epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 8, 2026

Chair Jacquelyn Baginski
Rhode Island General Assembly
Rhode Island House Innovation Internet and Technology Committee
82 Smith Street
Providence, RI 02903

Dear Chair Baginski and Members of the Committee:

EPIC writes in support of the goals of H. 7632, the Rhode Island Age-Appropriate Design Code, but suggests amendments to make the bill more resistant to legal challenge.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization founded 30 years ago to protect privacy, freedom of expression, and democratic values in the information age.[1] In recent years, EPIC has been very involved in defending reasonable kids' online safety laws from the tech industry's First Amendment challenges. And we bring the expertise gained from our involvement in those legal challenges to help state legislators craft strong kids online safety laws that can withstand constitutional challenge.[2] EPIC supports the AADC approach and has published its own model AADC bill informed by our expertise in data protection, design regulation, the First Amendment, and Section 230.[3]

There is an urgent need for Rhode Island to pass the RI AADC. Kids spend a lot of time online—often more than they would like. This is by design.[4] Companies design their platforms to extract as much time and data as possible, and in the process they prey on minors' psychological vulnerabilities for profit.[5] These manipulative design strategies lead to compulsive use, depriving minors of control of their online experiences and subjecting them to heightened health, privacy, and data security risks, all so that companies can generate more revenue. The design of these platforms is what is harming kids and teens, and regulating design is the best solution.

Kids often have bad experiences online. Many of these experiences can be traced to their lack of control over key aspects of their online experiences, like who can contact them and what

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] EPIC, *Platform Accountability & Governance*, https://epic.org/issues/platform-accountability-governance/.
[3] EPIC, EPIC's Model Age-Appropriate Design Code, https://epic.org/epic-model-aadc/.
[4] *See* Arvind Narayanan, Understanding Social Media Recommendation Algorithms, The Knight First Amendment Institute at Columbia Univ. 20–22 (2023), https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.
[5] 5Rights Foundation, Disrupted Childhood: The Cost of Persuasive Design 19-21 (Apr. 2023), https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf.

content they see in their feeds. This lack of control undermines their autonomy and increases the risk of harms like cyberbullying, sexual exploitation, bodily injury, and mental health harms.

We do have a few suggestions for further strengthening the RI AADC and making it more resilient to a legal challenge. Industry groups such as NetChoice who have challenged AADCs in other states have brought vagueness claims in their attempts to enjoin laws that require them to change their harmful business practices. The Supreme Court has held that provisions of a law are unconstitutionally vague when people "of common intelligence must necessarily guess at its meaning."[6] Several provisions of the California AADC were recently held to be unconstitutionally vague by the Ninth Circuit, and so legislators need to carefully draft legislation to avoid vagueness.[7]

First, we suggest defining the term "reasonably likely to be accessed by children." The term is used multiple times in the bill and may be vulnerable to a vagueness challenge if left undefined. Other AADC and Kids Codes define this term. Adding a definition will promote consistency among AADC models around the country, provide useful guidance to covered entities, and lower litigation risk. We suggest the following definition:

> *"Reasonably likely to be accessed by children" means the online service, product, or feature is reasonably likely to be accessed by children based on any of the following indicators:*
>
> *i. the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 and the Federal Trade Commission rules implementing that Act;*
>
> *ii. the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by an audience that is composed of at least two percent children; or*
>
> *iii. the covered business knew or should have known that at least two percent of the audience of the online service, product, or feature are children, provided that, in making this assessment, the business shall not collect or process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a minor is actively and knowingly engaged."*

Second, the term "reasonably known to be used by children" in §6-48.2-4.(a)(1) should be changed to "reasonably likely to be access by children" so that the bill uses one consistent term to refer to the likelihood that children are using a product, service, or feature, and that term is defined. Third, we recommend slightly changing the term "high level of privacy" in §6-48.2-4.(a)(5) to "highest level of privacy."

[6] *Connally v. General Construction Co.*, 269 U.S. 385, 391 (1926).
[7] *NetChoice, LLC v. Bonta*, No. 25-2366, 2026 WL 694471 (9th Cir. Mar. 12, 2026).

To improve clarity, and to avoid a successful vagueness challenge, we further suggest that the substantive provisions requiring adherence to the duty of care (§§ 6-48.2-4.(5), 6-48.2-5.(1), (2)(i), (7)) either explicitly refer to the company's analysis of risk in their DPIA or include a scienter requirement, which will implicitly refer to the DPIA. Section 6-48.2-5.(7) already includes a scienter requirement, and § 6-48.2-5.(1), which has a parallel construction, should be amended to use the same language. We suggest:

- § 6-48.2-4.(5) should read "configure all default privacy settings provided to known children by the online service, product, or feature to settings that offer ~~a high~~ the highest level of privacy, unless the covered entity can demonstrate in a DPIA required by § 6-48.2-4.(a)(1) a compelling reason that a different setting is consistent with the duty to use reasonable care to avoid any heightened risk of harm to children, as defined pursuant to the provisions of § 6-48.2–3(b)."
- § 6-48.2-5.(1) should read "process the personal data of any known child in a way that the covered entity knows, or has reason to know, ~~to be inconsistent~~ is not consistent with the duty to use reasonable care to avoid any heightened risk of harm to children, as defined pursuant to the provisions of § 6-48.2–3(b)."
- § 6-48.2-5.(2)(i) should read "the covered entity can demonstrate in a DPIA required by § 6-48.2-4.(a)(1) it has appropriate safeguards in place to ensure that profiling is consistent with the duty to use reasonable care to avoid any heightened risk of harm to known children."

