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

February 26, 2024

Chair Wendy Harrison
Vermont Senate Committee on Institutions
115 State Street
Montpelier, VT 05633

Dear Chair Harrison and Members of the Committee:

We write in support of S.69, the Vermont Age-Appropriate Design Code Act.[1] The Electronic Privacy Information Center is an independent nonprofit research organization founded 30 years ago to protect privacy, freedom of expression, and democratic values in the information age.[2] EPIC regularly advocates for privacy safeguards for minors online and participates as amicus to help judges understand how to evaluate constitutional challenges to data and design regulation.[3]

I. S. 69 is Needed to Protect Minors Online

Minors are online from a young age. They benefit from a lot of these experiences—from educational opportunities to gaming, messaging with friends, and more. Unfortunately, existing protections for the privacy of minors online are deeply inadequate. Apps and websites routinely share and sell minors' personal information to data brokers, advertisers, and others. Such data collection is pervasive, fueling commercial surveillance and profiling that leads to myriad

[1] Vermont Age-Appropriate Design Code Act of 2025, Sec. 1, §§ 2449a-j, as introduced on February 13, 2025 (Bill S. 69) [hereinafter *VTAADC*].
[2] EPIC, *About EPIC*, https://epic.org/about/.
[3] EPIC, *Platform Accountability & Governance*, https://epic.org/issues/platform-accountability-governance/.

privacy harms.[4] Many companies employ design features like endless scroll, push notifications, and recommender algorithms that can lead to extended or compulsive use by surveilling minors, and use the data to figure out the best way to manipulate each minor into staying on the platform as long as possible.[5] All of these practices deprive minors of their autonomy, taking control of their online experiences out of their hands, and subjecting them to heightened physical safety and data security risks.

Despite these known threats to minors' safety online, Congress has repeatedly failed to pass comprehensive federal privacy legislation or to update protections for minors beyond the decades-old Children's Online Privacy Protection Act (COPPA). States are stepping in and enacting state-level comprehensive data privacy laws to fill this gap, as well as laws that give minors special protections online. Vermont has the opportunity to pass a bill that is both effective and can withstand constitutional scrutiny. In doing so, Vermont can lead the way for other states and Congress to do the same.

The Vermont AADC protects minors' privacy, enhances minors' autonomy, and ensures their online safety by prohibiting abusive data and design practices. It does not ban minors from social media, and it does not block minors from accessing any type of content. The choices made in drafting make it stand on strong constitutional ground.

---

[4] *See* EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* 36–38, 61–62 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[5] *See* Arvind Narayanan, Understanding Social Media Recommendation Algorithms, The Knight First Amendment Institute at Columbia University 20–22 (2023), https://s3.amazonaws.com/kfai-documents/documents/4a9279c458/Narayanan---Understanding-Social-Media-Recommendation-Algorithms_1-7.pdf.

We will focus on the following sections of the bill: the coverage definitions, the minimum duty of care, default privacy settings and tools, transparency, prohibited data and design practices, and age assurance.

II. Coverage and Scope

This bill provides online privacy and safety protections for minors in spaces where minors are likely to be. It is not focused on a specific type of business, nor does it regulate websites or apps used only by adults.

The bill requires a "covered businesses" to provide certain privacy safeguards to "covered minors" on their service. A "covered business" is, essentially, a business that collects consumer personal data, determines the purpose and means of processing that data, and whose features or services are likely to be accessed by a minor.[6] Some of the AADC's provisions apply to all covered businesses, while others apply only to social media platforms, as that term is defined in the statute. Provisions that apply to social media platforms only target harms that are specific to, and prevalent on, social media, like unwanted adult contact. Meanwhile, provisions that apply to all covered businesses target harms from broader online business practices, like excessive data collection and push notifications.

