February 18, 2026

House Small Business and Information Technology Committee
Attn: Samantha Gerhart
702 Capital Ave
Frankfurt, KY 40601

Re: HB 227 - "Relating to Addictive Platforms" (Oppose)

Dear Chair Gordon and Members of the House Small Business and Information Technology Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 227 in advance of the House Small Business and Information Technology Committee hearing on February 19, 2026. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members.

The Association firmly believes that youth are entitled to security and privacy online. Our members have designed and developed parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.[2] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[3]

However, protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Lawful speech cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors.[4] While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).
[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[4] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975). *See also FCC v. Pacifica Found.* 438 U.S. 726, 749–50 (1978); *Pinkus v. United States*, 436 U.S. 293, 296–98 (1978).

Courts have repeatedly struck down laws containing speech restrictions intended to prevent harm to minors.

In 1997, the Supreme Court held that "the First Amendment does not tolerate" laws that "reduce[] the adult population ... to reading only what is fit for children."[5] Yet HB 227 effectively does exactly this: in order to restrict access to content potentially harmful to children, the proposed bill would restrict both children and adults' access to such content. The First Amendment applies to teens as well as adults,[6] and to content posted on social media.[7]

Nor do states have the authority to require parental consent for such viewing; the Court has likewise rejected the argument that "the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[8] Accordingly, the proposed bill unconstitutionally undermines established free speech protections for users of all ages.

The bill does not specify how a user's age is to be determined.

HB 227 would require covered services to treat users under age 18 differently from all other users. However, the bill fails to explain how each covered service would determine which of their users are under 18, specifying only that "reasonable means and efforts, taking into consideration available technology and the data in the possession" of the covered service must be used. Nowhere does the bill specify what methods are considered "reasonable" with a given set of information. Indeed, every covered service will possess a unique set of data regarding any given user. Covered services will thus be unable to determine with certainty whether they are complying with the law.

The bill's requirements undermine user privacy and competition.

While well-intentioned, the bill's requirements will inevitably lead to the collection of more sensitive data from young users and their parents. Verifying that an individual is a user's parent entails collecting some form of identifying document, and any document capable of verifying parenthood is likely to contain sensitive information. Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[9] These dangers are only heightened by the bill's requirement that covered services retain such data. Such dangers are far from hypothetical: several of the most devastating data breaches in recent years were caused by lawmakers forcing companies to collect sensitive age assurance data from their users.[10]

---

[5] *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).
[6] *See, e.g.*, *id.* at 855-56.
[7] *See, e.g.*, *Packingham v. North Carolina*, 582 U.S. 98, 105-06 (2017).
[8] *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011).
[9] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[10] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.

Additionally, excessive monitoring has been shown to negatively affect young people's mental health and development.[11] This provision is therefore at odds with the bill's ostensible goal of protecting young users online.

The bill's age assurance provisions will be detrimental as well if they are interpreted to require the collection of sensitive user data. There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[12] and small business sustainability.[13] Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[14]

Moreover, such mandates can undermine competition. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.[15] The report found that "smaller companies may not be able to sustain their business" if forced to determine user ages, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[16]

This danger is particularly acute given the bill's requirement that covered services update their estimates of users' ages every 100 hours, an excessive compliance obligation that provides no compensating benefit to consumers and would prove especially burdensome for smaller businesses. To avoid these problems, CCIA recommends explicitly allowing self-attestation as a reasonable method of age assurance under this bill, as this method does not require the collection of sensitive user data and allows small businesses to better compete with their more established counterparts.

To avoid restricting teens' access to information, HB 227 should regulate users under 13 rather than 18 in accordance with established practices.

HB 227 defines "minor" as an individual less than 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a

[11] *See, e.g.*, Hannah Quay-de la Valle, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. for Democracy & Tech. (May 5, 2022), https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/ (finding that "Monitoring programs, if not carefully implemented, can stifle growth and leave students vulnerable to the chilling effect, placing their mental health at risk").
[12] Kate Ruane, *CDT Files Brief in NetChoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[13] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[14] *See, e.g.*, Fair Information Practice Principles (FIPPs), Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; Principle (c): Data Minimisation, U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[15] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[16] *Id.* at 10.

school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We would suggest changing the scope of covered users to be minors under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[17] This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

Terms such as "addictive" in this online context lack adequate scientific foundation.

HB 227 prohibits the use of several design features that it deems "addictive." The term "addictive," however, has no established meaning in the online context. Humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. Compulsive behaviors could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, certain regular activities do not necessarily amount to "addictions". The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR)* declined to include definitions for "Internet gaming disorder," "Internet addiction," "excessive use of the Internet," or "excessive use of social media," noting that "[g]ambling disorder is currently the only non-substance-related disorder included in the *DSM-5-TR* chapter 'Substance-Related and Addictive Disorders.'"[18]

The connected nature of social media has led to allegations that online services are negatively impacting teenager's mental health. Researchers argue that this theory is not well supported by existing evidence and often mirrors the "moral panic" associated with new technologies. Studies from the leading universities indicate that depression has virtually no causal relation to special media use. The effects are nuanced,[19] individualized, reciprocal, and gender-specific.

This complexity was reinforced when the U.S. Surgeon General released an Advisory entitled *Social Media and Youth Mental Health*. Many were quick to highlight only the harms and risks it detailed. However, the Advisory is much more complex and also discusses many potential benefits of social media use among children and adolescents. For example, the Advisory concludes that social media provides young people with communities and connections with others who share identities, abilities, and interests.[20] It can also provide access to important information and create spaces for self-expression. Research further details that social media can especially benefit marginalized youth, including racial, ethnic, sexual, and gender minorities, as online peer support can mitigate the stresses they face.[21]

---

[17] *See* 15 U.S.C. § 6501(1).
[18] Am. Psychiatric Ass'n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).
[19] Amy Orben et al., *Social Media's Enduring Effect on Adolescent Life Satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[20] Off. of the Surgeon Gen., U.S. Department of Health & Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, *Social Media Has Both Positive and Negative Impacts on Children and Adolescents* (2023), https://www.ncbi.nlm.nih.gov/books/NBK594763/.
[21] *Id.*; *see also* Jennifer Marino et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, J. Med. Internet Rsch. (Sept. 22, 2021), https://www.jmir.org/2022/9/e38449.

The private right of action would result in the proliferation of frivolous lawsuits and questionable claims, and exorbitant statutory damages.

HB 227 permits users to bring legal action against persons that have been accused of violating new regulations. The bill would provide children and parents with "a private right of action for declaratory or injunctive relief, damages, including harm to mental health and emotional distress, court costs, reasonable attorney's fees, and any other appropriate relief as a result of any negligent, reckless, or intentional violation," and for reckless or intentional violations, a civil penalty of the greater of $10,000 or actual damages. Nowhere else in the bill does the "harm to mental health and emotional distress" language appear, and it is not defined.

By creating a new private right of action, the measure would open the doors of Kentucky's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. This danger is particularly acute given the vaguely defined requirements noted above. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individuals in Kentucky, disproportionately impacting smaller businesses and startups across the Commonwealth. Accordingly, CCIA recommends granting the Commonwealth exclusive authority to enforce these requirements.

* * * * *

CCIA remains committed to working with the Kentucky General Assembly on constructive, evidence-based approaches to online safety. However, because HB 227 relies on unconstitutional speech restrictions and mandates privacy-invasive age verification, we must respectfully oppose the bill in its current form.

We thank you for your consideration of these comments.

Sincerely,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association