CALIFORNIA DEPARTMENT OF JUSTICE

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

INITIAL STATEMENT OF REASONS

PROBLEM STATEMENT

The Protecting Our Kids from Social Media Addiction Act (the "Act") was enacted in 2024. Among other things, the Act makes it unlawful, beginning January 1, 2027, for an operator of an addictive internet-based service or application to provide an addictive feed, or to send notifications during certain hours, to users in California unless the operator has actual knowledge that the user is not a minor, reasonably determines that the user is not a minor, or obtains verifiable parental consent to provide the addictive feed or send the notifications to the user. Prior to January 1, 2027, operators are prohibited from providing an addictive feed or sending notifications during certain hours if they have actual knowledge that the user is a minor, unless the operator obtains verifiable parental consent. The Act also requires operators to provide parents with certain default settings for controlling access to features on the platform and to comply with other reporting requirements. (Health & Saf. Code, §§ 27000-27007.)

The Act directs the Attorney General to adopt regulations to further the purposes of the Act, including regulations regarding age assurance and parental consent. (Health & Saf. Code, § 27006, subd. (b).) Accordingly, the purpose of these proposed regulations is to provide clarity and specificity regarding the requirements of the Act and to operationalize the Act's requirements.

In passing the Act, the Legislature stated that some social media platforms have evolved to include addictive features that pose "a significant risk of harm to the mental health and well-being of children and adolescents." (Sen. Bill No. 976 (2023-2024 Reg. Sess.) § 1, subd. (b).) The purpose of the Act is to require that operators obtain parental consent before providing children and adolescents harmful and addictive social media features. (*Id.* § 1, subd. (g).) The Legislature noted that while social media provides an important tool for communication and information sharing, more than one-third of 12- to 17-year-olds report that they use social media almost constantly, and approximately 95 percent report that they use at least one social media platform. (*Id*, § 1, subd. (a).) As the Legislature further noted, the United States Surgeon General reported that recent evidence has identified "reasons for concern" about social media usage by children and adolescents, including a risk of poor mental health outcomes. (*Id*. § 1, subd. (c).) The Legislature cited several types of negative health outcomes, including low self-esteem, disordered eating, less healthy sleep patterns and sleep quality, depressive symptoms, and self-harm behaviors. (*Id.* § 1, subds. (c), (d), (e).) The Legislature noted that both California and the country as a whole are facing an "ongoing youth mental health crisis, with rates of adolescent suicides, depressive episodes, and feelings of sadness and hopelessness on the rise in recent years." (*Id.* § 1, subd. (f).) The Legislature concluded: "For these reasons, it is essential that California act to require that social media platforms obtain parental consent before exposing

children and adolescents to harmful and addictive social media features." (*Id*. § 1, subd. (g).) The Act addresses this issue by requiring operators of addictive internet-based services and applications to obtain verifiable parental consent before providing an addictive feed or sending specified notifications to a user unless the operator has actual knowledge that the user is not a minor or has made a reasonable determination that the user is not a minor. This requirement gives parents the necessary tools to make decisions about whether specific social media features are appropriate for their children.

The Act directs the Attorney General to adopt regulations to further the purposes of the Act, including regulations regarding age assurance and parental consent. (Health & Saf. Code, § 27006, subd. (b).) Section IV sets forth the purpose and rationale for why these regulations are reasonably necessary to further the purposes of the Act, as well as their anticipated benefits. Finally, it identifies the technical, theoretical, or empirical studies, reports, or similar documents relied upon in proposing the regulations and reasonable alternatives considered

BENEFITS ANTICIPATED FROM REGULATORY ACTION

The regulations will benefit California by providing clear guidance regarding compliance with the Act. By providing clarity and specificity to operators on how to make a reasonable determination that a user is not a minor and on how to obtain verifiable parental consent, these regulations will make it easier for operators to comply with the Act and better protect Californian children and adolescents from the numerous harms identified by the Legislature in its legislative findings. These regulations give minors the opportunity to decide whether they want the covered features and whether These regulations enable minors to make an informed decision about whether they want their parents to know that they want those covered features. By providing operators with flexibility in choosing the age assurance methods they deploy and by allowing operators the opportunity to utilize new methods as technologies emerge, these regulations encourage innovation. By operationalizing the Act's purpose of protecting children from social media addiction, and by encouraging innovation, these regulations will significantly benefit California.

SPECIFIC PURPOSE AND NECESSITY OF EACH SECTION

Article 1. General Provisions

§ 550. Title and Scope.

This regulation sets forth the title and scope for these regulations. The regulation is necessary because Health and Safety Code section 27006, subdivision (b), requires the Attorney General to establish rules and procedures to further the purposes of the Act.

Subdivision (a) provides that Chapter 5.5 shall be known as the "Protecting Our Kids from Social Media Addiction Act Regulations" and shall be referred throughout the Chapter as "these regulations." It also provides that these regulations govern compliance with the Act and do not limit any other rights that users may have. The purpose of this regulation is to establish the scope of the new chapter. It is necessary to identify the title and the shorthand "these regulations" and

to explain the scope of these regulations. Use of the phrase "these regulations" makes these regulations more concise, readable, and clear. The basis for subdivision (a) is Health and Safety Code, section 27006, subdivision (b), which provides that the Attorney General shall adopt regulations to further the purposes of the Act. In addition, Health and Safety Code section 27004, subdivision (c), provides that the protections provided by the Act are in addition to those provided by any other applicable law. Subdivision (a) is necessary to make clear that these regulations, which further the purposes of the Act, also do not limit other protections and rights that users may have under other applicable laws.

Subdivision (b) provides that a violation of these regulations shall constitute a violation of the Act and be subject to the remedies provided for therein. The purpose of this regulation is to identify the relationship between the Act and these regulations. It is necessary to clarify that these regulations are an extension of the Act and thus subject to the Act's enforcement provisions and remedies. The basis for the regulation is Health and Safety Code section 27006, subdivision (a), which provides that the Act may be enforced by the Attorney General, and section 27006, subdivision (b), which provides that the Attorney General shall adopt regulations to further the purposes of the Act.

§ 551. Definitions.

This regulation sets forth the definitions for these regulations. The regulation is necessary because Health and Safety Code section 27006, subdivision (b), requires the Attorney General to establish rules and procedures to further the purposes of the Act.

Subdivisions (a) through (g) of this section define terms used throughout these regulations. It is necessary to define these terms because they could have multiple meanings depending on the context of their usage. Defining the terms clarifies the meaning of these regulations and helps eliminate any misunderstandings or confusion between the Attorney General and the public. It assists businesses in implementing the law, as well as these regulations, and thereby increases the likelihood that the public will enjoy the benefits of the rights provided by the Act.

Subdivision (a) establishes that "addictive internet-based service or application" has the meaning set forth in Health and Safety Code section 27000.5. The purpose of defining this term is to provide clarity and avoid confusion that may result from different understandings of the term. This term is defined to have the identical meaning as that used by the Act. Defining this term provides clarity and guidance that an operator of an addictive internet-based service or application, as defined in the Act, must comply with these regulations before sending notifications to a user during the hours specified in the Act. Incorporating by reference the Act's definition of this term rather than repeating that language in its entirety makes these regulations more concise, readable, and clear.

Subdivision (b) establishes that "addictive feed" has the meaning set forth in Health and Safety Code section 27000.5. The purpose of defining this term is to provide clarity and avoid confusion that may result from different understandings of the term. This term is defined to have the identical meaning as that used by the Act. Defining this term provides clarity and guidance that an operator must comply with these regulations before providing a user an addictive feed, as

defined by the Act. Incorporating by reference the Act's definition of this term rather than repeating that language in its entirety makes these regulations more concise, readable, and clear.

Subdivision (c) establishes that "covered features" means either of the following: (1) addictive feed, as defined in Health and Safety Code section 27000.5, subdivision (a); or (2) notifications sent by an operator of an addictive internet-based service or application, as defined in Health and Safety Code section 27000.5, during the hours specified in Health and Safety Code section 27002, subdivision (a). The purpose of this term is to provide clarity to these regulations and to make these regulations more readable. Defining this term provides clarity and guidance that an operator must comply with these regulations before providing a user such addictive feeds or notifications. Because these regulations require operators to take the same measures before providing either an addictive feed or a notification as described in this definition, a definition including both statutory references reduces repetition and makes these regulations more concise, readable, and clear.