Industry has urged this committee to narrow the scope of businesses subject to this law, and the committee has considered limiting the entire bill to social media platforms alone. But what industry did not mention is that, in courts, they are arguing that laws that only apply to

[6] VTAADC, *supra* note 1 at §2449(a)(11).

social media companies are presumptively unconstitutional *solely because they apply to social media companies and not more broadly*. Although EPIC disagrees that this argument has merit, industry has prevailed on this argument in at least one district court.[7] Limiting this law to social media companies alone will thus introduce new litigation roadblocks to enforcement.

A "covered minor" is a resident of the State that the covered business actually knows is under 18 years of age *or* has been flagged as under 18 by age assurance pursuant to rules adopted by the Attorney General. The "or" here means that age assurance is not actually *required*—it is just an *option* available to companies to determine age. Because age assurance is an option and not a requirement, industry cannot argue that the law burdens minors' or adults' access to their services, insulating the law from such a constitutional challenge.

If a company chooses not to use age assurance on their platform, they are only required to provide the law's protections to a user when they actually know that they are under 18. An actual knowledge standard is a relatively low bar for entities to reach. Other bills either mandate age assurance or have a "constructive knowledge" standard: describing when a business "knows or should have known" a consumer is a minor.

At the same time, the VT AADC will be more effective at providing protections to minors than a law with only an actual knowledge standard, as the Attorney General can designate

[7] *NetChoice, LLC v. Reyes*, No. 2:23-CV-00911-RJS-CMR, 2024 WL 4135626, at •8 (D. Utah Sept. 10, 2024). NetChoice has also made this argument against California's addictive feeds law. The judge there rejected the argument that limiting the coverage definition to social media platforms made the entire law presumptively unconstitutional, but did enjoin the prohibition on nighttime notifications because it only applied to social media companies and not more broadly. *See* EPIC, *Judge Allows California Regulation of Addictive Feeds to Go Into Effect* (Dec. 31, 2024), https://epic.org/judge-allows-california-regulation-of-addictive-feeds-to-go-into-effect/.

existing company practices that estimate the age of users as age assurance under the law, requiring companies to treat as covered minors those users flagged through these systems as under 18. Companies that voluntarily estimate users' ages, like Meta[8] and Google,[9] would be required to use this estimate to provide minors with the VT AADC's privacy, data security and online safety protections.

III. §2449c Minimum Duty of Care

The minimum duty of care section requires companies to consider the potential that their data and design practices will cause specific harms to minors. Compared to last year's version, there are a few significant changes. First, this year's VT AADC has a new limitation that makes it explicit that content that causes emotional distress or compulsive use cannot lead to liability under the duty of care.[10] The limitation in § 2449i(1) reinforces this point: courts must interpret the AADC consistent with Section 230, and Section 230 prohibits holding companies liable for third-party content. Second, the version passed last year made every violation of the law a violation of the duty of care, which meant that, if a court were to find the duty of care unconstitutional, the entire law would have to be struck down, no matter whether the other provisions were constitutional on their own. This year's version of the bill makes the rest of the

[8] Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?* Meta (July 27, 2021), https://about.fb.com/news/2021/07/age-verification/; *Introducing New Ways to Verify Age on Instagram*, Instagram (Mar. 2, 2023), https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.
[9] Jen Fitzpatrick, *New digital protections for kids, teens and parents*, Google: The Keyword (Feb. 12, 2025), https://blog.google/technology/families/google-new-built-in-protections-kids-teens/; Emma Roth, *Google will use machine learning to estimate a user's age*, The Verge (Feb. 12, 2025), https://www.theverge.com/news/610512/google-age-estimation-machine-learning
[10] *Id*. at §2449c(c).

law independent of the duty of care, allowing the rest of the law to stand on its own in case of a successful constitutional challenge to the duty of care. Third, the minimum duty of care owed to minors is narrow: providing important online safety and privacy protections for minors in more extreme circumstances where the design or data use of a covered business may result in emotional distress, compulsive use or discrimination.[11] A limited duty of care that does not provide liability for content is most likely to pass constitutional scrutiny.