Finally, we recommend that the RI AADC include a severability clause, unless there is a strong presumption of severability in Rhode Island law. In the event that a court holds certain provisions invalid, other sections can still remain enforceable. However, it is worth noting that the bill's current structure may impact severability. Many of the substantive provisions are tied to the duty of care, which is tied to the DPIA. Even with a severability clause, if either the duty of care or DPIA are held invalid, all of these provisions would likely fall together as they are not severable. We suggest the following severability clause from our model bill:

> *If any clause, sentence, paragraph, subdivision, section, or part of this article chapter shall be adjudged by a court of competent jurisdiction to be invalid, such invalidation shall be restricted only to the clause, sentence, paragraph, subdivision, section, or part that has been adjudged invalid and shall not affect, impair, or invalidate any other provision of this article chapter that can be given effect without the invalidated portions. It is the intent of the legislature that this article chapter would have been enacted even if such invalid provisions had not been included herein.*

* * *

Parents can't solve this problem on their own, and they shouldn't have to. The design of these platforms is the problem, and regulating design is the solution. The companies building

these products must take responsibility for their harmful design choices and be required to integrate privacy and safety into their products.

Thank you for the opportunity to submit testimony on this important bill. We have provided a copy of EPIC's Model AADC to the Committee. EPIC is eager to remain a resource for the Rhode Island Legislature as this bill moves through the legislative process. Please contact Suzanne Bernstein at bernstein@epic.org with any questions.

Respectfully submitted,

/s/ *Caitriona Fitzgerald*	/s/ *Megan Iorio*	/s/ *Suzanne Bernstein*
Caitriona Fitzgerald	Megan Iorio	Suzanne Bernstein
EPIC Deputy Director	EPIC Senior Counsel	EPIC Counsel

EPIC'S AGE-APPROPRIATE DESIGN CODE

Model Legislation • February 2026

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

EPIC's Model Age-Appropriate Design Code

Each section, and most subsections, of this bill are designed to be modular—that is, they can be included or excluded from the bill without affecting the operation of the rest of the bill. The purpose is two-fold: (1) to give legislators flexibility to pick and choose protections to include in their legislation, depending on their goals; and (2) to ensure that any part of the law, if enjoined in litigation, does not affect the enforceability of another part of the law. EPIC is happy to advise legislators on any adaptations they would like to make in turning the model bill into legislation. We also have a Word version of the bill we can share upon request.

Section 1. Definitions.

As used in this chapter, unless the context otherwise requires:

(1) **"Affiliate"** means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity. As used in this definition, "control" or "controlled" means:

(a) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

(b) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(c) the power to exercise controlling influence over the management of a company.

(2) **"Age assurance"** encompasses a range of methods used to determine, estimate, or communicate the age or age status of an online user.

"Age assurance" definition
The model bill does not require covered businesses to use age assurance if they do not use data processing or design features tied to compulsive use. A business that wishes to engage in such a practice would have to seek consent from consumers and use age assurance to estimate that the consenting consumers are not minors. Legislators who would prefer not to have covered businesses use age assurance for consent will find suggested alternative language in the relevant provision (Section 3(a)(2)).

(3) **"Age status"** means either an interval with an upper and lower age limit or a label indicating age above or below a specific age.

(4) **"Algorithmic recommendation system"** means a computational process used to determine the selection, order, rank, relative prioritization, or relative prominence of

media provided to a user through an online service, product, or feature, including search results, ranking, recommendations, display, or any other method of automated selection.

"Algorithmic recommendation system" does not include a computational process that:

(a) enables users to find specific other users on a covered business's service, such as by entering individual information as a search query or uploading a list of contacts; or

(b) otherwise returns media responsive to a user's search query, as long as the system does not:

(i) process other personal data of the user to determine the selection, order, rank, relative prioritization, or relative prominence of the media; or

(ii) associate the search query with the user after the search results are returned.

"Algorithmic recommendation system" definition
This term describes the back-end computational process that determines what people see in an algorithmic feed. The definition comes from the Knight Georgetown Institute's Better Feeds model legislation. The definition exempts certain types of algorithmic recommendation systems that do not carry the same risk of harm as those that are regulated, making the bill more workable and easier to comply with.

(5) **"Algorithmic feed"** means a component of an online service, product, or feature that displays or delivers a stream or list of media that is selected, ranked, or arranged in whole or in part by an algorithmic recommendation system.

"Algorithmic feed" definition
This term describes the user interface or design feature of a feed that people see on their screens. We use this term instead of algorithmic recommendation system depending on the context.

(6) **"Biometric data"** means data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that allow or confirm the unique identification of the consumer, including:

(a) iris or retina scans;

(b) fingerprints;

(c) facial or hand mapping, geometry, or templates;

(d) vein patterns;

(e) voice prints or vocal biomarkers; or

(f) gait or personally identifying physical movement or patterns.

"Biometric data" does not include:

(a) a digital or physical photograph;

(b) an audio or video recording; or

(c) any data generated from a digital or physical photograph or an audio or video recording, unless such data can be used to identify a specific individual.

(7) **"Business associate"** has the same meaning as in the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA).

(8) **"Collect"** means buying, renting, gathering, obtaining, receiving, or accessing any personal data by any means. This includes receiving data from the consumer, either actively or passively, or by observing the consumer's behavior.

(9) **"Compulsive use"** means a pattern of use of a covered business's product or service that:

(a) is repetitive and is difficult for a user to stop or reduce despite a desire to do so; and

(b) materially disrupts one or more major life activities, including sleeping, eating, learning, reading, communicating, or working.

"Compulsive use" definition
Many of the provisions in this bill protect against "compulsive use." The definition of "compulsive use" here is consistent with the prevailing empirical definitions of the term. There is significant evidence showing that many tech companies engineer their products to cause compulsive use by designing to maximize engagement. This can only be remedied by changes in design, not by dictating what content minors can see. Focusing on compulsive use helps avoid First Amendment and Section 230 issues.