Subdivision (d) establishes that "minor" has the meaning set forth in Health and Safety Code section 27000.5. The purpose of defining this term is to provide clarity and avoid confusion that may result from different understandings of the term. This term is defined to have the identical meaning as that used by the Act. This definition is necessary because it provides greater clarity and guidance regarding a term that is used throughout these regulations, including regulations regarding how an operator must make a reasonable determination that a user is not a minor and obtain parental consent to provide covered features to minors. Incorporating by reference the Act's definition of this term rather than repeating that language in its entirety makes these regulations more concise, readable, and clear.

Subdivision (e) establishes that "operator" has the meaning set forth in Health and Safety Code section 27000.5. The purpose of defining this term is to provide clarity and avoid confusion that may result from different understandings of the term. This term is defined to have the identical meaning as that used by the Act. This definition is necessary because it provides greater clarity and guidance regarding a term that is used throughout these regulations, including regarding to whom these regulations apply. Incorporating by reference the Act's definition of this term rather than repeating that language in its entirety makes these regulations more concise, readable, and clear.

Subdivision (f) establishes that "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. This definition is necessary because Health and Safety Code section 27000.5, subdivision (f), defines the term "parent" as meaning a "parent or guardian, including as defined in regulations promulgated pursuant to this chapter." The purpose of defining this term is to provide operators with additional clarity on the relationships an individual must have with a user in order to provide verifiable parental consent as described in Article 3 of these regulations. This definition is consistent with other California laws that define "parent," including California Education Code section 56028. Furthermore, this definition is necessary to avoid any confusion that may result from different understandings of the term.

Subdivision (g) establishes that "user" has the meaning set forth in Health and Safety Code section 27000.5. The purpose of defining this term is to provide clarity and avoid confusion that may result from different understandings of the term. This term is defined to have the identical meaning as that used by the Act. This definition is necessary because it provides greater clarity and guidance regarding a term that is used throughout these regulations. Incorporating by reference the Act's definition of this term rather than repeating that language in its entirety makes these regulations more concise, readable, and clear.

Article 2. Reasonable Determination That the User is Not a Minor

§ 560. Actual Knowledge.

This regulation sets forth how an operator should respond when it has actual knowledge relating to a user's age. The regulation is necessary because Health and Safety Code sections 27001 and 27002 prohibit an operator from providing covered features if the operator has actual knowledge that the user is a minor.

Subdivision (a) provides that 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. The purpose of the regulation is to provide clarity and guidance regarding what measures an operator must take if it has or is deemed to have actual knowledge that a user is a minor. The regulation is necessary to make clear that there is no need or reason for an operator to take additional measures to reasonably determine whether a user is a minor if the operator already has actual knowledge that the user is a minor. The regulation thus reduces the burden on operators. The regulation is also necessary to make clear that a signal pursuant to the Digital Age Assurance Act that a user is under 18 years of age can constitute actual knowledge of age for the purposes of these regulations. The Digital Age Assurance Act provides a mechanism for an operator to be deemed to have actual knowledge of the age range of the user via a digital signal. Specifically, Civil Code section 1798.501, subdivision (b)(2), provides that receiving this digital signal constitutes actual knowledge of the age range of the user to whom that signal pertains, across all platforms of the application and points of access of the application, except that the entity shall not willfully disregard internal clear and convincing information that indicates a user's age is different. Thus, an operator that receives a signal pursuant to the Digital Age Assurance Act that a user is under 18 years of age, and that has knowledge that the user is located in California, must not provide covered features unless it obtains verifiable parental consent. This regulation furthers the purposes of the Act, which include protecting minors from covered features in the absence of verifiable parental consent.

Subdivision (b) provides that 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 covered features. The purpose of the regulation is to provide clarity and guidance regarding what measures an operator must take if it has actual knowledge that a user is not a minor. The regulation is necessary to make clear that there is no need or reason for an operator to take additional measures before

providing covered features if the operator already has actual knowledge that the user is not a minor. The regulation thus reduces the burden on operators. The regulation is also necessary to make clear that a signal pursuant to the Digital Age Assurance Act that a user is over 18 years of age can constitute actual knowledge for the purposes of these regulations unless the operator has clear and convincing information that indicates that the user is under 18 years of age. The Digital Age Assurance Act provides a mechanism for an operator to be deemed to have actual knowledge of the age range of the user via a digital signal. Specifically, Civil Code section 1798.501, subdivision (b)(2) provides that receiving this digital signal constitutes actual knowledge of the age range of the user to whom that signal pertains, across all platforms of the application and points of access of the application, except that the entity shall not willfully disregard internal clear and convincing information that indicates a user's age is different. This regulation makes clear to operators that they may rely on a signal pursuant to the Digital Age Assurance Act so long as the operator does not have clear and convincing information that indicates that the user is under 18 years of age. This section furthers the purposes of the Act by adding clarity to these regulations, reducing the burden on operators, and efficiently enabling operators to provide adult users with covered features.

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

This regulation sets forth the requirements that an operator must follow when making a reasonable determination that a user is not a minor. The regulation is necessary because Health and Safety Code section 27001, subdivision (a)(1), requires an operator to reasonably determine that a user is not a minor before it may provide an addictive feed to the user, and Health and Safety Code section 27002, subdivision (a)(2), requires an operator to reasonably determine that a user is not a minor before it may provide notifications at certain hours to a user. Both provisions state that an operator's reasonable determination that a user is not a minor shall be made "including pursuant to regulations promulgated by the Attorney General." (Health & Saf. Code, §§ 27001, subd. (a)(1)(B), 27002, subd. (a)(2).)

Subdivision (a) requires an operator to make a reasonable determination that a user is not a minor by using one or more commercially reasonable and technically feasible age assurance methods. Subdivision (a) also provides examples of age assurance methods that can be used to make a reasonable determination that a user is not a minor.

This subdivision is necessary to provide guidance on what types of age assurance methods can be used to make a reasonable determination of whether or not a user is a minor. By listing these methods as examples, rather than requirements, this subdivision provides operators with flexibility to innovate in this space and allows them to use commercially reasonable and technically feasible age assurance methods that are appropriate or their use cases. The examples provided in subdivision (a)(1) through subdivision (a)(4) are age assurance methods that can yield a reasonable determination that a user is not a minor. Subdivision (a)(5) does not identify a specific age assurance method but rather states that a method that satisfies the framework set forth by the International Standards Organization's ISO/IEC 275666: "Information security, cybersecurity and privacy protection—Age assurance systems" may yield a reasonable determination that a user is not a minor. This underscores operators' flexibility in choosing age

assurance methods and allows the opportunity to utilize methods that are not yet technologically possible to be developed in the future.

Subdivision (b) requires that the age assurance method 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. The reasonableness of an operator's determination will depend on a number of factors, but one main factor is whether the method, as applied, yields accurate results. Using empirical data to measure accuracy tests an age assurance method's effectiveness in identifying users under the age of 18, including comparing the accuracy of different age assurance methods against each other, is a sound approach to evaluating an age assurance method's effectiveness. This section is necessary so that operators use a data-driven approach when evaluating whether the age assurance methods they are using are reasonably effective.

Subdivision (c) requires an operator to publish and maintain on its website a report describing the measures it takes to reasonably determine that a user is not a minor. Section 561 provides operators with a significant amount of discretion and flexibility to select a workable age assurance method while setting a baseline requirement that the method result in a reasonable determination that a user is not a minor. A publicly available report describing the information required in subdivisions (c)(1) through (c)(4) is necessary to provide transparency and show that an operator's determinations about age are reasonable. This report is necessary to provide the public with sufficient information to decide whether or not they wish to engage with an operator's age assurance process. Additionally, the report is necessary to increase regulatory efficiency by providing key information to assess whether operators are complying with the Act. The subdivisions discussed below set forth in further detail the information an operator must furnish in their report and offer additional guidance to operators by providing illustrative examples of the information an operator could include in the report.

Subdivision (c)(1) requires an operator to describe the age assurance method(s) used, the data relied upon, and how that data is collected. This subdivision is necessary because requiring a description of the methods used, the data relied upon, and how the data is collected provides important information regarding whether an operator is using an age assurance method and data together in a way that is likely to yield a reasonable determination that a user is not a minor. This information is also critical in giving users and their parents the information they need to make decisions about participating in an age assurance method.

Subdivision (c)(2) requires an operator to include its basis for relying on the data it describes pursuant to subdivision (c)(1). This subdivision is necessary to clarify that an operator must be able to articulate to the public their basis for relying on the data used for age assurance. To yield a reasonable age determination, operators must have both an effective age assurance method and data that can be relied upon in applying that method. Requiring an operator to explain its basis for relying on the data used in its age assurance method is necessary to assess whether that data, as used by the operator, is likely to yield a reasonable determination that a user is not a minor.