IV. §2449d Required Default Privacy Settings and Tools

This section requires covered businesses to configure all default privacy settings to the highest level of privacy for covered minors.[12] It also requires a mechanism for covered minors to delete their social media accounts. Many of these default settings guard against unwanted adult contact on social media sites. As we've heard in the Meta whistleblower testimony and through other reporting, this is an ongoing safety and privacy issue for minors – one that many social media companies are aware of but have not sufficiently addressed through self-regulation. [13] These settings put minors in control of if and how they would like to interact with adults. And minors can turn the settings off themselves if they choose—no parental action required. These default settings are drafted to guard against unwanted adult contact, while still allowing adult contact if "expressly and unambiguously requested."[14]

[11] *Id*. at §2449c(b).
[12] VTAADC, *supra* note 1 at §2449d.
[13] Jeff Horwitz, *His Job Was to Make Instagram Safe for Teens. His 14-Year-Old Showed Him What the App Was Really Like*, Wall Street Journal (Nov. 2, 2023), https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1?reflink=desktopwebshare_permalink.
[14] VTAADC, *supra* note 1 at §2449d(a)(1).

This section also includes an important setting that turns off all push notifications by default. This is the first of two times that push notifications are addressed in this bill. Section §2449f (prohibited data and design practices) prohibits push notifications for covered minors between midnight and 6am.[15] Push notifications are used to prod users to open the app when they are not in it. They are an important design feature encouraging compulsive use. TikTok, for instance, admits that push notifications are key to drawing users attention back to the app, and they have sometimes sent thousands of notifications a day to minors.[16]

Push notifications are also a nuisance and an invasion of privacy—like robocalls. And push notifications should be regulated like robocalls. That is precisely what the VT AADC does. Just as the federal Telephone Consumer Protection Act (TCPA) opts consumers out of robocalls by default, the VT AADC turns push notifications off (opts minors out) by default. And just as the TCPA has been repeated upheld as a constitutional time, place, and manner restriction,[17] so too will the VT AADC's restrictions on push notifications.[18]

---

[15] *Id*. at §2449f(a)(5).
[16] Complaint at 32-37, Commonwealth of Massachusetts v. TikTok Inc., No. 2484CV2639-BLS-1 (Mass. Super Ct., Oct. 8, 2024), https://www.mass.gov/doc/tiktok-complaint-unredacted/download (unredacted complaint) [hereinafter *MA Complaint*].
[17] Courts have repeatedly upheld the Telephone Consumer Protection Act (TCPA) as a constitutional, content-neutral time, place, and manner regulation. *Barr v. AAPC*, 591 U.S. 610 (2020); *also Moser v. FCC, 46 F.3d 970* (9th Cir.), cert. denied, 515 U.S. 1161 (1995); *Gomez v. Campbell-Ewald Co.*, 768 F.3d 871, 876-77 (9th Cir. 2014), *aff'd on other grounds*, 136 S. Ct. 663 (2016) (finding the TCPA constitutional post-*Reed v. Town of Gilbert*, 135 S. Ct. 2218 (2015)); *Duguid v. Facebook, Inc.*, 926 F.3d 1146, 1157 (9th Cir. 2019), *rev'd in part on other grounds*, 592 U.S. 395 (2021) ("Excising the debt-collection exception preserves the fundamental purpose of the TCPA and leaves us with the same content-neutral TCPA that we upheld—in a manner consistent with *Reed*—in *Moser* and *Gomez*.")
[18] A district court judge in California recently recognized that restrictions on nighttime notifications are a content-neutral time, place, and manner restriction, but enjoined that state's prohibition on nighttime notifications pending further development of the record. That law only applies to social media companies, and the judge thought that it

To ensure that these default settings are effective in providing covered minors with autonomy and choice over their online activity, a covered business cannot provide a single setting for a covered minor to turn all of them off at once or continuously prod minors to make their privacy settings less protective.