(10) **"Consumer"** means an individual who is a resident of this State.

"Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the covered business occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(11) **"Covered business"** means a sole proprietorship, partnership, limited liability company, corporation, association, other legal entity, or an affiliate thereof:

(a) that conducts business in this State;

(b) that generates a majority of its annual revenue from online services;

(c) whose online products, services, or features are reasonably likely to be accessed by a minor;

(d) that collects consumers' personal data or has consumers' personal data collected on its behalf by a processor; and

(e) that alone or jointly with others determines the purposes and means of the processing of consumers' personal data.

"Covered business" definition
This definition was tailored to ensure that the bill applies only to primarily online businesses that serve minors and collect and control their personal data. Examples of businesses that would likely be covered include a social media platform used by teens, an online gaming company that collects user data, and a streaming service with significant viewership among minors.

Businesses that would *not* be covered include a brick-and-mortar store with a basic website, a business-to-business software company with no minor users, and a business that does not collect personal data.

Legislators should avoid making industry-specific exemptions, as tech companies are likely to use these exemptions to argue that the law violates the First Amendment.

(12) **"Covered entity"** has the same meaning as in HIPAA.

(13) **"Covered minor"** is a consumer that a covered business knows or should have known, based on knowledge fairly implied under objective circumstances, is under 18 years of age.

"Covered minor" definition
This constructive knowledge standard is derived from proposed federal legislation as well as enacted state laws, such as the Arkansas Children and Teens' Online Privacy Protection Act. The definition requires a covered business not to turn a blind eye to information indicating that a consumer is a minor, but it does not require the business to collect any additional information to estimate the consumer's age. Covered businesses will use this definition to determine which consumers they must provide with heightened privacy defaults and safety tools. Legislators may also choose to use this term to define the group of consumers who cannot consent to high-risk data or design practices, if they do not wish to require companies to use age assurance.

(14) **"Default"** means a preselected option adopted by the covered business for the online service, product, or feature.

(15) **"De-identified data"** means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to the individual, if the covered business that possesses the data:

(a) takes reasonable measures to ensure that the data cannot be used to reidentify an identified or identifiable individual or be associated with an individual or device that identifies or is linked or reasonably linkable to an individual or household; and

(b) for purposes of this paragraph, "reasonable measures" includes the de-identification requirements set forth under 45 C.F.R. § 164.514;

(i) publicly commits to process the data only in a de-identified fashion and not attempt to reidentify the data; and

(ii) contractually obligates any recipients of the data to comply with all provisions of this chapter.

(16) **"Derived data"** means data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about a minor or a minor's device.

(17) **"Direct messaging"** means sending private one-on-one or group messages to other users, separate from public posts.

(18) **"Design feature"** means any aspect of an online service, product, or feature the covered business develops or creates, in whole or in part, to facilitate use of the online service, product, or feature. "Design feature" includes, in whole or in part, any:

(a) algorithmic recommendation system;

(b) algorithmic feed;

(c) user interface;

(d) notification or push alert system; or

(e) reward or incentive system.

"Design feature" does not include any:

(a) media;

(b) content moderation policy; or

(c) component of an algorithmic recommendation system that enforces the business's content moderation policies.

"Design feature" definition
Regulating personal data processing and design features) is the most effective—and the most constitutionally sound—way of addressing harms to minors online. The definition of design feature targets non-expressive—or functional— aspects of product design, which can be regulated consistent with the First Amendment, and explicitly excludes expressive aspects, which may trigger the highest level of constitutional scrutiny.

(19) **"Genetic data"** means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), epigenetic markers, uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(20) **"Identified or identifiable individual"** means an individual who can be readily identified, directly or indirectly, including by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(21) **"Known adult"** is a user that a covered business knows or should have known, based on knowledge fairly implied under objective circumstances, is 18 years of age or older.

"Known adult" definition
This definition uses the same constructive knowledge standard as "covered minor." The term is used to define the category of users a covered business should not connect to covered minors except under specific circumstances. The definition prohibits a covered business from ignoring information the business collects or processes that indicates a user's adult age status, but it does not require the business to collect any additional information to estimate the user's age.

(22) **"Media"** means text, an image, a video, or an audio recording.

(23) **"Minor"** means an individual under 18 years of age.

(24) **"Online service, product, or feature"** means a digital product that is accessible to the public via the internet, including a website or application, and does not mean any of the following:

(a) telecommunications service, as defined in 47 U.S.C. § 153;

(b) a broadband internet access service as defined in 47 C.F.R. § 54.400; or

(c) the sale, delivery, or use of a physical product.

(25) **"Personal data"** means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household.

"Personal data" does not include de-identified data or publicly available information.

(26) **"Process"** or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, modification, or otherwise handling of personal data.

(27) **"Processor"** means a person who processes personal data on behalf of:

(a) a covered business;

(b) another processor; or

(c) a federal, state, tribal, or local government entity.

(28) **"Publicly available information"** means information that:

(a) is made available through federal, state, or local government records or to the general public from widely distributed media; or

(b) a covered business has a reasonable basis to believe that the consumer has lawfully made available to the general public.

"Publicly available information" does not include:

(a) biometric data collected by a business about a consumer without the consumer's knowledge;

(b) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;

(c) information that is made available for sale;

(d) an inference that is generated from the information described in subparagraphs (b) or (c) of this paragraph;

(e) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(f) personal data that is created through the combination of personal data with publicly available information;

(g) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;

(h) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or

(i) intimate images, authentic or computer-generated, known to be nonconsensual.

