Written Testimony of Holly Grosshans

Senior Counsel, Tech Policy; Common Sense Media

Before the Maryland House Economic Matters Committee

regarding

"Maryland Online Data Privacy Act of 2024"
Bill No: HB0567

Position: Favorable

February 13, 2024

My name is Holly Grosshans. I am the Senior Counsel for tech policy at Common Sense Media, the nation's largest organization dedicated to ensuring that children and families thrive—and remain safe—in the rapidly-changing digital age. In Maryland alone, more than 2,000 teachers have registered to teach Common Sense Media's digital citizenship and literacy materials to their students in nearly 800 Common Sense recognized schools. But perhaps most importantly, I am the mother of two elementary school-age children and I care deeply about the privacy and well-being of my kids, and the millions of children like them, who are depending on this committee and this legislature to establish desperately-needed protections for their online safety, privacy, and overall well-being.

My testimony will focus on the consumer risks associated with unregulated online data privacy, the potential harms of personal data processing and targeted advertising to kids and teens, and how the Maryland Online Data Privacy Act will be an effective tool to protect Marylanders' online privacy.

I. Introduction: Internet privacy is a pressing issue; states are beginning to regulate

Common Sense Media strongly supports the proposed Maryland Online Data Privacy Act of 2024 (HB0567). Recent research makes it clear that concerns about internet privacy are growing—as many as 71% of Americans are worried about how companies are using their personal data, while 89% are somewhat or very concerned about social media companies collecting data about kids.[1] As of this writing, 13 states[2] have passed comprehensive data privacy bills while at least 20 more[3] have proposed bills that would particularly strengthen kids'

[1] Colleen McClain et al., *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023).
[2] F. Paul Pittman, *US Data Privacy Guide*, White & Case (Feb. 5, 2024).
[3] Kirk J. Nahra, *State Child Privacy Law Update*, WilmerHale (Feb. 28, 2023).

data privacy protections. Common Sense believes that Maryland's kids and families also deserve strong data privacy protections and so supports the Maryland Online Data Privacy Act.

Among the provisions of this bill that we particularly support, this bill offers strong protections against the sale of user data and targeted advertising, will prevent companies from pretending they don't have kids on their sites, and will protect teenagers' privacy and create additional benefits for safety. While we recommend that the bill could be further strengthened by clarifying the ban on targeted advertising to children under 13 by changing 14-4607(A)(5) to remove "at least 13 years old and" so that it applies to all consumers under 18, Common Sense Media offers our unambiguous support for your bill.

II. Background: Marylanders, and especially kids, suffer from a lack of data privacy

There is no comprehensive federal data privacy law, and the only federal children's data privacy law is 25 years old. Maryland does not have its own online data privacy law for adults or for minors. This leaves Marylanders in significant need of this legislation.

The vast majority of Americans believe that they have little or no control over their personal data.[4] Many report that companies are too opaque about what they do with user data for individuals to even have a say, and the majority of surveyed Americans who report taking their data privacy seriously think that even their making good privacy decisions would have little or no impact on whether companies actually collect their data. Recent consumer research suggests Americans are troubled by this state of affairs—74% of whom rate their data privacy as highly important to them.[5] But there are also practical concerns: lack of robust data privacy increases the risk of abuse, fraud, and identity theft, and may dissuade users from visiting certain sites or taking advantage of certain internet resources.

Data privacy concerns are particularly acute for kids. Recent research suggests that kids' internet usage is at an all-time high.[6] Teens are spending an average of 4.5 hours per day on their phones, with about a quarter of them spending as much as 5 to 8 hours in front of their screens every day. Nearly half of teens report that they feel addicted to their phones.[7] Teens connect with each other through these platforms at higher rates than any other group, report that these platforms form a larger part of their social life than any other group, and have outsized levels of difficulty stopping technology use once they've started.[8] And kids and teens must use technology for educational purposes, meaning that K–12 students in Maryland and elsewhere don't have the option to avoid tech and the data privacy concerns it raises. As a result, teens and kids are being surveilled by platforms and having their behavior tracked, packaged, and sold to third-parties at an alarming rate.

---

[4] McClain et al., *supra*.
[5] *What Is Data Privacy & Why Is It Important?*, Dashlane (Apr. 18, 2023).
[6] Jenny S. Radesky et al., *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*, Common Sense (2023).
[7] Kim Chronister, *Teen Phone Addiction*, Key Healthcare (May 4, 2022).
[8] *Id*.