V. §2449e Transparency

The transparency section of this bill requires that covered businesses provide information on their website or app about their privacy policies and community standards, algorithmic recommendation systems that they use, and descriptions of the service features that use the personal data of covered minors.[19]

Currently, many of these covered businesses use personal data in many ways that are beyond what a minor or parent could reasonably expect. To make informed decisions about which services to use, covered minors and their parents deserve transparency about how these products work and how their personal data is used in service features. This section requires descriptions of algorithmic recommendation systems and the factors that it uses to build recommendation systems for any given covered minor on their platform. It also requires descriptions about every feature of the service that uses personal data of minors.

---

was unclear, based on the current record, whether social media companies were responsible for a significant amount of the nighttime notifications minors receive. The judge did signal that a generally applicable prohibition on nighttime notifications to minors would pass constitutional scrutiny. *See* EPIC, *Judge Allows California Regulation of Addictive Feeds to Go Into Effect* (Dec. 31, 2024), https://epic.org/judge-allows-california-regulation-of-addictive-feeds-to-go-into-effect/.

[19] VTAADC, *supra* note 1 at §2449e.

Importantly, this provision also includes a requirement for covered businesses to describe if and how it shares or transfers the personal data of covered minors outside of their own platform or service. Beyond seeking transparency for how a covered business uses personal data internally, it's just as important to understand the data flow of personal data to third parties.

This section is drafted in a way that avoids the issues raised in recent litigation in California.[20] It does not require companies to opine about what content is "harmful." It does not require companies to explain how they moderate content the government thinks is "harmful." It isn't about content at all – and it doesn't require companies to make any assessment of harm. It simply asks covered businesses to provide truthful, descriptive information about how they design their algorithmic systems and use minors' personal information in service features. These are just the type of disclosures that courts have traditionally given broad deference to legislatures to require.[21]

VI. §2449f Prohibited Data and Design Practices

This section is short but mighty. It provides critical privacy protections for covered minors and is autonomy enhancing, giving them control over their user experience. The first provision requires companies to minimize the data they collect, process, and share, while the

[20] *See X Corp. v. Bonta*, 116 F.4th 888 (9th Cir. 2024); EPIC, *Ninth Circuit Strikes Down Portion of California AADC but Leaves the rest Intact for Now* (Aug. 16, 2024), https://epic.org/ninth-circuit-strikes-down-portion-of-california-aadc-but-leaves-the-rest-intact-for-now/. *See also* Megan Iorio, *NetChoice v. Bonta: An exacting level of scrutiny no privacy law could survive*, EPIC (Jan. 15, 2024) https://epic.org/netchoice-v-bonta-an-exacting-level-of-scrutiny-no-privacy-law-could-survive/ (discussion of the constitutionality of transparency requirements).

[21] *Zauderer v. Office of Disc. Counsel*, 471 U.S. 626 (1985) (holding that laws that compel a commercial service to disclose truthful, non-controversial information to the public do not involve the same First Amendment interests as laws that prevent companies from engaging in protected speech and so deserve more deference).

second prohibits companies from using data for any purpose other than the one it was collected for. This framework is found in all strong data protection laws and proposals today.[22] The goal is to stop companies from collecting more data than they need to provide users with the service they are currently using, and to stop them from transferring the data to third parties or otherwise using it for purposes that the user did not expect and that could cause harm.

This section also prohibits the covered business from allowing any consumer – including parents or guardians – from monitoring the activity or location of a covered minor without conspicuously informing the minor. This differs from approaches in other states that allow parents or guardians to access their minors' accounts. Here, minors' safety and autonomy is enhanced by letting them know when they are being watched.