(29) **"Reasonable alternative design"** means an alternative design feature for which the risk of encouraging compulsive use in minor users is lower, unless the use of this alternative design would reduce the benefit of the product to minor users in a way that substantially outweighs the reduction in the risk of compulsive use to minor users.

"Reasonable alternative design" definition
This definition is used in Section 4, the requirement to minimize risk of compulsive use. The concept is imported from products liability law.

(30) **"Reasonably likely to be accessed"** means the online service, product, or feature is reasonably likely to be accessed by a covered minor based on any of the following indicators:

(a) the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 and the Federal Trade Commission rules implementing that Act;

(b) the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by an audience that is composed of at least two percent minors two through 17 years of age; or

(c) the covered business knew or should have known that at least two percent of the audience of the online service, product, or feature includes minors two through 17 years of age, provided that, in making this assessment, the business shall not collect or process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a minor is actively and knowingly engaged.

"Reasonably likely to be accessed" definition
An entity is considered to meet this standard if it fulfills any one of the listed indicators. The list includes the COPPA standard for directed to a child, an audience composition measurement of two percent or more minors, and constructive knowledge that at least two percent of the business's users are minors. These indicators aim at identifying online products, services, or features minors are likely to use. The definition tracks the commonsense idea that products minors are likely to use should contain adequate safeguards, while products minors are highly unlikely to use need not.

(31) **"Small business"** means a covered business that meets the following criteria for the three preceding calendar years (or for the period during which the covered business has been in existence if such period is less than three years):

(a) the covered business's average annual gross revenues during the period did not exceed $25,000,000, as adjusted annually to reflect changes to the Consumer Price Index; and

(b) the covered business, on average, did not annually collect, process, retain, or transfer the personal data of more than 50,000 individuals during the period for any purpose other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product.

(32) **"Third party"** means a natural or legal person, public authority, agency, or body other than the covered minor or the covered business.

(33) **"Weight"** means the individual numeric setting that controls the output of a recommender system at a high level across a covered online platform's user base, such as the relative contributions of different factors to an item's ranking.

"Weight" definition
This definition comes from the Knight Georgetown Institute's Better Feeds model legislation.

Section 2. Exclusions.

Section 2
Lawmakers should avoid making any additional exemptions, particularly industry-specific exemptions, as tech companies are likely to use these exemptions to argue that the law violates the First Amendment.

This chapter does not apply to:

(a) any federal, state, tribal, or local government entity in the ordinary course of its operation;

(b) protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, HIPAA;

(c) information used only for public health activities and purposes described in 45 C.F.R. § 164.512;

(d) information that identifies a consumer in connection with:

(1) activities that are subject to the Federal Policy for the Protection of Human Subjects as set forth in 45 C.F.R. Part 46;

(2) research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(3) activities that are subject to the protections provided in 21 C.F.R. Part 50 and 21 C.F.R. Part 56; or

(4) research conducted in accordance with the requirements set forth in paragraphs (A)–(C) of this subsection or otherwise in accordance with State or federal law;

(e) any entity whose primary purpose is journalism as defined in **[statute]** and that has a majority of its workforce consisting of individuals engaging in journalism; or

(f) any financial institution subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act.

Section 3. High-Risk Data Processing and Design Features.

Section 3
This section is substantially the same as Section 6 of the Vermont Age-Appropriate Design Code, with a few additions to (1) clarify that companies should provide the protections in this section to all consumers by default and only allow adult consumers to opt into risky designs; (2) to prohibit specific design features linked to compulsive use; and (3) to prevent businesses from nudging consumers to change default settings to be less privacy-protective. We moved the section to the top of the bill to improve readability.

(a) **Requirement for consent to be subjected to high-risk personal data processing or design features.** A covered business shall not implement any of the high-risk personal data processing or design features listed in subsection (b) of this section with respect to any consumer unless:

Section 3(a)
Unlike some laws that purport to protect kids online, this model bill does not require age assurance to access an online product or service. Instead, the bill requires businesses to perform age assurance only if (a) they want to subject consumers to high-risk data practices or design features, and (b) a consumer indicates they want those practices and features.

(1) the consumer expressly and unambiguously requests the specific personal data processing or design feature; and

(2) the business has used a commercially reasonable and technically feasible age assurance method to determine that the consumer is not a minor.

Section 3(a)(2)
This provision depends on the state having an Attorney General who can issue rules on what a "commercially reasonable and technically feasible age assurance method" is. For states that do not have the capacity to conduct an AG rulemaking on age assurance, you can replace this provision with the following: "(2) the consumer is not a covered minor."

(b) **High-risk personal data processing and design features.** A covered business shall not:

(1) collect, sell, share, or retain any personal data of the consumer that is not necessary to provide an online service, product, or feature with which the consumer is actively and knowingly engaged;

(2) use previously collected personal data of the consumer for any purpose other than a purpose for which the personal data was collected, unless necessary to comply with any obligation under this chapter;

Section 3(b)(1)–(2)
These two provisions are basic data protection requirements. The provisions protect consumers against data misuse by minimizing the collection and disclosure of their data and limiting the purposes for which the data can be used.

(3) permit any individual, including a parent or guardian, to monitor the online activity of the consumer or to track the location of the consumer without providing a conspicuous signal to the consumer when the consumer is being monitored or tracked;

Section 3(b)(3)
This provision requires online activity and location tracking to be disclosed to consumers but does not prohibit products or features that facilitate this tracking.

