CALIFORNIA DEPARTMENT OF JUSTICE

TITLE 11. LAW
DIVISION 1. ATTORNEY GENERAL
CHAPTER 5.5. PROTECTING OUR KIDS FROM SOCIAL MEDIA ADDICTION ACT REGULATIONS

TEXT OF PROPOSED REGULATIONS

Chapter 5.5. Protecting Our Kids from Social Media Addiction Act Regulations

Article I. General Provisions

§ 550. Title and Scope.

(a) This Chapter will be known as the Protecting Our Kids from Social Media Addiction Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the Protecting Our Kids from Social Media Addiction Act and do not limit any other rights that consumers have.

(b) A violation of these regulations shall constitute a violation of the Protecting Our Kids from Social Media Addiction Act and is subject to the remedies provided for therein.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 2700, 27001, 27002, 27003, 27004, 27005, 27006 and 27007, Health and Safety Code.

§ 551. Definitions.

For purposes of these regulations:

(a) "Addictive internet-based service or application" has the meaning set forth in Health and Safety Code section 27000.5.

(b) "Addictive feed" has the meaning set forth in Health and Safety Code section 27000.5.

(c) "Covered features" means either of the following:

  (1) Addictive feed; or

  (2) Notifications sent by an operator of an addictive internet-based service or application during the hours specified in Health and Safety Code section 27002, subdivision (a).

(d) "Minor" has the meaning set forth in Health and Safety Code section 27000.5.

(e) "Operator" has the meaning set forth in Health and Safety Code section 27000.5.

(f) "Parent" or "parental" refers to any of the following:

(1) A biological or adoptive parent of a child;

(2) A foster parent;

(3) A legal guardian; or

(4) An individual acting in the place of a biological or adoptive parent, including a grandparent, stepparent, or other relative, with whom the child lives, or an individual who is legally responsible for the child's welfare.

(g) "User" has the meaning set forth in Health and Safety Code section 27000.5.

Note: Authority cited: Section 27006 and 27000.5, Health and Safety Code. Reference: Section 27000.5, Health and Safety Code.

Article II. Reasonable Determination That the User Is Not a Minor

§ 560. Actual Knowledge.

(a) If an operator has actual knowledge that the user is a minor, including via a signal pursuant to the Digital Age Assurance Act, the operator must not provide covered features unless it obtains verifiable parental consent.

(b) If an operator has actual knowledge that the user is not a minor, including via a signal pursuant to the Digital Age Assurance Act, the operator need not make a reasonable determination that the user is not a minor before providing the user with covered features.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

§ 561. Reasonable Determination That a User Is Not a Minor.

(a) If an operator does not have actual knowledge that the user is a minor, an operator must make a reasonable determination that the user is not a minor before providing covered features. This reasonable determination must be made by using one or more commercially reasonable and technically feasible age assurance methods. Examples of commercially reasonable and technically feasible age assurance methods that can be used to make a reasonable determination include the following:

(1) Using biological or behavioral signals, such as facial analysis, hand-gesture or gait patterns, and vocal analysis.

(2) Using verified information other than age, such as behavioral patterns, data collected about the user, digital interactions, and metadata.

(3) Using a cryptographic technique, such as a zero-knowledge proof, that allows a user to demonstrate whether they are a minor using verified data that does not reveal any other information about the user to the operator or a third-party.

(4) Using government-issued identification, such as a driver's license, California identification card, passport, military identification, or validation against an official government record, provided that the operator complies with section 562.

(5) Using an age assurance method that satisfies the framework set forth in ISO/IEC 27566: "Information security, cybersecurity and privacy protection – Age assurance systems," incorporated by reference herein.

(b) The age assurance method(s) used by an operator must be reasonably effective at identifying users under the age of 18, perform with measurable consistency, and be testable, with quantifiable results to show accuracy rate.