The fourth provision in this section is similar to, but improves on, laws recently passed in California and New York that regulate what they call "addictive feeds."[23] The provision limits the personal data social media companies can use to curate feeds for minors. They are meant to address the current design practice of ordering feeds based on passive surveillance of users – tracking clicks, time spent watching, even time spent hovering over media. Companies use this data to predict what arrangement of media is likely to keep a user on the platform longer.[24] This design practice thus invades minors' privacy and contributes to compulsive use.

[22] EPIC, *Data Minimization*, http://epic.org/issues/consumer-privacy/data-minimization/.
[23] Cal. Health & Safety Code § 27000.5 (Protecting Our Kids from Social Media Addiction Act); NY SAFE for Kids Act, N.Y. Gen. Bus. Law §1501(2) (McKinney 2024).
[24] *See*, *e.g.*, MA Complaint, *supra* note **Error! Bookmark not defined.** at 1, 31.

The VT AADC prohibits the use of these "surveillance feeds" and instead directs companies to provide minors with "autonomy-enhancing feeds" that select and order media based on minors' explicit preferences. This gives minors more control over what they see and how much time they spend looking. This bill's approach differs and improves on the New York and California laws by expanding the categories of explicit preference data companies can use to generate minors' feeds. A judge recently upheld the California law against a First Amendment challenge from NetChoice (relying much on one of our amicus briefs),[25] which means that this provision stands on strong constitutional ground.

The final provision in this section directs the Attorney General to do periodical rulemakings to ensure that the bill's protections keep up with changing technology. The bill requires the Attorney General to, at least once every two years, update rules prohibiting data processing or design practices that "lead to compulsive use or subvert or impair user autonomy, decision making, or choice."[26] Where other laws have defined and prohibited practices like "dark patterns," this bill requires the Attorney General to proactively identify and prohibit specific dark patterns. This is a more effective approach because it allows the Attorney General to define the scope of prohibited dark patterns without first having to bring an enforcement action. It also gives companies clear notice of prohibited practices, making it more likely that companies will comply.

[25] EPIC, *supra* note **Error! Bookmark not defined.**.
[26] VTAADC, *supra* note 1 at §2449f(b).

VII. §2449g Age Assurance Privacy

This provision requires the Attorney General to issue rules about how companies can use age assurance to determine whether a user is a minor. There are many different types of age assurance tools available on the market today.[27] The bill directs the Attorney General to prioritize privacy and ease of access in choosing approved age assurance methods as well as the commercial reasonableness of implementing these methods.

To address concerns around the protection of data provided for age assurance purposes, the bill includes strict statutory privacy requirements.[28] These statutory privacy protections are the strongest of any online safety bill for minors to date. The bill also directs the Attorney General to adopt additional privacy rules if necessary.

To address concerns around the accuracy of age assurance methods, the bill also requires companies to implement review and appeals processes and directs the Attorney General to issue rules for how companies should design these processes. An appeals process helps achieve accuracy without requiring the age assurance methods used to be highly accurate—that is, it allows for high accuracy using methods that are inherently less accurate but potentially more privacy protective.

[27] *See* Ariel Fox Johnson, *U.S. Age Assurance Is Beginning to Come of Age: The Long Path Toward Protecting Children Online and Safeguarding Access to the Internet*, Common Sense Media (Sept. 30, 2024), https://www.commonsensemedia.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf.
[28] VTAADC, *supra* note 1 at §2449g.

To make age assurance as efficient and easy as possible, the bill directs the Attorney General to consider the feasibility of encouraging companies to offer a menu of age assurance options to users and to adopt interoperable methods that allow users to assure their age once and to use that determination across platforms.

Conclusion

Thank you for the opportunity to testify in support of this important bill and contribute to the record. EPIC is happy to answer any further questions, and eager to remain a resource for the Vermont Legislature as this bill moves through the legislative process. Please contact Suzanne Bernstein at bernstein@epic.org with any questions.

Respectfully submitted,

/s/ *Megan Iorio*
Megan Iorio
EPIC Senior Counsel

/s/ *Tom McBrien*
Tom McBrien
EPIC Counsel

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Counsel