1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

June 30, 2026

Via Electronic Submission

CA Department of Justice, Consumer Protection Section
Attn: D. DuBois
1515 Clay Street Oakland, CA 94612
SB976@doj.ca.gov

Re: Notice of Proposed Rulemaking — Protecting Our Kids from Social Media Addiction Act Regulations, Cal. Code Regs., tit. 11, §§550–581

Dear Department Staff,

The Future of Privacy Forum (FPF) is pleased to submit comments to the California Department of Justice (California DOJ), Consumer Protection Section regarding the Notice of Proposed Rulemaking on regulations implementing the Protecting Our Kids from Social Media Addiction Act (SB 976 or the Act).[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices.[2]

We appreciate the California DOJ's invitation for input on several timely topics subject to agency rulemaking under the Act. Our comment addresses three primary areas of the proposed rulemaking: age assurance, verifiable parental consent (VPC), and data retention and minimization. Accordingly, we comment on the following:

1. **Age Assurance:** FPF appreciates that the Department has already considered our work on age assurance within the research repository consulted during the creation of these regulations. FPF welcomes the opportunity to further discuss any age assurance questions the Department has while working towards finalizing these regulations.
2. **Verifiable Parental Consent:** When exploring appropriate methods for verifiable parental consent, consider the known problems, concerns, and friction points that already exist with verifiable parental consent under COPPA.

---

[1] *Notice of Proposed Rulemaking, Protecting Our Kids from Social Media Addiction Act Regulations*, California Department of Justice (published May 15, 2026), https://oag.ca.gov/system/files/media/sb976-proposed-rulemaking.pdf.

[2] The views expressed in this comment are those of FPF and do not necessarily reflect the views of FPF's supporters or Advisory Board.

3. **Data Retention and Use Limitation:** When considering data retention and limitation provisions, consider aligning the regulatory approach with the statutory language provided by § 27001.

FPF's comments are informational in nature and do not seek to recommend or endorse any particular method of age assurance or verifiable parental consent but instead intend to provide information about current industry practices to further inform the agency's rulemaking efforts.

I. Age Assurance — Scope

The proposed regulations already establish a detailed, performance-based framework for age assurance: acceptable methods are identified at § 561(a); each must be "reasonably effective," demonstrate "measurable consistency," and be testable under § 561(b); and insufficient methods are listed at § 563. FPF takes no position on the relative merits of any specific method identified in these provisions but refers the Department to FPF's infographic, *Unpacking Age Assurance: Technologies and Tradeoffs*, for additional detail on how these methods function and their relative privacy/assurance tradeoffs.[3] In particular, FPF draws the Department's attention to FPF's 2026 updates, which, in line with the Department's proposed regulations, downplay age declaration as a standalone solution to age assurance. However, when utilized in a waterfall or layered approach, alongside other mechanisms, can remain useful, particularly for lower-risk contexts. Additionally, the 2026 updates detail inferences as a new category of age assurance, which the Department may consider not only for disproving an age determination, as noted in § 563(a), but also as an additional layer of *affirming* age. FPF welcomes the opportunity to discuss this resource, or any aspect of age assurance, further with the Department.

II. Verifiable Parental Consent

The proposed verifiable parental consent (VPC) requirements under §§ 570–574 establish a two-step process for obtaining VPC. Section 570(b) would require operators to obtain a minor's own permission before seeking parental consent, and § 571(b) ties acceptable VPC methods to those already approved under COPPA, 16 C.F.R. § 312.5(b)(2). FPF appreciates the Department's efforts to layer informed consent into these requirements through this sequential structure—first the minor's permission, then the parent's consent for access to a covered feed. But we also note that, although the proposed sequential approach to informed consent respects both minors' and parents' autonomy, layering multiple consent or permission prompts can also contribute to consent fatigue, where users grow less attentive to each successive request for consent.[4] As a result, the successive consent processes may ultimately be less effective than the Department

---

[3] Future of Privacy Forum, *Unpacking Age Assurance: Technologies and Tradeoffs* (Feb. 2026), https://fpf.org/wp-content/uploads/2026/02/FPF-Age-Assurance-v2.0.pdf.

[4] Sakshi Shivhare, *Keeping Up with "Consent" in Data Protection Frameworks: A Comprehensive Update for APAC*, Future of Privacy Forum, p.2 (Apr. 2025), https://fpf.org/wp-content/uploads/2025/05/Issue-Brief-_-Updated-APAC-Consent-Report-Google-Docs.pdf.

intended and create ambiguity for consumers concerning the purposes of each consent process. The potential for fatigue under this two-step consent scheme may be further exacerbated when combined with required user consent or authorization under other laws, such as teen consent processes under the California Consumer Privacy Act (CCPA).[5]

Furthermore, FPF appreciates the intent of § 571(c)—requiring that operators offer at least one VPC option that does not require an account, a purchase, or government-issued form of identification—to ensure that parents have access to a COPPA-compliant consent method that does not rely on disclosing sensitive information or creating a new user account. Even with this added language, however, existing COPPA VPC methods are known to generate specific friction points for parents and children seeking access to online services.[6] These friction points include:

- **Efficacy.** Children can and do get around VPC requirements. One parent FPF interviewed on VPC in the course of research described children doing so "by making up birthdays, finding wallets around the house for their parents' IDs, or entering their own credit card or email information into a VPC prompt."[7] Even well-designed methods aren't immune, which counsels weighing the privacy cost of collecting sensitive verification data against the modest efficacy gains it produces.
- **Accessibility.** Methods requiring a credit card or government ID disadvantage two populations: the roughly 5.9 million U.S. households without a bank account,[8] and parents, including undocumented immigrants, who lack government identification.[9] This is also a nondiscrimination question the Department is statutorily obligated to weigh: Health & Saf. Code § 27006(c) requires the DOJ to solicit comments on the impact of any proposed regulation based on the characteristics protected under Civil Code § 51, which include immigration status and national origin. These gaps are direct support for why § 571(c)'s carve-out matters.
- **Privacy/security hesitancy.** Parents are often wary of submitting sensitive personal information tied to their child's account, and COPPA's experience shows this can redirect parents and children to other comparable products or services where they can avoid VPC processes.
- **Cost/convenience drop-off.** Friction drives drop-off, and drop-off can push a minor toward an adult experience without oversight—the opposite of the statute's goal.

---

[5] See e.g., Cal. Civ. Code § 1798.120, subd. (c) (providing that consumers aged 13-16 must provide opt-in consent for the sale or share of their personal data, and, in the case of minors under 13, parents provide opt-in consent).

[6] *See also* Future of Privacy Forum, *The State of Play: Verifiable Parental Consent and COPPA* (June 2, 2023), https://fpf.org/verifiable-parental-consent-the-state-of-play/.

[7] *Id.* at 11.

[8] FDIC, *National Survey of Unbanked and Underbanked Households*, at 1, 13 (2021), fdic.gov/analysis/household-survey/2021report.pdf.

[9] FPF, *State of Play*, *supra* note 4.

FPF offers three considerations for how to alleviate some of these difficulties in implementing VPC requirements. First, rather than relying solely on the static list of methods approved under 16 C.F.R. § 312.5(b)(2), it may be beneficial for the Department to consider a criteria-based or updateable VPC standard. COPPA's own approval mechanism illustrates the risk of a static list: since 2013, the FTC has approved only two new VPC methods, and has received no new submission since 2015.[10] Second, it may be beneficial to provide greater clarity in the notice required under § 572 regarding data practices involved, such as explicitly disclosing to consumers why VPC data is collected, how it's used, and how long it's retained. Doing so may ease the consumer hesitancy described above and benefit covered entities by providing clear guidance on transparency requirements when complying with these obligations. Third—regarding § 573's "as easy to use as the mechanism used to give consent" revocation standard—it may be beneficial for the agency to provide illustrative examples of effective compliance for this provision in the final text, consistent with the Department's approach elsewhere (e.g., §§ 561, 565) to further clarify these regulations for businesses' compliance efforts.

III. Data Retention & Use Limitations

Section 561(e) of the proposed regulations would require that data collected to comply with the age assurance requirement be minimized to no more than necessary than to comply with legal requirements of this specific section, used for no other purpose, securely held, and deleted immediately once its compliance purpose is served. FPF understands the data protection goals of this proposed regulatory provision but notes that this language is narrower than the data limitation obligation articulated in the statutory text and may lead to unintended compliance outcomes.

California Health & Safety Code § 27001(2)(b) requires that data collected to comply with the age assurance requirement be used for no other purpose than complying with that chapter ***"or with another applicable law"*** and deleted immediately once its compliance purpose is served.[11] In contrast, the proposed regulations only allow operators to use information collected for age assurance for compliance with that chapter and no other state or federal laws. As a result, operators may experience ambiguity when determining compliance with these regulatory provisions or the statutory text. Additionally, if operators were to rely on the narrowed data limitation approach in the regulations, only allowing age data to be used for compliance with this chapter may run counter to other data protection or online safety goals the Department aims to achieve through compliance. That is, operators would need to conduct additional age assurance processes to comply with other legal requirements instead of relying upon age determinations made through these regulations or may be precluded from using age data collected under these obligations to implement minor privacy and/or safety obligations required under other laws.

---

[10] *Id.* at 16-17.

[11] Cal. Health & Safety Code § 27001(b) (2025) (emphasis added).

As a result, it may be beneficial to further clarify the intention of this proposed data limitation requirement or align the approach of these proposed data retention and limitation requirements with the statutory text in § 27001.

* * *

Thank you for this opportunity to provide comments on these proposed regulations. FPF welcomes any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Daniel Hales at dhales@fpf.org.

Sincerely,

Daniel Hales
Policy Counsel, US Legislation

Jack Maketa
US Legislation Intern