Subdivision (c)(3) requires an operator to explain how the operator's application of the age assurance method(s) yields a reasonable determination that a user is not a minor. This

subdivision is necessary to clarify that an operator is responsible for deploying an age assurance method will yield a reasonable determination that a user is not a minor. Regardless of the soundness of an age assurance method or the integrity of data being inputted, a failure to correctly use the method will negatively impact accuracy. This section is necessary to make sure operators know that they cannot deploy an ineffective iteration of an age assurance method or ineffectively administer that method such that it undermines the integrity of the age assurance method's results.

Subdivision (c)(4) requires an operator to provide a summary of the measures taken to ensure the accuracy of the age assurance methods it uses. This subdivision is necessary because the reasonableness of an age determination is based on both the determinations themselves and on the measures taken to ensure that the methods used to reach those determinations are likely to yield accurate results. Operators have discretion on what measures they take but must, at a minimum, satisfy the requirements in subdivision (c)(4)(i) through subdivision (c)(4)(v) and describe how they have done so.

Subdivision (c)(4)(i) requires an operator to describe the measures it takes pursuant to section 565 to account for circumvention, fraud, or. This subdivision is necessary because a method that is easily circumvented or susceptible to fraud or misuse is unlikely to result in reasonable determinations. Requiring operators to summarize the measures they take to account for circumvention, fraud, or misuse provides transparency as to how operators have accounted for and are taking measures to prevent these issues, as required by section 565.

Subdivision (c)(4)(ii) requires an operator to describe the measures it takes to avoid the use of low-quality or falsified data. This subdivision is necessary because even with the most accurate age assurance method, low-quality or falsified data is likely to result in an incorrect or inconclusive determination rather than a reasonable age determination. Requiring operators to summarize the measures they take to prevent the use of low-quality or falsified data provides transparency as to how the operators have accounted for and are taking measures to address these issues.

Subdivision (c)(4)(iii) requires an operator to provide a description of how each age assurance method used is testable and how the operator confirms that it is reasonably effective and measurably consistent, as required by Section 561, subdivision (b). As discussed in Section 561, subsection (b) operators must use a data-driven approach when evaluating whether their age assurance methods are reasonably effective. Requiring operators to describe the testability, reasonable effectiveness, and measurable consistency of their age assurance methods provides transparency as to how operators are using an empirical approach to make reasonable determinations that a user is not a minor.

Subdivision (c)(4)(iv) requires an operator to include a quantitative description of its age assurance methods' effectiveness at correctly identifying minors as being under 18 years of age. This information is critical in determining whether the age assurance method the operator is using is reasonably effective. Requiring operators to include this information in their reports provides transparency as to how operators are testing their age assurance methods for accuracy and gathering empirical information to ensure that their age determinations are reasonable.

Subdivision (c)(4)(v) requires an operator to describe how and how often the operator tests, audits, and reviews each age assurance method used. This subdivision is necessary to provide transparency as to how operators are regularly evaluating the efficacy of the age assurance methods that they are using. This subdivision provides clarity that operators must ensure, on an ongoing basis, that the age assurance methods they use yield reasonable age determinations. Requiring operators to describe how and how often they test, audit, and review their age assurance methods is the most effective and efficient way to promote transparency, accountability, and compliance with these regulations.

Subdivision (d) states that operators may identify any other state, federal, or international frameworks that the operator believes their age assurance method complies with. Making users and regulators aware of an operator's compliance with age assurance requirements outside of California is useful in determining whether or not an operator's age assurance method yields a reasonable determination as required by the Act.

Subdivision (e) sets out collection and handling requirements for data collected for the purpose of complying with these regulations. The Attorney General recognizes that operators must collect data on users in order to make a reasonable age determination. This section is necessary to clarify that operators must treat this data in a way that is consistent with the purposes of the Act and for no other purposes. This section is also necessary because Health and Safety Code section 27001, subdivision (b), expressly limits the information collected for compliance with the Act, and because it furthers the purposes of the Act to protect the privacy and security of consumer data from other unintended uses or potential abuses.

Subdivision (e)(1) requires an operator to collect no more data than what is necessary to comply with the requirements of these regulations. This subdivision is necessary to limit operators to collecting the minimum amount of data to make reasonable age determinations and to make clear that nothing in these regulations may be construed to allow operators to collect additional or unnecessary data on users. Limiting the amount of data benefits both consumers and operators because it reduces the impact and liability associated with security breaches and increases trust that data is only used for specific purposes and not for further monetization or commercialization. This subdivision is also necessary to manage consumers' expectations on the limitations for how much data can be used as required by the Act.

Subdivision (e)(2) requires an operator to use the data collected only for the purpose of complying with the requirements of these regulations and for no other purpose. This subdivision is necessary to limit operators to collecting the minimum amount of data to make reasonable age determinations and to make clear that nothing in these regulations may be construed to allow operators to collect additional or unnecessary data on users. Data minimization serves important functions, such as by reducing the risk that unintended persons or entities will access personal information and by limiting the circulation of information about a user that a user does not want to be shared.

Subdivision (e)(3) requires an operator to collect and store the data using industry-standard security measures and as required by law. This subdivision is necessary to clarify that nothing in

these regulations may be construed to allow operators to fail to meet industry standards or comply with the law when collecting or using a user's data to make an age determination.

Subdivision (e)(4) requires an operator to hold the data collected for the minimum amount of time necessary to comply with this section and to immediately delete the data after it has done so. This subdivision is necessary to limit operators from storing or using data beyond what is necessary to make reasonable age determinations and to clarify that nothing in these regulations may be construed to allow operators to store a user's data for longer than is necessary to comply with this section.

§ 562. Government-Issued Identification.

This regulation provides that an operator must not require as the sole method of age assurance that a user provide government-issued identification. The regulation is necessary so that at least one age assurance method is available to individuals who do not have access to or do not want to provide government-issued identification. Health and Safety Code section 27006, subdivision (b), requires the Attorney General to solicit public comment regarding the impact that any of these regulations might have based on the nondiscrimination characteristics set forth in Section 51 of the Civil Code or any other applicable law. Prior to entering the formal rulemaking process, the Attorney General held a public forum and solicited comment from the public. Multiple comments directly addressed concerns that requiring users or parents to provide a government-issued identification would have a discriminatory impact. There are also privacy concerns with requiring users to provide government-issued identification. Not all users have government-issued identification. Requiring this type of documentation could lead to additional inferences or conclusions about a person. This type of documentation may reveal more personal information than necessary or required to determine a person's age, such as an individual's address correlating to their home. Some consumers may also not want to provide their government-issued identification to specific companies, including online platforms, for personal reasons or because of the potential for that data to be compromised in a security breach. This subdivision therefore aims to reduce the dissemination of unnecessary information that does not advance the purpose or goals of the Act. Additionally, there are multiple, alternative age assurance methods that do not rely on government-issued identification. Allowing operators to require that a user provide government-issued identification could hinder operators from providing a large portion of California's adult population with covered features, which does not serve the purposes of the Act.

§ 563. Unreasonable Determination.

This regulation provides guidance and clarity regarding what constitutes a reasonable determination that a user is not a minor by setting forth categories that do not constitute reasonable determinations for purposes of the Act and these regulations. The regulation is necessary because the Act requires operators to make a reasonable determination that a user is not a minor or to obtain verifiable parental consent before providing covered features. These regulations provide operators with flexibility and discretion in how to make a reasonable determination regarding minor status. By setting forth methods that do not result in a reasonable determination, this regulation provides guidance to operators as they decide what age assurance

methods to use and specific examples to illustrate methods that would not comply with the Act. The categories enumerated in section 563 are not exhaustive, and an operator must still ensure that its age assurance methods result in reasonable determinations of minor status.

Subdivision (a)(1) states that an operator does not reasonably determine that a user is not a minor when the operator relies on self-declaration that the user is not a minor. This section is necessary because minors may easily self-declare that they are not minors, with few if any meaningful checks or guards against false self-declarations, which would frustrate the purposes of the Act. The Attorney General has reviewed studies that indicate that users self-declaring as adults have not yielded accurate results and that without additional information or analysis, self-declaration is ineffective as a method of determining that a user is not a minor. Therefore, methods that rely on self-declaration do not result in a reasonable determination that a user is not a minor.

Subdivision (a)(2) states that an operator does not reasonably determine that a user is not a minor when the operator relies on contractual restrictions or terms regarding the use of the operator's services. This section is necessary because minors may easily agree to such terms, with few if any meaningful measures to detect or guard against breach, which would frustrate the purposes of the Act. The Attorney General has reviewed studies that indicate that such terms and restrictions, including contractual terms that restrict use of a service based on age, are not an effective method of determining a user's age. For example, studies have shown that millions of minors under the age of 13 use services for which access is contractually restricted to users 13 years or older. Therefore, methods that rely on contractual restrictions or terms are ineffective as a method of determining that a user is not a minor and do not result in a reasonable determination that a user is not a minor.