(c) An operator must publish and maintain on its website a report describing the measures it takes to reasonably determine that a user is not a minor. The operator must include the following in its report:

(1) A description of the age assurance method(s) used, the data relied upon, and how that data is collected. For example, an operator may state that one of its age assurance methods is to check a user's age using government-issued identification, list the forms of identification it accepts, state that it relies on the date of birth listed on government-issued identification, and describe that it uses a photo upload to collect that data. The operator may state that it also uses biometric facial analysis, describe how it uses live video to collect that data, and describe the methodology and data used to conduct its analysis.

(2) The operator's basis for relying on that data for age assurance purposes. For example, an operator using biometric facial analysis may describe the known connection between certain facial features and age as compared to an existing, identified database.

(3) An explanation of how the operator's application of the age assurance method(s) yields a reasonable determination that a user is not a minor. For example, an operator

using a method that relies on a photo upload of government-issued identification may explain that it uses computer software that identifies the date of birth on the government-issued identification and then automatically calculates a user's age based on that information. As another example, an operator using biometric facial analysis may describe how it applies an algorithmic computer program that analyzes specific facial features to determine age.

(4) A summary of the measures taken to ensure the accuracy of the age assurance method(s) used, including all of the following:

(i) The measures taken by the operator to prevent and account for circumvention, fraud, or misuse of the age assurance method, including detecting and avoiding the use of falsified data. For example, an operator using a method that relies on government-issued identification may describe its measures to detect falsified identification documents, detect modified or falsified age information on identification documents, and maintain a record of users who have submitted such documents. As another example, an operator using biometric facial analysis may describe its measures to detect when users present a static image of a face that is not their own.

(ii) The measures taken by the operator to avoid the use of low-quality data that could result in incorrectly identifying a minor as at least 18 years of age or in an inconclusive age assurance outcome where the operator is unable to reach a determination as to whether the user is a minor. For example, an operator using a method that relies on government-issued identification may state that it uses computer software to identify watermarks and other features on the government-issued identification that confirm authenticity. As another example, an operator using biometric facial analysis may describe how it detects that a user has a low-quality camera or poor lighting and how it responds under those circumstances.

(iii) A description of how each age assurance method used is testable and how the operator ensures that it is reasonably effective and measurably consistent.

(iv) A quantitative description of the effectiveness of the age assurance method(s) used to correctly identify minors as being under 18 years of age. For example,

an operator may include in its report that the age assurance methods it provides have a rate of false positives for an age assurance method that is equal to or less than the following: 0.1% of minors ages 0 to 7; 1% of minors ages 8 to 13; 2% of minors ages 14 to 15; 8% of minors age 16; 15% of minors age 17, excluding failures or refusals by a user to provide requested data and inconclusive age assurance outcomes; and that the operator has a rate of detecting circumvention of an age assurance method that exceeds 98%. As another example, an operator may demonstrate the quantitative effectiveness of an age assurance method it uses by including in its report a confusion matrix that details how often the age assurance method correctly predicts that a minor user is a minor, that an adult user is an adult, and incorrectly predicts that a minor user is an adult, and an adult user is a minor.

(v) A description of how and how often the operator tests, audits, and reviews each age assurance method used.

(d) If the operator uses the same age assurance method to meet the legal requirements of another state, federal, or international framework, the operator may identify that framework as part of the report published and maintained on its website.

(e) Data collected for the purpose of complying with this section:

(1) Must be no more than is necessary to comply with this section;

(2) Must not be used for any purpose other than to comply with this section;

(3) Must be collected and stored using industry-standard data security measures and as required by law; and

(4) Must be held no longer than the time required to comply with this section and thereafter must be immediately deleted.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

§ 562. Government-Issued Identification.

An operator must not require that a user provide government-issued identification and must not use as its sole method of age assurance a method that requires a user to provide government-issued identification.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

§ 563. Unreasonable Determination.

(a) An operator's determination that a user is not a minor is not reasonable if the operator:

(1) Relies on self-declaration that the user is not a minor.

(2) Relies on general contractual restrictions or terms regarding the use of the internet website, online service, online application, or mobile application, including restrictions based on age.

(3) Relies on online payment methods that are available to minors.