(4) use the personal data of the consumer to select, recommend, or prioritize media for the consumer in an algorithmic feed, unless the personal data is:

(A) the consumer's express and unambiguous request to receive:

(i) media from a specific account, feed, or user, or to receive more or less media from that account, feed, or user;

(ii) a specific category of media, such as "cat videos" or "breaking news," or to see more or less of that category of media; or

(iii) more or less media with similar characteristics as the media they are currently viewing;

(B) user-selected privacy or accessibility settings;

(C) the consumer's location, but only to determine whether the consumer is within the State for purposes of complying with this section;

(D) the consumer's age status, but only to implement the covered business's policies regarding media appropriate for minors; or

(E) a search query, provided the search query is only used to select and prioritize media in response to the search;

Section 3(b)(4)
This provision gives consumers more control over what they see in their feeds by requiring personalized feeds to use only data that reflects consumers' preferences for what they want to see. It targets algorithmic feeds that surveil user behavior and uses this data to extend engagement in ways that can lead to compulsive use. This use of personal data serves the functional purpose of predicting user behavior to maximize advertising revenue, rather than the expressive purpose of selecting or excluding media based on the message expressed. By regulating a functional, rather than an expressive, aspect of feed design, the provision should not violate the First Amendment.

The provision is inspired by provisions in the New York SAFE for Kids Act and California's Protecting Our Kids from Social Media Addiction Act, the latter of which has so far survived constitutional challenges in the district and federal appeals courts. The primary difference between the model bill provision and the NY and CA provisions is that the model bill—like an analogous provision in the Vermont Age-Appropriate Design Code—allows businesses to use a wider range of personal data that reflects users' express preferences. The provision works in tandem with the filter tool in Section 5.

(5) send push notifications to the consumer between 12:00 midnight and 6:00 a.m.; or

(6) implement any design feature or component of a feature that:

(A) automatically plays a video, unless the video is the next in a series and the user expressly and unambiguously chose to play a prior video in the series;

(B) uses intermittent variable reward schedules;

(C) continuously loads new media in an algorithmic feed seamlessly and absent a specific request from the user, such as an infinite scroll feed;

(D) is intended to induce compulsive use;

(E) has been identified and declared by the Attorney General as a prohibited personal data processing or design feature pursuant to the rulemaking process outlined in subsection (c) of this section.

Section 3(b)(6)
This provision prohibits specific design features that have been linked to compulsive use, as well as any features that are intended to induce compulsive use. The provision targets the practice of intentionally designing to hack user attention and borrowing addictive design tactics from other industries, like gambling.

(c) **Prohibition on undermining user autonomy in settings.** A covered business shall not:

(1) provide a single setting to make more than one setting under this subsection or Section 4 of this chapter less protective; or

(2) prompt or nudge a consumer to change any of their settings under this subsection or Section 4 of this chapter unless strictly necessary to provide the consumer with the online product, service, or feature with which they are actively or knowingly engaged.

Section 3(c)
This provision ensures that companies do not harass consumers into opting into the high-risk practices outlined in this section.

(d) **Rulemaking.** The Attorney General shall, on or before **[implementation date]**, adopt rules pursuant to this chapter that prohibit personal data processing or design features of a covered business that, in the opinion of the Attorney General:

(1) carry a risk of causing compulsive use that is not substantially outweighed by any benefits provided by the practice or feature to users; or

(2) subvert or impair user autonomy, decision making, or choice during the use of an online service, product, or feature of the covered business.

(e) The Attorney General shall, at least once every two years, review and update the rules promulgated under subsection (c) of this section as necessary to keep pace with emerging technology.

Section 3(d)–(e)
Attorney General rulemaking is an important future-proofing feature of this model bill. However, legislators in states where AG rulemaking is unlikely or unavailable could make the rulemaking permissive instead of required.

Section 4. Requirement to Minimize Risk of Compulsive Use.

Section 4
This section draws from the risk-utility concepts in products liability law to require covered businesses to assess their design features for the risk of causing compulsive use in minors. The section also requires businesses to use less risky reasonable alternative designs when available. A "reasonable alternative design" is defined in the bill and involves weighing the risk of causing compulsive use against the usefulness of the feature, ensuring that user experience is not substantially reduced to make a product only marginally safer. Covered businesses may offer more risky design features to adult consumers, but only with their consent. **Small businesses are exempt from the requirements of this section.**

(a) **Requirement to assess for risk of causing compulsive use.** Prior to deploying any new design feature, or a material change to any existing design feature, to consumers, a covered business must assess the risk that the design feature will cause compulsive use in minors.

(b) **Requirement to adopt reasonable alternative design.** For any design feature that carries a reasonably foreseeable risk of causing compulsive use in minors, a covered business must:

(1) determine if there is a reasonable alternative design; and

(2) if one or more reasonable alternative designs do exist, provide the reasonable alternative design that carries the lowest risk of causing compulsive use as a default to each consumer, until:

(A) the consumer expressly and unambiguously requests the design feature; and

(B) the covered business determines, using a commercially reasonable and technically feasible age assurance method, that the consumer is not a minor.

Section 4(b)(2)(B)
As with Section 3(a)(2), legislators in states that do not have the capacity to conduct AG rulemaking on age assurance can replace this provision with the following: "the consumer is not a covered minor."

(c) **Prohibition on providing design features where risk outweighs benefit.** Notwithstanding subsection (b) of this section, a covered business shall not deploy any design feature to consumers if its assessed risk of causing compulsive use in minors outweighs the assessed benefit of the design feature to minors, unless:

(1) the consumer expressly and unambiguously requests the design feature; and

(2) the covered business determines, using a commercially reasonable and technically feasible age assurance method, that the consumer is not a minor.

Section 4(c)(2)
As with Section 3(a)(2), legislators in states that do not have the capacity to conduct AG rulemaking on age assurance can replace this provision with the following: "the consumer is not a covered minor."

(d) **Requirement to assess existing design features upon implementation.** Prior to **[implementation date]**, a covered business shall assess all existing design features and mitigate the risk of causing compulsive use in minors as described in this section.