Subdivision (a)(3) states that an operator does not reasonably determine that a user is not a minor when the operator relies on online payment methods that are available to minors. This section is necessary because payment methods that are available to minors do not provide sufficient checks or guards against use by minors, and depending on such methods to determine that a minor is not a user would frustrate the purposes of the Act. Operators may not rely on data from payment methods that are accessible by minors because it would make reliance on online payment methods ineffective as a method of determining that a user is not a minor. Therefore, methods that rely on such payment methods do not result in a reasonable determination that a user is not a minor.

Subdivision (a)(4) states that an operator does not reasonably determine that a user is not a minor when the operator relies on an age assurance method that uses biometrics without taking reasonable measures to mitigate the risks of user circumvention through use of a static image, pre-recorded video, digitally altered face or image, or other means. This subdivision is necessary because without reasonable measures to mitigate these risks, minors may easily circumvent the age assurance method, which would frustrate the purposes of the Act. This section is also necessary to make clear that operators bear the responsibility for reasonably mitigating risks associated with the age assurance methods they use. This section is consistent with section 565, which makes clear that an operator must take reasonable measures to prevent circumvention, fraud, or misuse of methods to determine whether a user is a minor, including that an operator using biometric facial analysis must ensure that the face presented is a live person rather than a

photo or pre-recorded video. Advances in technology will necessarily change the nature of attempts at circumvention, fraud, and misuse. This makes use of biometrics without taking reasonable measures to mitigate against the risks of circumvention ineffective as a method of determining that a user is not a minor. Therefore, using these methods without taking reasonable mitigation measures does not result in a reasonable determination that a user is not a minor.

Subdivision (a)(5) states that an operator does not reasonably determine that a user is not a minor when the operator relies on age assurance methods that have known or documented risks related to the submission of low-quality or incomplete documents, images, video, or other data from a user, if the operator relies on such methods without taking reasonable measures to mitigate those risks. These risks are likely to impact the accuracy of an age determination. Unless an operator takes reasonable mitigation measures, minors may easily circumvent age assurance methods that have these known or documented risks, which would frustrate the purposes of the Act. This subdivision is necessary to make clear that operators bear the responsibility for mitigating risks associated with the age assurance methods they use. Use of age assurance methods that have known or documented risks without reasonable measures to mitigate those risks is ineffective as a method of determining that a user is not a minor. Therefore, using these methods without taking reasonable mitigation measures does not result in a reasonable determination that a user is not a minor.

Subdivision (a)(6) states that an operator does not reasonably determine that a user is not a minor when the operator relies on an age assurance method that has known or documented risks related to varying error rates across demographic groups other than age, if the operator relies on such a method without taking reasonable measures to mitigate against those risks. This subdivision provides guidance that 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 group, the operator must take mitigation 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. This regulation is necessary under Health and Safety Code section 27006, which provides that in promulgating regulations the Attorney General shall consider the impact that any regulation might have on the nondiscrimination characteristics set forth in Section 51 of the Civil Code. Use of assurance methods that have known or documented risks related to varying error rates across demographic groups other than age without taking reasonable measures to mitigate against those risks is ineffective as a method of determining that a user is not a minor. Therefore, using these methods without taking reasonable mitigation measures does not result in a reasonable determination that a user is not a minor.

Subdivision (a)(7) states that an operator does not reasonably determine that a user is not a minor when the operator relies on an age assurance method that has substantial known or documented risks other than those covered in subdivision (a)(5) and subdivision (a)(6), if the operator relies on such a method without taking reasonable measures to mitigate those risks. Unless an operator takes reasonable mitigation measures, minors may circumvent age assurance methods that have substantial known or documented risks, which would frustrate the purposes of the Act. These regulations provide operators with flexibility and discretion in how to make a reasonable determination regarding minor status, and this subdivision is necessary to make clear

that operators bear the responsibility for mitigating risks associated with the age assurance methods they choose to use. Use of age assurance methods that have known or documented risks without reasonable measures to mitigate those risks is ineffective as a method of determining that a user is not a minor. Therefore, using these methods without taking reasonable mitigation measures does not result in a reasonable determination that a user is not a minor.

Subdivision (a)(8) states that an operator does not reasonably determine that a user is not a minor when the operator 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. This subdivision is necessary to make clear that regardless of the method an operator uses, its determination of a user's minor status must be reasonable in light of all information known to the operator. This subdivision is necessary because allowing operators to ignore information indicating that a user may be a minor would frustrate the purposes of the Act by unreasonably allowing operators to provide minors covered features. The subdivision does not require operators to be bound by any single piece of information known about a user. Instead, it states only that a determination must be reasonable based on all information about a user known to the operator, not just based on the age-assurance method used. The subdivision further makes clear that only information known to the operator at the time the determination is made is relevant in determining reasonableness. Failing to take into consideration all information about a user known to an operator at the time an operator makes a determination does not result in a reasonable determination that a user is not a minor.

Subdivision (b) states that an operator does not reasonably determine that a user is not a minor when it relies on an age assurance method that yields an inconclusive result. This section is necessary to make sure that operators know that they cannot provide minors covered features without verifiable parental consent simply because the age assurance method employed could not reach a conclusive determination of whether or not the user was a minor. This section is necessary to further the purposes of the Act because Health and Safety Code sections 27001 and 27002 prohibit operators from providing covered features to a user unless it determines that the user is not a minor or obtains verified parental consent. This section is also necessary to distinguish these regulations from other jurisdictions' laws or frameworks that require a different approach when an age assurance method yields an inconclusive result and may not comply with the requirements of the Act.

§ 564. Appeals Process.

This regulation requires that an operator 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. This regulation is necessary in the event where an individual who is at least 18 years of age is determined by the operator to be a minor, or for whom the determination process resulted in an inconclusive determination. This regulation provides guidance and clarity to operators regarding how to resolve these situations, and provides a process for adult users who may be incorrectly determined to be a minor and wish to correct that determination.

Subdivisions (a)-(d) set out the minimum requirements that operators must meet to satisfy this section.

Subdivision (a) requires an operator to offer one or more methods for a user to submit additional information demonstrating that the user is not a minor. This requirement is necessary because operators will likely need additional information in order to review their earlier determination and potentially make a new determination. The most effective and efficient means for obtaining this information is a process by which users may submit additional information; otherwise, an appeals process is not likely to be effective.

Subdivision (b) requires an operator to evaluate all the information submitted by the user. This requirement is necessary because an appeals process can only be effective if an operator conducts an evaluation of the submitted information. This requirement is necessary to make clear that when a user appeals a decision, operators must apply the appeals process they put in place and review information to determine whether to change their previous determination.

Subdivision (c) requires an operator to determine in good faith whether the information submitted provides a reasonable basis to change their previous determination. By requiring good faith and a reasonable basis for changing an operator's previous determination, the regulation is necessary to prevent operators from summarily denying or granting appeals, which would render any appeals process ineffective, be contrary to the purposes of the Act, and could lead to circumvention, fraud, and misuse.

Subdivision (d) requires an operator to provide a written notice to the user of the decision it made on the appeal. The notice must provide an explanation of the basis of the operator's decision. This requirement is necessary for an effective appeals process, and to notify users of the operator's decision and to enable them to understand why the operator made the decision it did.

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

This regulation requires that an operator (1) take reasonable measures to prevent circumvention, fraud, or misuse of methods used by the operator to determine whether the user is a minor, and (2) maintain and document this protocol. An operator must consider how advances in technology can lead to emerging forms of circumvention, including how users can conceal whether they are located in California. This regulation is necessary because any method of reasonably determining whether the user is not a minor will have some risk of circumvention, fraud, or misuse, and an operator is in the best position to assess how users and third parties may interact with its method to do so and how to prevent circumvention, fraud, and misuse of the method. This regulation furthers the purposes of the Act, which includes protecting minors from the harms of covered features, by making clear that operators must take reasonable measures to prevent against attempts to thwart those protections. By requiring operators to maintain and document a protocol for doing so, the regulation helps ensure that an operator has a systematic process to prevent circumvention, fraud, or misuse and to track emerging developments. The regulation explains that advances in technology will necessarily change the nature of attempts at circumvention, fraud, and misuse. This regulation makes clear that operators must monitor how developments in

technology will impact these attempts, including with respect to attempts to conceal the fact that a user is located in California. Examples in this regulation provide further clarity and guidance regarding reasonable measures an operator must take in specific situations. Operators using live biometric facial analysis to analyze real-time data must confirm that a face presented to a system is a live person to prevent circumvention of the live biometric facial analysis technology. Operators must consider geographic location information collected for other purposes, including marketing, commercialization of user engagement, or generating personalized content, when making a determination regarding whether the user is a minor because it would be unreasonable for operators to disregard that information for purposes of the Act while using it for commercial or other purposes.