(4) Relies on an age assurance method that uses biometrics without taking reasonable measures to mitigate the risks of presentation attacks, where a user attempts to circumvent the method by using a static image, pre-recorded video, digitally altered face or image, or other means.

(5) Relies on an age assurance method that has known or documented risks related to the submission of low-quality or incomplete documents, images, video, or other data from a user without taking reasonable measures to mitigate those risks.

(6) Relies on an age assurance method that has known or documented risks related to varying error rates across demographic groups other than age without taking reasonable measures to mitigate those risks. For example, if an operator uses an age assurance method that relies on biometric facial analysis that has known or documented error rates specific to a particular demographic group, the operator must take mitigating measures to eliminate the bias and improve the fairness and equity of the age estimation model, such as by investigating and correcting for any imbalances in composition of the existing dataset or training population used.

(7) Relies on an age assurance method that has other known or documented risks without taking reasonable measures to mitigate those risks.

(8) Makes a determination that is not reasonable based on all information about the user known to the operator, including information used for marketing, content selection, or other purposes, or inferential data that indicates that a user may be a minor, at the time the determination is made.

(b) An inconclusive age assurance outcome cannot provide the basis for an operator to reasonably determine that the user is not a minor.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

§ 564. Appeals Process.

An operator must implement and maintain a process for a user to appeal the operator's determination that the user is a minor or when the operator cannot reasonably determine that the user is not a minor. The operator must:

(a) Offer one or more methods for a user to submit information demonstrating that the user is not a minor;

(b) Evaluate all information submitted by the user;

(c) Determine in good faith whether the information provides a reasonable basis to reverse the operator's previous determination that the user is a minor or to change an inconclusive age assurance outcome; and

(d) Provide a written notice to the user of its decision that includes an explanation of the basis for the decision.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

§ 565. Circumvention, Fraud or Misuse of Methods to Determine Minor Status.

An operator must: (1) take reasonable measures to prevent circumvention, fraud, or misuse of the method(s) used by the operator to determine whether the user is a minor, and (2) maintain and document its reasonable measures. An operator must consider emerging forms of circumvention, including through advances in technology; consider how a user can conceal or misrepresent whether they are located in the State of California; and take reasonable mitigating measures against circumvention, fraud, or misuse. For example, an operator that uses biometric facial analysis must analyze real-time data to confirm that a face presented to a system is a live person and not a photo, pre-recorded video, mask, deep fake, or other circumvention. As another example, an operator must consider in its determination any data regarding the geographic

location of a user that is collected for other purposes, including marketing, commercialization of user engagement, or generating personalized content.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27001, Health and Safety Code.

§ 566. Consistency Across Points of Access.

An operator with actual knowledge that a user is a minor or that reasonably determines that a user is a minor must use this information across all points of access to the operator's platform, including the operator's internet website, online service, online application, or mobile application. For example, if the operator of a mobile application determines that a user is a minor, the operator must not provide that user covered features on the internet website version of its application.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27001, Health and Safety Code.

§ 567. Report or Information Indicating a User is a Minor.

An operator must implement a process to receive and respond to any report or information, including information used for marketing, content selection, or other purposes, or inferential data, indicating a user is a minor or that data was falsified regarding their age or location. The operator must (1) investigate and determine in good faith if the report or information provides a reasonable basis to change the operator's previous determination regarding the user's status as a minor, and (2) provide written notice to the user of its decision if it changes its previous determination that a user is not a minor, including an explanation of the basis for its decision.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Section 27001, Health and Safety Code.

Article III. Verifiable Parental Consent

§ 570. Preliminary Requirements for Seeking Verifiable Parental Consent.

Prior to seeking verifiable parental consent as required by Health and Safety Code section 27001, subdivision (a)(2) and section 27002, subdivision (a)(1), an operator must first:

(a) Provide the user with notice that the operator cannot legally provide the user covered features without verifiable parental consent; and

(b) Obtain consent from the user to seek verifiable parental consent for the operator to provide covered features.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27003 and 27004, Health and Safety Code.