(e) **Record retention.** A covered business shall document each step taken in accordance with subsections (a), (b), and (c) of this section, along with any experiments, evidence, and data that supports the assessments and determinations made, and retain such documents for a period of 10 years. All personal data collected about individual users to support this subsection shall be de-identified.

(f) **Audit.** A covered business shall annually submit all records related to the assessments and determinations made in subsections (a), (b), and (c) of this section to an independent auditor, who will assess the records for compliance with this section and recommend any changes that would bolster compliance.

(g) **Limitation.** Nothing in this section shall require a covered business to:

(1) assess any media for the media's risk of causing compulsive use; or

(2) limit any consumer's access to any specific user-generated content or category of user-generated content.

Section 4(g)
The limitation here is meant to preempt arguments from industry that Section 4 requires them to assess the media on their platforms for harm and to change their content moderation practices. The provision helps avoid First Amendment concerns raised in the California AADC litigation.

(h) **Exemption for Small Businesses.** The provisions of this section shall not apply to any covered business that qualifies as a small business.

Section 5. Required Default Privacy Settings and Tools.

Section 5
The general approach of this section is to default covered minors into privacy-protective settings and to give them more control over their online experiences. The default settings and controls create an environment where covered minors can learn to exercise their autonomy without the undue influence of manipulative design.

(a) Default privacy settings.

Section 5(a)
Most of these provisions are substantively the same as the default privacy settings in the Vermont AADC. The most significant change is to require these settings on any online product—not just a social media platform—that uses a risky design choice (e.g., an algorithmic recommendation system to recommend new contacts to covered minors).

(1) A covered business shall configure all default privacy settings provided to a covered minor through the online service, product, or feature to the highest level of privacy.

(2) **Visibility controls.** A covered business shall not, by default, configure its online product, service, or feature to:

(A) use an algorithmic recommendation system to recommend to any known adult user that they connect to a covered minor as a friend, follower, or contact;

(B) use an algorithmic recommendation system to recommend to any known adult user that they follow a covered minor's media, unless the covered minor's account was connected to the known adult's account as a friend, follower, or contact prior to the recommendation;

(C) use an algorithmic recommendation system to recommend to any known adult user that they communicate with a covered minor through direct messaging, unless the covered minor's account was connected to the known adult's account as a friend, follower, or contact prior to the recommendation;

(D) use an algorithmic recommendation system to recommend to a covered minor that they communicate with any known adult through direct messaging, unless the covered minor's account was connected to the known adult's account as a friend, follower, or contact prior to the recommendation;

(E) display a covered minor's friends, followers, or contacts; or

(F) enable search engine indexing of a covered minor's account profile and media.

Section 5(a)(2)
The first four visibility controls protect minors from unwanted contact from adult strangers. They target common product features like friend suggestions that may currently match covered minors with adult strangers, increasing the risk of grooming, stalking, and other safety concerns.

(3) Location controls.

(A) A covered business shall not display the location of any covered minor to any other user by default.

(B) A covered business shall only display the covered minor's location to another user when the covered minor has expressly and unambiguously chosen to share their location with the specific user.

Section 5(a)(3)
Displaying a covered minor's physical location endangers the minor's privacy and physical safety. The location controls do not display covered minors' locations by default. The controls also prevent minors from disclosing their locations to large groups of people (or everyone on a platform) at once, instead requiring the minor to specify which individuals can see their locations.

(4) Notification controls.

(A) A covered business shall not:

(i) send push notifications to any covered minor by default; or

(ii) provide a single setting that enables all push notifications.

(B) A covered business shall provide covered minors with settings to enable or disable each specific category of push notification offered by the covered business on the product or service, such as marketing notifications, direct message notifications, media interaction notifications, and any other category of notification pushed by the product or service.

Section 5(a)(4)
Push notifications, or alerts businesses send to users who are not currently in an app, are a means of drawing users back to the app. Much like automated calls, push notifications are nuisances and invasions of privacy that interrupt other life activities. They are also linked to compulsive use. The notification controls turn all push notifications off by default and give covered minors granular control over which notifications to turn on.

(5) Interaction controls.

(A) A covered business shall:

(i) disable by default all interaction counts, including counts of reactions and comments, on all of the covered minor's media;

(ii) offer settings to enable or disable specific types of interaction counts, such as comments, reactions, reshares, or other categories of interactions; and

(iii) offer a single setting to turn all interaction counts on at once only if the settings to turn specific interactions on are equally or more prominent and accessible.

Section 5(a)(5)
The interaction controls give covered minors control over whether they see design features such as like counts, which have been linked to unhealthy social comparison and compulsive use. A similar provision of California's Protecting Our Kids from Social Media Addiction Act ran afoul of the First Amendment because it gave parents, and not minors, control over this setting, so this bill was drafted to avoid that concern.

(6) **Prohibition on undermining user autonomy in settings.** A covered business shall not:

(A) provide a covered minor with a single setting that makes more than one default privacy or design feature setting less protective at once; or

(B) request or prompt a covered minor to make any of their settings less protective, unless the change is strictly necessary for the covered minor to access a service or feature they have expressly and unambiguously requested.

Section 5(a)(6)
This provision ensures that companies do not harass covered minors into making their privacy settings less protective.

(b) **Blocking tool.** A covered business that facilitates communications between users shall:

(1) provide a prominent, accessible, and responsive tool that gives a covered minor the option to block specific users from taking, at minimum, each of the following actions:

(A) accessing the user's media;

(B) interacting with the user's media;

(C) communicating with the user through their media;

(D) communicating with the user through direct messaging; and

(E) communicating with the user through any other means offered by the covered business through the product or service.