§ 566. Consistency Across Points of Access.

This regulation provides that an operator with actual knowledge that a user is a minor or that reasonably determines that a user is a minor must apply this information to all points of access when providing covered features, including the operator's internet website, online service, online application, or mobile application. This regulation furthers the purposes of the Act, which include protecting minors from covered features unless verifiable parental consent is obtained, by ensuring that users known or determined to be minors cannot evade or circumvent this determination simply by accessing the platform from a different device or point of access, such as from a web browser instead of the operator's application. This regulation is necessary because it provides consistency in when an operator provides covered features across the user experience, including for minors who may access a platform from multiple devices or from a web browser instead of the operator's application. This regulation also seeks to clarify that the prohibitions related to covered features apply to the minor as opposed to the device or the way by which an operator's platform is accessed.

§ 567. Report or Information Indicating that a User is Not a Minor.

This regulation requires that an operator 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 that a user is a minor or that data was falsified regarding their age or location. The regulation also requires that the operator must (1) investigate and make a good-faith determination if the report or information provides a reasonable basis to change a prior determination that a user is not a minor, and (2) provide written notice to the user if it changes its previous determination that a user is not a minor, and the basis for that decision. This regulation is necessary to clarify that operators must evaluate potential errors, circumvention, fraud, or misuse brought to their attention indicating that a user is a minor, and to require that operators implement and maintain a process to respond to reports that they are providing a minor covered features without verifiable parental consent. This regulation furthers the Act's purpose of protecting minors from covered features unless verifiable parental consent is obtained. The purpose of this regulation is to require that when an operator receives a report or information that a user is a minor or falsified data regarding whether they are a minor, the operator takes reasonable measures to ensure that it does not provide covered features to a minor without parental consent. For example, an operator may make a reasonable determination that a user is not a minor that is inaccurate or based on falsified data, but if information is brought to their

attention that indicates the user is a minor, the operator cannot simply ignore that information. By requiring a good-faith determination of whether the information provides a reasonable basis to change a prior determination, the regulation provides clarity and guidance on operators' obligations to investigate and act on information brought to their attention. By requiring written notice to the user, this regulation ensures that users receive information regarding operators' decisions and an opportunity to use that information to decide next steps, such as accessing a platform without covered features or availing themselves of the appeal process as set forth in section 564 of these regulations.

Article 3. Verifiable Parental Consent

§ 570. Preliminary Requirements for Verifiable Parental Consent.

This regulation requires an operator to provide notice to, and obtain consent from, a user to seek verifiable parental consent. This regulation is necessary to further the purposes of the Act because it gives minors, the group the statute is intended to protect, the opportunity to decide whether they want the covered features and whether they want their parents to know that they want those covered features. Health and Safety Code section 27006, subdivision (c), requires the Attorney General to solicit public comment regarding the impact that any regulation might have based on the nondiscrimination characteristics set forth in applicable law. The Attorney General received comments expressing concern about the verifiable parental consent requirements of the Act giving parents or guardians of LGBTQ+ children a means to prevent their access to community or information. There was also concern expressed that LGBTQ+ children may not wish their parents or guardians to know about the platforms they use. By requiring operators to first obtain permission from minors before seeking parental consent, this section limits the risk that parents are informed by operators what platforms their child is visiting unless the child wishes their parents to know. This also allows operators to only make efforts to obtain verifiable parental consent for minors who want the covered features.

Subdivision (a) requires that prior to seeking verifiable parental consent, an operator must first provide the user with notice that the operator cannot legally provide minor users covered features without verifiable parental consent. This subdivision operationalizes Health and Safety Code section 27001, subdivision (b)(2) and section 27002, subdivisions (a)(1) and (a)(2). The purpose of section 570 of these regulations is to set forth preliminary requirements operators must follow before seeking verifiable parental consent. This regulation is necessary to further the purposes of the Act because it gives minors, the group the statute is intended to protect, the opportunity to decide whether they want the covered features and whether they want their parents to know that they want those covered features. This also allows operators to only make efforts to obtain verifiable parental consent for minors who want the features.

Subdivision (b) requires that an operator, prior to seeking verifiable parental consent, must first obtain consent from the user to request verifiable parental consent to provide covered features. This subdivision operationalizes the requirements under Health and Safety Code section 27001, subdivision (b)(2) and section 27002, subdivisions (a)(1) and (a)(2) that allow operators to provide covered features to minors only if the operator obtains verifiable parental consent. The purpose of this regulation is to set forth preliminary requirements and procedures operators must follow prior to seeking verifiable parental consent to provide minor users with covered features.

This regulation is necessary to further the purposes of the Act because it gives minors, the group the statute is intended to protect, the opportunity to make a decision about whether they want the covered features and whether they want their parents to know that they want those covered features This also allows operators to only make efforts to obtain verifiable parental consent for minors who want the features. This subdivision is necessary because it gives minors the choice of whether the operator should notify their parents that they want the covered features. In response to comments received during the preliminary rulemaking process regarding the impact that any regulation might have based on the nondiscrimination characteristics, the regulation reflects the concern that not every minor wants their parent involved in their online activity. This provision is also consistent with the legislative intent of the Act to limit the harmful effects of covered features on minors. It does so by making clear that if a minor does not seek to be provided with an operator's covered features, the operator cannot contact the parent, since not all minors may wish to be provided with covered features or to request consent from their parents to do so.

§ 571. Methods of Verifiable Parental Consent.

This regulation sets forth the requirements operators must follow when obtaining verifiable parental consent. This regulation is necessary to further the purposes of Health and Safety Code sections 27001 and 27002 because it provides guidance to operators on how to comply with the verifiable parental consent requirements of the Act. Rules related to verifiable parental consent are consistent with the Act's requirement that the Attorney General adopt regulations to further the purposes of the Act, including the express requirement to adopt regulations regarding parental consent in Health and Safety Code section 27006, subdivision (b).

Subdivision (a) requires an operator to provide the parent with notice at or prior to seeking verifiable parental consent. The notice must meet the requirements of Section 572. The operator must also offer the parent access to a method of verifiable parental consent as set forth in subdivisions (b) and (c) of this regulation. This subdivision is necessary to require operators to provide relevant information for parents so they can make decisions about whether to allow operators to provide their children with covered features. It is also necessary to clarify that the method by which parents may provide consent is reasonably calculated to ensure that the individual providing consent is a parent of the user, does not require the parent to furnish government-issued identification, and does not require the parent to create an account with the operator or make any purchase from the operator.

Subdivision (b) requires that the method used to obtain verifiable parental consent from a parent be reasonably calculated, in light of available technology, to ensure that the individual providing consent is a parent of the minor, such as the example methods for verifiable parental consent set forth in 16 C.F.R. § 312.5(b)(2). This subdivision is necessary to provide guidance to operators on how to verify that the individual providing parental consent is a parent of the user. The subdivision makes clear that methods compliant with the Children's Online Privacy Protection Rule may be used to obtain verifiable parental consent for purposes of the Act. The regulations for the Children's Online Privacy Protection Act (COPPA) have been tested and used for over 25 years. While COPPA is only applicable when operators have actual knowledge that the users are under the age of 13, this subdivision makes clear that operators can expand their use of COPPA-

compliant methods, for purposes of the Act, for users under the age of 18. Additionally, this subdivision provides operators with flexibility to adapt their methods for obtaining verifiable parental consent to emerging technologies that may go beyond the methods identified in 16 C.F.R. § 312.5(b)(2)(i)-(ix).

Subdivision (c) sets forth the requirements for obtaining verifiable parental consent and is necessary to provide guidance to operators on obtaining verifiable parental consent as required by the Act.

Subdivision (c)(1) requires that an operator provide at least one option that does not require the parent to create an account with the operator.

Subdivision (c)(2) requires that an operator provide at least one option that does not require the parent to purchase additional goods or services from the operator. These subdivisions are necessary because neither requiring a parent to create an account nor requiring the purchase of additional goods is necessary to provide verifiable parental consent. Furthermore, those requirements are not worth the net effect of potentially unfairly burdening or discriminating against individuals.