§ 571. Methods of Verifiable Parental Consent.

(a) If a user consents to an operator seeking verifiable parental consent to provide the user with covered features, the operator must provide the parent with notice pursuant to section 572 and offer the parent access to a method of verifiable parental consent as set forth in subdivision (b). The operator must provide the parent with the required notice at or before any request for consent.

(b) Any method of verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the individual providing consent is a parent of the minor, such as the methods for verifiable parental consent set forth in 16 C.F.R. § 312.5(b)(2) (2026).

(c) An operator seeking verifiable parental consent must provide at least one option that does not require any of the following:

    (1) That the parent create an account with the operator;

    (2) That the parent make a purchase from the operator; or

    (3) That the parent furnish government-issued identification. If the operator already possesses the parent's government-issued identification to comply with other laws, seeking the parent's consent to use that government-issued identification for verifiable parental consent does not constitute requiring the parent to furnish government-issued identification for purposes of this subdivision.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27003 and 27004, Health and Safety Code.

§ 572. Notice Requirements.

(a) The notices required by section 570, subdivision (a) and section 571, subdivision (a) must:

(1) Identify the internet website, online service, online application, or mobile application for which the covered features apply;

(2) Identify the minor's account, profile, and username, as applicable; and

(3) State, with equal prominence and in plain language that is understandable to the target audience, that California law does not allow the operator to provide covered features to a minor without verifiable parental consent; the user can access the platform without being provided covered features; and a parent can revoke their consent at any time. The notice must describe how a parent may revoke their consent.

(b) In addition to the requirements set forth in section 572, subdivision (a), the notice required by section 570, subdivision (a) must also state, with equal prominence and in plain language that is understandable to the target audience, that the operator will not seek verifiable parental consent without first obtaining consent to do so from the user; the user does not need to provide consent and can access the platform, except as to covered features, without providing consent; and the user can revoke their consent at any time. The notice must describe how a minor may do so.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27003 and 27004, Health and Safety Code.

§ 573. Revocation of Consent.

(a) A user's consent for an operator to seek verifiable parental consent is revocable at any time. If a user revokes consent, the operator shall immediately cease any further effort to obtain parental consent. An operator must provide users with a simple, easily accessible mechanism to revoke the user's consent.

(b) Parental consent for an operator to provide covered features to a minor is revocable at any time. If a parent revokes consent for a minor, the operator shall immediately cease providing

the user covered features. An operator must provide parents with a simple, easily accessible mechanism to revoke consent for an operator to provide covered features to their child.

(c) The mechanism to revoke consent must be as easy to use as the mechanism used to give consent. For example, a user or parent must not be required to interact with a live representative to withdraw consent if it was not required to give consent.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27003 and 27004, Health and Safety Code.

§ 574. Circumvention, Fraud or Misuse of the Method(s) Used to Obtain Verifiable Parental Consent.

An operator must implement, maintain, and document a protocol to prevent circumvention, fraud, or misuse of the method(s) of verifiable parental consent used by the operator. As part of this protocol, an operator must consider emerging forms of circumvention, including through advances in technology, and take reasonable mitigating measures. For example, an operator must monitor whether the same individual, as determined by an identifier such as an email address, IP address, username, or account with the operator's online platform, purports to be the parent of dozens of minors.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27003 and 27004, Health and Safety Code.

Article IV. Miscellaneous

§ 580. Other Laws.

(a) Nothing in these regulations limits an operator's existing obligations to comply with state and federal law, including data privacy laws.

(b) Nothing in these regulations requires an operator to offer or provide covered features to users.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27001, 27003, and 27004, Health and Safety Code.

§ 581. Severability.

Each provision of these regulations is severable from the remainder. If any provision, or application of these regulations, to any person or circumstance is held invalid, that invalidity does not affect other provisions or applications of these regulations that can be given effect without the invalid provision or application.

Note: Authority cited: Section 27006, Health and Safety Code. Reference: Sections 27007, Health and Safety Code.