(2) The tool described in paragraph (1) of this subsection shall provide a covered minor with the option to prevent media from the blocked user from appearing in the covered minor's feed.

(3) The tool described in paragraph (1) of this subsection shall, at a minimum, be accessible from a feature located:

(A) proximate to every instance of another user's username and/or avatar;

(B) on all media shared by another user;

(C) on every direct message or direct message thread; and

(D) in a first-level settings menu labeled "Blocked Users."

(4) The features described in subparagraphs (A) through (C) of paragraph (3) of this subsection shall provide a covered minor with the option to:

(A) block the other user, which will trigger all of the settings in paragraphs (1) and (2) of this subsection; or

(B) go to the settings page to select more granular block settings for the other user.

Section 5(b)
The blocking tool will help protect covered minors from online harassment, stalking, and cyberbullying by giving minors control over who can interact with them on communications platforms.

(c) **Filter tool.** A covered business that offers an algorithmic feed to a covered minor that uses the covered minor's personal data to select, recommend, or prioritize media in the feed shall:

(1) provide a prominent and accessible user interface that enables the covered minor to:

(A) expressly and unambiguously communicate their preferences about the types of media to be recommended and to be blocked in the output of the relevant algorithmic recommendation system; and

(B) access, review, and make changes to any personal data the covered business uses to determine the output of the relevant algorithmic recommendation system; and

(2) ensure that the relevant algorithmic recommendation system is informed by these preferences.

Section 5(c)
The filter tool gives covered minors more control over what they see in their algorithmic feeds. It is based on the filter provision of the Knight Georgetown Institute's Better Feeds model bill.

(d) **Follower-only algorithmic feed option.** A covered business that offers an algorithmic feed to a covered minor that uses the covered minor's personal data to select, recommend, or prioritize media in the feed shall provide the minor with the choice of an algorithmic feed that only selects media from sources the minor affirmatively chose to follow or otherwise include in the feed.

Section 5(d)
The follower-only algorithmic feed option gives a covered minor the choice of an alternative feed that only shows them media from content providers the minor selects. This gives the minor more control over what they see in their feed, as the minor—and not the business—is selecting the sources of all of the media.

(e) **Account deletion tool.** A covered business shall:

(1) provide a prominent and accessible tool to allow:

(A) a covered minor to request the covered business delete any account profiles, media and personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the covered business, personal data the covered business obtained from another source, and derived data; and

(B) the parent or legal guardian of a covered minor to take such a request on the child's behalf.

(2) honor that request not later than 15 days after a covered business receives the request.

(3) **Exception.** A covered business shall not delete de-identified data collected for the purpose of complying with the transparency requirements in Section 4(e) of this chapter.

Section 5(e)
The account deletion tool requires covered businesses to honor covered minors' (or their parents') requests to delete their personal data. The provision was expanded from the VT AADC to cover more than just social media platforms.

Section 6. Transparency on Personal Data Use in Design Features.

Section 6
These provisions were revised from the VT AADC to focus more closely on covered businesses' data practices that contribute to compulsive use rather than their content moderation practices. While requiring companies to disclose their content moderation practices generally—and not on specified categories of disfavored messages—is likely to be constitutionally permissible, even under Ninth Circuit precedent like *X v. Bonta*, we wanted to keep the transparency provision in this bill consistent with its main purpose: regulating manipulative design.

A covered business shall prominently and clearly provide on its website or mobile application:

(a) the covered business's privacy information, terms of service, policies, and community standards;

(b) for each algorithmic feed in use by the covered business:

(1) the purpose of the feed; and

(2) the algorithmic recommendation system(s) used to determine the feed;

(c) for each algorithmic recommendation system in use by the covered business:

(1) the purpose of the system;

(2) a description of any personal data of minors that is used as an input or to inform an input;

(3) the source of the personal data;

(4) the purpose of using the personal data; and

(5) how each personal data input:

(A) is measured and determined, if it is derived data; and

(B) is weighed relative to the other inputs reported in this paragraph, categorized into one of four quartile groups according to the input's relative importance in contributing to the system's output; and

(d) for every other feature of the product or service that uses the personal data of covered minors, descriptions of:

(1) the purpose of the service feature;

(2) the personal data collected by the service feature;

(3) the personal data used by the service feature;

(4) how the personal data is used by the service feature;

(5) any personal data transferred to or shared with a processor or third party by the service feature, the identity of the processor or third party, and the purpose of the transfer or sharing; and

(6) how long the personal data is retained.

Section 7. Rules and Enhanced Privacy Protections for Age Assurance.

(a) **Privacy protections for age assurance data.** During the process of conducting age assurance, covered businesses and processors shall:

(1) only collect personal data of a consumer that is strictly necessary for determining a consumer's age status;

(2) immediately upon determining whether a consumer is a covered minor, delete any personal data collected of that consumer for age assurance, except the determination of the consumer's age status;

(3) not use any personal data of a consumer collected for age assurance for any other purpose;

(4) not combine personal data of a consumer collected for age assurance, except the determination of the user's age status, with any other personal data of the consumer;

(5) not disclose personal data of a consumer collected for age assurance to a third party that is not a processor; and

(6) implement a review process to allow consumers to appeal their age determination.

Section 7(a)
The model bill does not require covered businesses to use age assurance, but those that do must protect the personal data they collect and process for that purpose. These requirements are the same as in the VT AADC, with only small changes to conform to the terminology used in this model (e.g., "age status" instead of "age range"). The requirements apply regardless of whether the business uses age assurance to comply with the law's consent provisions or to voluntarily use it for other purposes.

(b) **Safe harbor.** A covered business or processor that complies with the provisions and rules of this chapter shall not be liable for any inaccuracies in a consumer's age status.