Subdivision (c)(3) requires that an operator provide at least one option for verifiable parental consent that does not require the parent to furnish government-issued identification, unless the covered operator collects or possesses that form of identification to comply with other laws, and obtains consent to use this identification for verifiable parental consent. Health and Safety Code section 27006, subdivision (b), requires the Attorney General to solicit public comment regarding the impact that any of these regulations might have based on the nondiscrimination characteristics set forth in Section 51 of the Civil Code or any other applicable law. Prior to entering the formal rulemaking process, the Attorney General held a public forum and solicited comment from the public. Multiple comments directly addressed concerns that requiring users or parents to provide a government-issued identification would have a discriminatory impact. There are also privacy concerns with requiring users to provide government-issued identification. Not all users have government-issued identification. Requiring this type of documentation could lead to additional inferences or conclusions about a person. This type of documentation may reveal more personal information than necessary or required to determine a person's age, such as an individual's address correlating to their home. Some consumers may also not want to provide their government-issued identification to specific companies, including online platforms, for personal reasons or because of the potential for that data to be compromised in a security breach. This subdivision therefore aims to reduce the dissemination of unnecessary information that does not advance the purpose or goals of the Act.

§ 572. Notice Requirements.

This regulation sets forth the requirements for the notices that operators must provide to parents and users before or when seeking verifiable parental consent. This regulation is necessary to further the purposes of Health and Safety Code sections 27001 and 27002 because parents and users must be provided with relevant information necessary to make the decisions afforded to them by the Act before they make those decisions. The notice requirements enable users the

opportunity to make a decision about whether they want the covered features and whether they want their parent to know that they want those features. This regulation requires operators to provide information so that parents can decide whether they want to permit operators to provide their children with covered features. This section further addresses concerns received during the preliminary rulemaking period regarding the impact that any regulation might have based on the nondiscrimination characteristics set forth in applicable law, including for LGBTQ+ children that may not wish their parents or guardians to know about the platforms they use. By requiring operators to provide minors with notice, this section seeks to give children and adolescents the opportunity to understand that their parent could be informed about what platforms they seek to visit before they agree to permit an operator to seek verifiable parental consent. This also allows operators to only take measures to obtain verifiable parental consent for minors who want the covered features.

Subdivision (a) sets forth requirements that apply to both the notice provided to users set forth in section 570, subdivision (b)(1), and the notice provided to parents set forth in section 570, subdivision (a).

Subdivision (a)(1) requires the notice to identify the internet website, online service, online application, or mobile application that offers covered features a minor seeks to access. This subdivision is necessary to give users and parents information identifying which site or account they are giving consent when a minor wants to access covered features. A user may have attempted to access multiple websites, services, or applications and so must be notified of the specific website, service, or application for which an operator seeks verifiable parental consent, so that the user can decide whether they want the covered features and whether they want their parent to know that they want those covered features. Similarly, a parent must know what website, service, or mobile application they are providing consent to for that consent to be effective. Because an operator may operate more than one website, service, or application, it is necessary that the notice identify the specific website, service, or application that the user seeks verifiable parental consent for these covered features.

Subdivision (a)(2) requires the notice to identify the minor's account, profile, and username, as applicable. This provision is necessary to allow the minor and parent to confirm that the account, profile, or username for which the operator seeks consent is the correct account, profile, and username.

Subdivision (a)(3) requires the notice to disclose, with equal prominence and in plain language that is understandable and accessible to the target audience, that California law does not allow the operator to provide covered features to a minor without verifiable parental consent, that the minor can access the platform without being provided covered features, and that a parent can revoke their consent at all times. It also requires the notice to describe how a parent may revoke their consent. This subdivision is necessary to provide users and parents with meaningful notice regarding the user's ability to access the operator's platform, the import of parental consent, and parents' ability to revoke consent, so that users and parents can understand and make decisions regarding consent. The subdivision makes clear that without verifiable parental consent, the operator cannot provide covered features but that the user is not precluded by this law from accessing the operator's platform generally or its other features. This reduces confusion about

how the law impacts users' interactions with platforms and may inform both a user's decision of whether to allow an operator to seek verifiable parental consent and a parent's decision of whether to consent to an operator providing their child covered features. The subdivision also makes clear that providing verifiable parental consent is not irrevocable and is necessary to inform parents on how they can revoke consent should they choose to do so.

Subdivision (b) sets forth additional information that must be disclosed in the notice provided to users set forth in section 570, subdivision (b)(1). It requires that the notice 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. It also requires the notice to describe how a user may revoke their consent. This subdivision is necessary to further the purposes of Health and Safety Code sections 27001 and 27002 because it explains the process for verifiable parental consent to minors, the group the statute is intended to protect. This subdivision is necessary to provide users meaningful notice regarding their ability to access the operator's platform, the import of providing consent, and the ability to revoke consent, so that users can make decisions regarding whether they want the covered features and whether they want their parents to know that they want those features.

§ 573. Revocation of Consent.

This regulation provides guidance to operators regarding the revocation of consent. This regulation is necessary because Health and Safety Code section 27006, subdivision (b) requires the Attorney General to establish rules and procedures to further the purposes of the Act, including the express requirement to adopt regulations regarding parental consent. This regulation is necessary to further the purposes of the Act by clarifying that the protections afforded minors are not one-time protections but rather are ongoing protections, and that parents and minors have the flexibility to change their decisions about whether an operator may provide covered features.

Subdivision (a) provides that a minor's consent for an operator to seek verifiable parental consent is revocable at any time. If a minor revokes consent, the operator shall immediately cease any further effort to obtain verifiable parental consent. An operator must provide minors with a simple, easily accessible mechanism to revoke consent. This section further addresses concerns received during the preliminary rulemaking period regarding the impact that any regulation might have based on the nondiscrimination characteristics set forth in applicable law, including for LGBTQ+ children that may not wish their parents or guardians to know about the platforms they use. This regulation is necessary to further the purposes of the Act by clarifying that the protections afforded minors are not one-time protections but rather that minors have the flexibility to change their decisions about whether an operator may seek verifiable parental consent. This provision is also consistent with the legislative intent of the Act to limit the harmful effects of covered features on minors by making clear that if a minor does not seek to be provided with covered features, a covered operator cannot contact the parent, since not all minors may wish to be provided with covered features or to request consent from their parents to do so.

Subdivision (b) provides that parental consent for an operator to provide covered features to a minor is revocable at any time. If a parent revokes consent, the operator shall immediately cease providing the minor covered features. An operator must provide parents with a simple, accessible mechanism to revoke consent for the minor to receive covered features. Health and Safety Code section 27006 requires the Attorney General to establish rules and procedures to further the purposes of the Act. This regulation is necessary to further the purposes of the Act by clarifying that the protections afforded minors are not one-time protections but rather are ongoing protections, and that parents have the flexibility to change their decisions about whether an operator may provide their child covered features. For example, a parent may not choose to provide consent for an operator to provide their 13-year-old child covered features but may feel differently when that same child turns 16 years of age. As another example, a parent may initially choose to allow an operator to provide their child with covered features but later revoke that consent if they determine those features are problematic for their child or that it would be better for their child to no longer have them.

Subdivision (c) requires that 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 revoke consent if it was not required to give consent. This subdivision is necessary to require that operators do not erect barriers to discourage users or parents from exercising their right to revoke consent or dissuade them from doing so. The regulation specifically prohibits operators from requiring a user or parent to interact with a live representative to revoke consent if they were not required to do so when providing consent. This provision is necessary because requiring interaction with a live representative to revoke consent can discourage people from exercising their right to revoke consent.

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

This regulation requires an operator to 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 mitigation 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. This regulation is necessary because Health and Safety Code section 27006, subdivision (b), requires the Attorney General to establish rules and procedures to further the purposes of the Act, including with respect to parental consent. The regulation is also necessary to further the purposes of the Act because the operator is likely in the best position to assess how users and third parties interact with a consent-flow method and take mitigation measures that are reasonable under the circumstances. This regulation does not require a specific protocol and instead provides operators with flexibility in determining how to prevent circumvention, fraud, and misuse of its method for verifiable parental consent. Unless an operator takes reasonable mitigation measures, minors may circumvent verifiable parental consent methods, which would frustrate the purposes of the Act. These regulations provide operators with flexibility and discretion in how to obtain verifiable parental consent, and this subdivision is necessary to make clear that operators bear the responsibility for mitigating risks

associated with the methods they choose to use. This subdivision provides further guidance that to satisfy this requirement, by way of example, an operator should be monitoring 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.

Article 4. Miscellaneous

§ 580. Other Laws.

This regulation provides that nothing in these regulations limits an operator's existing obligations to comply with the law and that nothing in these regulations requires an operator to provide covered features to users.

