United States, the California Privacy Protection Agency.

[1] Established in 2020, the California Privacy Protection Agency was created to protect Californians' consumer privacy. The CPPA implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

[2] Cal. Civ. Code § 1798.199.40(i).

[3] National Conference of State Legislatures, 2022 Consumer Privacy Legislation (updated June 10, 2022), https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation.

[4] Proposition 24, The California Privacy Rights Act § 2 (2020), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.

[5] Cal. Cons. Art. 1 § 1.

[6] Cal. Civ. Code § 1798.100 et seq.

Proposition 24 added new substantive provisions to the CCPA, such as new limitations on businesses' collection, use, retention, and sharing of personal information, a right to correction, and additional protections for sensitive data, which went into effect on January 1, 2023. On April 21, 2022, rulemaking authority under the CCPA formally transferred to the Agency. Along with the Attorney General, the Agency is vested with the authority to undertake enforcement to protect Californians' privacy.

Overview of California law

The CCPA includes specific notice requirements for businesses, grants new privacy rights to consumers, and imposes corresponding obligations on businesses. The rights granted to consumers include the right to know what personal information businesses have collected about consumers and how that information is being used, sold, and shared; the right to delete personal information that businesses have collected from consumers; the right to stop businesses' sale and sharing of personal information; and the right to non-discrimination in service, quality, or price as a result of exercising their privacy rights. As of January 1, 2023, California consumers have the right to correct inaccurate personal information the business maintains about them, and the right to limit a business's use and disclosure of sensitive personal information about them to certain business purposes, among other protections.

The CCPA provides additional protections for children under 16. Businesses are not permitted to sell the personal information of consumers if the business has actual knowledge that the consumer is under 16, unless the consumer, or the consumer's parent or guardian in the case of consumers who are under 13, has affirmatively authorized the sale of the consumer's information.

The CCPA covers information that identifies, relates to, or could reasonably be linked with a particular consumer or household—subject to certain exceptions. The measure applies to for-profit businesses that do business in California, collect consumers' personal information (or have others collect personal information for them), determine why and how the information will be processed, and meet any of the following thresholds: have a gross annual revenue of over $25 million; buy, sell, or share the personal information of 100,000 or more California consumers or householders; or derive 50% or more of their annual revenue from selling or sharing California residents' personal information.

Businesses have corresponding duties, including with respect to:

- *Data minimization and purpose limitations*
  - Businesses' collection, use, retention, and sharing of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.
  - Businesses must not further process personal information in a manner that is incompatible with those purposes.
- *Dark patterns*
  - In obtaining consent from consumers, businesses are prohibited from using "dark patterns," which are defined to mean a user interface "designed or manipulated with the

> substantial effect of subverting or impairing user autonomy, decisionmaking, or choice[.]"[7]

Overview of CPPA Rulemaking

The California Privacy Protection Agency is currently engaged in a formal rulemaking process to issue regulations to further the intent of the CCPA, as amended.[8] On July 8, 2022, the Agency published its notice of proposed action in the California Regulatory Notice Register, beginning the formal rulemaking process. The proposed regulations primarily do three things: (1) update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; (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. They place the consumer in a position where they can knowingly and freely negotiate with a business over the business's use of the consumer's personal information.

HB 807 and State Privacy Laws

As noted above, the Agency appreciates that HB 807 shares similarities with California's approach. It's important that consumers have effective tools to protect their privacy, as well as default protections that provide key privacy safeguards even without taking additional steps. For example, like California and other states, HB 807 has several provisions that help ensure this ease of use for consumers:

- ***Global opt-out***. California, Colorado, and Connecticut each have a provision in their privacy laws requiring businesses receiving opt-out requests to honor requests submitted by browser privacy signals.[9] The CPPA's proposed regulations reiterate the requirements for an opt-out preference signal that consumers may use to easily opt-out of the sale or sharing of their personal information with all businesses that they interact with online. With the goal of strengthening consumer privacy, the regulations support innovation in pro-consumer and privacy-aware products and services and help businesses efficiently implement privacy-aware goods and services.

  The California Attorney General is currently enforcing the browser privacy signal requirement in the existing CCPA regulations. Last year, it announced its first public case, against Sephora, alleging that Sephora failed to disclose to consumers that it was selling their personal information and failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA.[10]

[7] Cal. Civ. Code § 1798.140(l).

[8] For more information about the Agency's work to implement the regulations, please see California Privacy Protection Agency, California Consumer Privacy Act Regulations, https://cppa.ca.gov/regulations/consumer_privacy_act.html.

[9] See, Cal. Civ. Code § 1798.135(e).

[10] Press release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act* (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement. For information on additional AG enforcement activity, see State of California Department of Justice, CCPA Enforcement Case Examples (updated Aug. 24, 2022), https://oag.ca.gov/privacy/ccpa/enforcement.

- ***Prohibition on dark patterns***. California, Colorado, and Connecticut all have a provision prohibiting businesses from using dark patterns, defined in California as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation[,]" in obtaining consent.[11] California's proposed regulations set forth clear requirements for how businesses are to craft their methods for submitting consumer requests and obtaining consumer consent so that the consumer's choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. They address not only narrow situations where consent must affirmatively be given, but general methods for submitting CCPA requests to address abuse by businesses who craft methods in ways that discourage consumers from exercising their rights.[12]

- ***No requirement for authentication to opt out***. Like HB 807, neither the CCPA nor Connecticut's privacy law require authentication of opt-out requests. Verification often creates friction for consumers, making it more difficult for consumers to exercise their rights. This is particularly important as online identifiers that are used for behavioral tracking cannot be easily accessed or verified by the consumer. Like HB 807, California and Connecticut do require identity verification for access, deletion, and correction requests, where consumer privacy could be undermined in the case of an unauthorized request.

However, there are some elements of California law that are not included in HB 807. For example:

- ***Broad definition of personal information.*** California has a broad definition of personal information, including "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." It also specifically identifies online identifiers, inferences, and pseudonymous identifiers as personal information.[13]

- ***Protections with respect to non-discrimination/loyalty program*s.** The CCPA prohibits businesses from discriminating against consumers for exercising any of the rights provided by the measure, including by denying goods or services, offering a different price or a different level of quality for goods or services, or retaliating against an employee. Businesses are permitted to charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data. Businesses are not permitted to use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.[14]

Conclusion

We hope that our work in implementing the CCPA is helpful to you as you consider legislation. I am happy to answer any questions.

[11] Cal. Civ. Code § 1798.140(l)

[12] See, California Privacy Protection Agency, Draft Final Regulations Text at § 7004 (Feb. 3, 2023), https://cppa.ca.gov/meetings/materials/20230203_item4_text.pdf.

[13] See, Cal. Civ. Code § 1798.140(v).

[14] Cal. Civ. Code § 1798.125.