Section 7(b)
The safe harbor was added to address concerns that covered businesses and processors may face liability for inaccurately labeling a minor user as not a minor and vice versa.

(c) Rulemaking.

(1) Subject to paragraph (2) of this subsection, the Attorney General shall, on or before **[implementation date]**, adopt rules:

(A) identifying commercially reasonable and technically feasible methods for covered businesses and processors to determine if a consumer is a minor;

(B) describing:

(i) appropriate review processes for consumers appealing their age status determinations; and

(ii) transparency measures that would increase consumer trust in age assurance; and

(C) providing any additional privacy protections for personal data collected for age assurance.

(2) The Attorney General shall periodically review and update these rules as necessary to keep pace with emerging technology.

(3) In adopting these rules, the Attorney General shall:

(A) prioritize consumer privacy and accessibility; and

(B) consider:

(i) the size, financial resources, and technical capabilities of covered businesses and processors;

(ii) the costs and effectiveness of available age assurance methods;

(iii) the impact of age assurance methods on users' safety, utility, and experience; and

(iv) the efficacy of requiring covered businesses and processors to:

(I) use previously collected data to determine the age status of some or all consumers;

(II) adopt interoperable age assurance methods; and

(III) provide consumers with multiple options for age assurance.

Section 7(c)
For legislators in states where AG rulemaking is unavailable or unlikely, or where they prefer a constructive knowledge standard instead of age assurance for determining which users can consent to high-risk designs, this rulemaking provision can be modified to be permissive, as follows:

(a) The attorney general may adopt and update rules implementing this section, including:

(1) describing:

(A) how covered businesses may comply with the covered minor and known adult standards;

(B) appropriate review processes for consumers appealing their age status determinations; and

(C) transparency measures that would increase consumer trust in age assurance; and

(2) providing any additional privacy protections for personal data collected for age assurance.

Section 8. Enforcement.

(a) A covered business or processor that violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of **[state UDAP statute]**.

(b) The Attorney General shall have the same authority under this chapter to make rules, conduct civil investigations, bring civil actions, and enter into assurances of discontinuance as provided under **[state UDAP statute]**.

(c) Any violation of this chapter or rules adopted pursuant to these sections constitutes an injury in fact to a consumer.

(d) A consumer injured by a violation of this chapter may bring a civil action against the covered business or processor that violates this chapter, in which the court may award a prevailing plaintiff:

(1) statutory damages of $5,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is greater;

(2) punitive damages, for reckless or knowing violations;

(3) injunctive relief;

(4) declaratory relief; and

(5) reasonable attorney's fees and litigation costs.

Section 8(c)–(d)
This model includes a private right of action, which allows consumers to enforce the law if their rights are violated. A private right of action is essential because businesses are not likely to comply with a law unless there is a real threat of enforcement. Unfortunately, resource-constrained AGs can only bring a small number of cases every year, which limits the enforcement threat. A private right of action makes the enforcement threat real, bolstering compliance.

This private right of action is independent of a state's unfair and deceptive practices (UDAP) law, but a state with a strong private right of action under their UDAP law might either remove or modify these provisions to allow suit through the UDAP law. That is the path the VT AADC took.

Section 9. Rules of Construction.

Nothing in this chapter shall be interpreted or construed to:

(a) impose liability in a manner that is inconsistent with 47 U.S.C. § 230;

(b) impose liability in a manner that is inconsistent with the First Amendment of the United States Constitution;

(c) force any consumer to undergo age assurance as a condition of accessing the products or services of any covered business;

(d) prevent any consumer from accessing any user-generated media; or

Section 9(a)–(d)
These provisions ensure that, if there is litigation over the enforceability of this law, a judge will not strike down the law if there is a permissible interpretation of it that is consistent with Section 230 and the First Amendment. This will prevent industry from successfully challenging the law by presenting a strawman interpretation that violates Section 230 or the First Amendment, as has occurred in some NetChoice litigation.

(e) preempt or otherwise affect any right, claim, remedy, presumption, or defense available at law or in equity, including but not limited to anti-discrimination, consumer protection, labor, and civil rights laws.

Section 9(e)
This provision ensures that nothing in the bill unintentionally limits consumers' rights under other laws.

Section 10. Nondiscrimination.

Section 10
The nondiscrimination provision ensures that covered businesses don't degrade their products for covered minors or other consumers who do not opt into high-risk designs.

A covered business shall not discriminate or retaliate against any consumer, including denying products or services, charging different prices or rates for products or services, or providing lower quality products or services to the consumer, for receiving any of the protections contained in this chapter, exercising any of the rights contained in this chapter, for refusing to change their privacy and safety settings, or for refusing to agree to the collection or processing of personal data or to the use of any design feature.

Section 11. Rights and Freedoms of Covered Minors.

It is the intent of the **[legislative body]** that nothing in this chapter may be construed to infringe on the existing rights and freedoms of covered minors or be construed to discriminate against the covered minors based on race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, religion, or national origin.

Section 12. Effective Dates.

This act shall take effect on **[date]**, except that **[the rulemaking authority provisions]** shall take effect on **[date]**.

Section 13. Severability.

Section 13
A strong severability clause is necessary to ensure that, in the event of a successful litigation challenge to one provision of the law, the rest of the law can still be enforced.

If any clause, sentence, paragraph, subdivision, section, or part of this article chapter shall be adjudged by a court of competent jurisdiction to be invalid, such invalidation shall be restricted only to the clause, sentence, paragraph, subdivision, section, or part that has been adjudged invalid and shall not affect, impair, or invalidate any other provision of this article chapter that can be given effect without the invalidated portions. It is the intent of the legislature that this article chapter would have been enacted even if such invalid provisions had not been included herein.