Subdivision (a) provides that nothing in these regulations limits an operator's existing obligations to comply with state and federal law, including data privacy laws. This regulation furthers the purposes of the Act because it provides clarity and guidance regarding the requirements of Health and Safety Code section 27001, subdivision (b), which states that information collected for the purpose of determining a user's age or verifying parental consent should not be used for any purpose other than compliance with the Act or with another applicable law, and should be deleted immediately except as necessary to comply with state or federal law. The regulation is also consistent with Health and Safety Code section 27004, subdivision (c), which states that the protections provided by the Act are in addition to any other protections under other applicable laws.

Subdivision (b) provides that nothing in these regulations shall be construed as requiring an operator to offer or provide covered features. The purpose of the regulation is to provide clear and straightforward guidance, and is necessary to prevent confusion, regarding an operator's obligations to provide users with covered features. Neither the Act nor these regulations require that an operator provide covered features. Health and Safety Code section 27001, subdivision (a), states only that it is unlawful for an operator of an addictive internet-based service or application to provide an addictive feed to a user unless certain requirements are met. Health and Safety Code section 27004, subdivision (a), states that an operator can choose not to provide services to minors entirely, which would necessarily include covered features. Additionally, Health and Safety Code section 27003, subdivision (b), states that the Act shall not be construed as preventing any action taken in good faith to restrict access to, or availability of, media. Similarly, while Health and Safety Code section 27001, subdivision (a)(2), prohibits operators from providing covered features to minors unless verifiable parental consent is obtained, the Act does not require operators to obtain verifiable parental consent. This regulation makes clear that nothing in the Act or these regulations imposes an affirmative obligation to offer or provide covered features.

§ 581. Severability.

This regulation provides that each provision of these regulations is severable from the remainder. This regulation is substantively identical to Health and Safety Code section 27007 and is intended to provide clarity that the same severability applicable to the Act is applicable to these

regulations. This regulation is necessary to ensure that if any regulation is held invalid, the remaining regulations, all of which further the purpose of the Act, remain operable and enforceable. Although these regulations contain cross-references and use defined terms that incorporate multiple concepts, the provisions of the proposed rule have been designed to work equally well separately or together, such that if any of the provisions is held invalid, the remaining provisions would continue to fulfill the purposes for which they were proposed.

ECONOMIC IMPACT ASSESSMENT/ANALYSIS

The Department concludes:

(1) It is unlikely that the proposal would create or eliminate jobs within the state because most businesses would obtain actual knowledge of the age range of users via a digital signal pursuant to the Digital Age Assurance Act. Businesses that may have to make a large number of reasonable determinations regarding users' age could require increased staffing to meet this need and may opt to reduce staffing to offset the cost of compliance.

(2) It is unlikely that the proposal would create new businesses or eliminate existing businesses within the state because the annual compliance costs associated with the proposed regulations represent an incremental increase of less than 0.5 percent of current annual compliance spending by operators. However, it is possible that businesses may be created to support implementation or eliminated if a business cannot afford the necessary compliance infrastructure.

(3) It is unlikely that the proposal would result in the expansion of businesses currently doing business within the state because many operators already employ some form of age assurance and parental consent verification to comply with other laws. However, it is possible that businesses in the age assurance and parental consent verification industries may experience expansion as a result of the proposed regulations due to increased demand for these services.

The Department also concludes that:

(1) The proposal would benefit the health and welfare of California residents because it implements the Act, which provides Californians with more control concerning when operators may provide addictive features to minors. By providing clear standards for the measures operators must take to comply with the Act, the proposed regulations reduce the transaction costs of compliance, increase legal certainty, and allow for more efficient implementation.

(2) The proposal would not benefit worker safety because it does not regulate worker safety standards.

(3) The proposal would not benefit the state's environment because it does not regulate any applicable environmental standards.

TECHNICAL, THEORETICAL, AND/OR EMPIRICAL STUDIES, REPORTS OR DOCUMENTS

Age Check Certification Scheme, Age Assurance Technology Trial Final Report (2025) <https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report> [as of Mar. 23, 2026].

Age Check Certification Scheme, Age Assurance Technology Trial Practice Statements - Age Verification, A-5.1.2 (2025) <https://ageassurance.com.au/wp-content/uploads/2025/06/Practice-Statements-for-Age-Verification.pdf> [as of Mar. 23, 2026].

Ariel Fox Johnson, Common Sense Media, *U.S. Age Assurance is Beginning to Come of Age: The Long Path Toward Protecting Children Online and Safeguarding Access to the Internet* (2024) < https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf> [as of Mar. 23, 2026].

Christine Marsden, *Age Verification Laws in the Era of Digital Privacy*, 10 Nat. Sec. L.J. 210 (2023) <https://www.nslj.org/wp-content/uploads/Marsden-10.2-v272.pdf> [as of Mar. 23, 2026].

Common Sense Media, A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health 30-31. (2024) <https://www.commonsensemedia.org/research/double-edged-sword-how-diverse-communities-of-young-people-think-about-social-media-and-mental-health> [as of Mar. 23, 2026].

Common Sense Media, Constant Companion: A Week in the Life of a Young Person's Smartphone Use (2023) <https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf> [as of Mar. 23, 2026].

Digital Wellness Lab, The Digital Wellness Lab's Pulse Survey – Adolescent Media Use: Attitudes, Effects, and Online Experiences (2022) <https://digitalwellnesslab.org/wp-content/uploads/Pulse-Survey_Adolescent-Attitudes-Effects-and-Experiences.pdf> [as of Mar. 23, 2026].

Rescorla et al., Knight-Georgetown Institute, Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations (2026) <https://kgi.georgetown.edu/wp-content/uploads/2026/01/Age_Assurance_Online_Technical-Assessment_Report_KGI.pdf>

Faverio et al., Pew Research Center, Teens, Social Media and AI Chatbots 2025. (2025) <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/> [as of Mar. 23, 2026].

Federal Trade Commission, Disclosures: How to Make Effective Disclosures in Digital Advertising 2013) <https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-

disclosures-information-about-online-advertising.pdf> [as of Mar. 23, 2026].

Federal Trade Commission, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services (2024) <https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf> [as of Mar. 23, 2026].

Federal Trade Commission., Staff Report: Bringing Dark Patterns to Light (2022) <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf> [as of Mar. 23, 2026].

Future of Privacy Forum, Unpacking Age Assurance: Technologies and Tradeoffs, Infographic, <https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf> [as of Mar. 23, 2026].

International Association of Privacy Professionals, U.S. State Privacy Legislation Tracker <https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf> [as of Mar. 23, 2026].

ISO/IEC 27566-1, Information security, cybersecurity and privacy protection—Age assurance systems—Part 1: Framework, First edition 2025-12 (2025) <https://www.iso.org/standard/88143.html> [as of Mar. 23, 2026].

Siegel et al., Future of Privacy Forum, *New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs* (2023) <https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs> [as of Mar. 23, 2026].

Hanaoka, et al., National Institute of Standards and Technology, Interagency Report: Face Analysis Technology Evaluation: Age Estimation and Verification, 12th Update (2025) <https://doi.org/10.6028/NIST.IR.8525> [as of Mar. 23, 2026].

Apthorpe et al., *Online Age Gating: An Interdisciplinary Evaluation* (2025) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937328> [as of Mar. 23, 2026].

Office of Communications ("Ofcom"), United Kingdom, Guidance on Highly Effective Age Assurance and Other Part 5 duties (2025) <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/guidance-on-highly-effective-age-assurance-and-other-part-5-duties.pdf> [as of Mar. 23, 2026].

Papadamou et al., Disturbed YouTube for Kids: Characterizing and Detecting Inappropriate Videos Targeting Young Children, Proceedings of the International AAAI Conference on Web and Social Media, volume 14, May, 2020, pages 522–533 <https://doi.org/10.1609/icwsm.v14i1.7320> [as of Mar. 23, 2026].

Panić et al., *Addressing Demographic Bias in Age Estimation Models through Optimized Dataset*

Composition, volume 12, No. 15, Mathematics (2024) <https://doi.org/10.3390/math12152358> [as of Mar. 23, 2026].

Stop Addictive Feeds Exploitation (SAFE) for Kids Act, Notice of Proposed Rulemaking, New York Register Volume XLVII, Issue 39, October 1, 2025. <https://ag.ny.gov/sites/default/files/regulatory-documents/safe-for-kids-act-nprm.pdf> [as of Mar. 23, 2026].

U.S. Surgeon Gen., U.S. Dept. Health & Human Services, Our Epidemic of Loneliness and Isolation, Advisory (2023) <https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf> [as of Mar. 23, 2026].