Worse still, teens are more susceptible than older users to targeted ads and to data mining. Teens are far more likely to overshare information about themselves online thanks in part to their unique social relationship with media platforms, and in part to the underdevelopment of the parts of their brain responsible for dealing with judgment and long-term consequences.[9] Research suggests teens are less able to identify targeted advertising and, in many cases, don't fully understand that features like algorithmic personalization both require large amounts of their data to function properly and make it harder for teens to stop or decrease screen time.[10]

Data privacy regulation is sorely needed. As Americans seek greater protection for their online data and wish for greater control over how their data is used, trust in online companies and their ability to self-regulate is at an all-time low. Decisive regulatory action is the only option and Common Sense supports the Online Data Privacy Act as exactly this kind of action.

III. Common Sense Media Supports the Maryland Online Data Privacy Act of 2024

The Online Data Privacy Act is essential legislation to protect online privacy for kids and their families. We point to three provisions that, as we understand the legislation, provide robust protections.

Strong Protections Against Sale of User Data and Targeted Advertising — Section 14-4607(A) broadly prohibits and limits the collection of personal data "for the sole purpose of content personalization or marketing" without consent from the user. It further bans outright the sale of "sensitive data" which includes data of children under 13. Common Sense believes that these provisions are essential to protecting privacy online. They protect children, teens, and everyone from having their behavior tracked, processed, and monetized. The provisions enable adult users to have control over how their data is used by requiring their consent to process their data. And they allow consumers autonomy in what they choose to reveal to companies; permitting users to make case-by-case judgment calls about the value of the personalization service relative to their data privacy.

The bill also safeguards teens. It only permits sale of teen data with user consent, and creates a blanket ban on the processing for purposes of targeted advertising of teens' (aged 13-18) user data. That there is no consent provision for teens to opt-in to processing and sale of their data is an important safeguard for teens. Otherwise, teens who are primed to engage in risky behavior for short-term rewards may be tempted to give up privacy in order to maximize the personalization of their user experience but, as mentioned, may not fully be able to grasp the consequences of doing so.

As noted above, while we support this section of the bill we believe it could be strengthened. The bill could be clarified with respect to targeted advertising and children under 13; it is not clear that targeted advertising is outright prohibited with respect to such users as it is with

[9] Devorah Heitner, *Here's why your teen overshares online, and why that could be good*, Washington Post (Sept. 15, 2023).
[10] Samuel Levine, *Protecting Kids from Stealth Advertising in Digital Media*, FTC (Sept. 2023).

teenagers. Specifically, we recommend changing 14-4607(A)(5) to remove “at least 13 years old and” so that it applies to all consumers under 18. This would maximize the Bills’ protection of the most vulnerable users.

Prevent Companies From Pretending They Don’t Have Kids On their Sites — Throughout the bill, heightened protections apply when platforms “know or should have known” that a user was either a child (under 13) or a teen (13-18). Common Sense emphasizes its support for this ‘knew or should have known’ language throughout the bill. The ‘should have known’ portion powerfully holds companies to account by preventing them from pleading ignorance of violations. Without such language, platforms are incentivized to purposefully turn a blind-eye to user age so as to claim they ‘didn’t know’ that their data collection activity swept in children or teens. The ‘should have known’ language creates a statutory safeguard against that ignorance defense by holding companies to what they could reasonably know, not just what they choose to note in their records.

Protect Teenagers’ Privacy and Create Knock-on Benefits for Safety — The bill gives heightened protections not just to children 12 and under, but also to teenagers. This fills an important gap in the federal Children's Online Privacy Protection Act (COPPA), which currently applies only to children under 13 years of age. In particular, several aspects of the Online Data Privacy Act balance the interests of protecting teens’ data privacy while also encouraging them to develop autonomy concerning their own user data.

As referenced above, teens in particular are spending more and more time on their phones and report skyrocketing rates of digital addiction. This state of affairs is no idle coincidence; social media companies’ business model—based on targeted advertising and data collection—encourages the production of addictive design features such as endless scrolling pages and notification nudging. Common Sense additionally supports this bill to help change those incentives. A general prohibition on the use and sale of consumer data, and children’s data in particular, would curtail the incentive to create features that encourage users to spend more time on their phones.

IV. Conclusion

Marylanders’ online data privacy is currently underprotected and susceptible to use or abuse by companies and others. This presents a particular threat for Maryland’s kids and teens, who are the most vulnerable with respect to data breaches and targeted advertising. The Maryland Online Data Privacy Act creates a stalwart framework for protecting adults’ and childrens’ data privacy, while balancing consumers’ interests in personalized user experiences and parents’ interests in their kids’ online development. Common Sense applauds the bill sponsors for bringing forward this important legislation at a critical time for children and teens online and we urge the committee and the House of Delegates to approve this important measure.