U.S. Surgeon Gen., U.S. Dept. Health & Human Services, Social Media and Youth Mental Health, Advisory (2023) <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf> [as of Mar. 23, 2026].

Verifymy White Paper, Innovative age assurance: Email address as the new benchmark for frictionless age estimation (2024) <https://verifymy.io/wp-content/uploads/2024/11/Verifymy-White-Paper-Innovative-age-assurance-Email-address-as-the-new-benchmark-for-frictionless-age-estimation.pdf> [as of Mar. 23, 2026].

Yoti Facial Age Estimation White Paper (2025) <https://cdn.aws.yoti.com/wp-content/uploads/2026/01/Yoti-Age-Estimation-White-Paper-July-2025-PUBLIC-v1.pdf> [as of Mar. 23, 2026].

EVIDENCE SUPPORTING DETERMINATION OF NO SIGNIFICANT STATEWIDE ADVERSE ECONOMIC IMPACT DIRECTLY AFFECTING BUSINESS

The Department has made an initial determination that the proposed action would not have a significant statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states.

The proposed regulations cover businesses with users in California, regardless of the business' location. Businesses without California users operate in different markets and therefore would not have a competitive advantage or disadvantage based on location. However, businesses operating outside of California, even with no California users, could incur compliance costs in other jurisdictions that regulate addictive feeds and notifications, such as New York and Utah. Additionally, California standards may become national standards because of the size of the California economy and because businesses may prefer to implement a uniform approach rather than differentiating their offerings. It is therefore unlikely that complying with the regulations will put any California businesses at a disadvantage.

REASONABLE ALTERNATIVES TO THE PROPOSED REGULATORY ACTION THAT WOULD LESSEN ANY ADVERSE IMPACT ON SMALL BUSINESS

Alternative: The Attorney General considered and declined to create exceptions to the Act, as

authorized by Health and Safety Code section 27006, subsection (b), that would exempt certain operators based on size as determined by their number of users, user engagement metrics, or financial metrics.

***Reasoning*:** The Attorney General determined that the Act's protections should apply regardless of the size of the operator. The Legislature identified addictive feeds and specified notifications as harmful for children and adolescents. The legislature did not articulate any basis in the statute or legislative history to conclude that those addictive feeds or notifications would be less harmful based on the size of an operator nor did it provide any other basis for exempting smaller operators.

REASONABLE ALTERNATIVES AND THE ATTORNEY GENERAL'S REASONS FOR REJECTING THOSE ALTERNATIVES

The Attorney General considered several alternatives in drafting the proposed regulations. In considering the following alternatives, the Attorney General sought to further the purposes of the Act and to balance the benefits to operators, users, and users' parents with the burdens to operators, users, and users' parents. The alternatives considered and rejected are below, along with the Attorney General's reasoning.

A. Section 561 – Reasonable Determination that the User is Not a Minor

Alternatives: The Attorney General considered and rejected, in relation to operators' obligation to make a reasonable determination that a user is not a minor, adopting specific accuracy-minimum requirements for the age-assurance methods used by an operator to make a reasonable determination that a user is not a minor.

Reasoning: The Attorney General determined that for the purposes of the Act, and after weighing the benefits and burdens to operators and users, that operators should have flexibility in how to make a reasonable determination that a user is not a minor. Although setting specific accuracy minimums could provide clarity as to whether a determination is reasonable, it is not the only way to do so. The proposed regulations set forth specific requirements for how an operator may make a reasonable determination while still providing operators with a significant amount of discretion and flexibility in selecting a workable approach that fits their particular circumstances. By requiring operators to publish and maintain a report describing the measures they take to reasonably determine that a user is not a minor, the proposed regulations allow operators to demonstrate the reasonableness of their determinations rather than prescribing specific quantitative results when conducting age assurance. The Attorney General also acknowledges that age assurance technology is rapidly evolving, and by not setting accuracy minimums, the proposed regulations provide flexibility to account for future technological developments. This flexibility furthers the Act's purpose of protecting minors.

B. Sections 563(a)(1) - (a)(3) – Unreasonable Determination

Alternatives: The Attorney General considered and rejected adopting regulations authorizing, as a reasonable determination that a user is not a minor, the methods set forth in sections 562(a)(1)

through 562(a)(3). After concluding that these methods do not result in reasonable determinations, the Attorney General considered and rejected remaining silent on these methods rather than expressly stating that determinations are not reasonable when an operator relies on these methods.

Reasoning: The Attorney General determined that a determination that a user is not a minor is not reasonable if the operator relies on the methods set forth in sections 562(a)(1) through 562(a)(3). Despite widespread use in other contexts, relying on a self-declaration that a user is not a minor or relying on a contractual restrictions or terms regarding the use of an operator's services are not reliable methods of determining that a user is not a minor. Research indicates millions of children under the age of 13 and millions more under the age of 18 have accounts and are active on platforms that use these methods of age assurance, showing that these methods are not generally effective and do not further the purpose of protecting minors from addictive features. An operator's determination that a user is not a minor that relies on online payment methods that are available to minors is also not reasonable. Because minors have access to those payment methods, those methods are unlikely to provide the operator with sufficient information about the user's age.

In considering these methods and concluding that an operator's determination is not reasonable if it relies on these methods, the Attorney General determined that including a regulation setting forth a non-exhaustive list of what constitutes unreasonable determinations would provide clarity and guidance to operators.

C. Section 565 – Circumvention, Fraud, or Misuse of Methods to Determine Minor Status.

Alternatives: The Attorney General considered and rejected, in relation to operators' obligation to take reasonable measures to prevent circumvention, fraud, or misuse of methods to determine minor status, adopting specific accuracy-minimum requirements for the age-assurance methods used by an operator to make a reasonable determination that a user is not a minor.

Reasoning: By requiring operators to maintain and document the protocol they adopt to prevent circumvention, fraud, or misuse, these regulations allow operators to demonstrate the reasonableness of their detection and prevention measures rather than prescribing specific quantitative results. The Attorney General also acknowledges that age assurance technology is rapidly evolving, and by not setting accuracy minimums, the proposed regulations provide flexibility to account for future technological developments. A specific accuracy requirement prescribed for this section today could soon fall short of industry standards. The standard that the operator take reasonable measures to detect and prevent circumvention, fraud, or misuse of the age assurance method provides flexibility to account for future technological improvements to mitigate these risks. This flexibility furthers the Act's purpose of protecting minors.

D. Section 572, subdivision (b) – Methods of Verifiable Parental Consent

Alternative: The Attorney General considered and rejected alternative approaches to how operators should obtain verifiable parental consent. Specifically, the Attorney General considered

and rejected deeming any method that complies with Children's Online Privacy Protection Act Rule ("COPPA Rule")(16 C.F.R. 312.5(b)) as satisfying the verifiable parental consent requirement. The Attorney General also considered and rejected departing from COPPA more substantially to create a new framework for obtaining verifiable parental consent.

Reasoning: The Attorney General determined that adopting the Children's Online Privacy Protection Act COPPA Rule's ("COPPA Rule") requirement that any method to obtain verifiable parental consent "must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent" (16 C.F.R. 312.5(b)(1)) likely reduces the operator's burden of implementation and furthers the purposes of the Act. The COPPA Rule's requirements have been widely adopted for online platforms directed to or having actual knowledge of users who are under the age of 13, and the Attorney General has determined that it would be less burdensome for operators to use methods that comply with the COPPA Rule to obtain verifiable parental consent for purposes of the Act rather than be subject to a new and separate set of requirements. However, the Attorney General determined that it was necessary to exclude two of the methods in 312, subdivision (b)(2)(i) through (ix) to satisfy the requirements of the Act: methods that require a parent to furnish government-issued identification unless the operator already obtained this from the parent to comply with other laws, and methods that require the parent to create and account or make a purchase with the operator. The Attorney General determined that operators must provide at least one method for verifiable parental consent other than these methods because of the privacy concerns with requiring users to provide government-issued identification or provide unnecessary information and the disparate impact they could have on vulnerable populations in California.

Furthermore, while the Attorney General considered restricting operators to only using the methods specifically listed in section 312.5, subdivision (b)(2)(i) through (ix), of the COPPA Rule, it determined that it is neither practical nor helpful in encouraging technological innovation to limit operators to a static list. Additionally, changing technology could render some of the methods in section 312.5, subdivision (b)(2)(i) through (ix) obsolete, which further underscores the importance of providing operators with the flexibility to beyond the specifically listed methods.

Performance Standard as Alternative:

The proposed regulations do not mandate the use of specific technologies or equipment or prescribe specific actions or procedures.