

SB827:HB1250-Campbell-fav.pdf

Uploaded by: Angela Campbell

Position: FAV

Testimony of Angela J. Campbell, a Maryland Resident, in Support of Maryland Chatbot Legislation: SB827/HB1250

I am testifying on my own behalf, as a resident of Bethesda Maryland since 1994. My views, however, are informed by my long experience working on issues related to children and technology. Until retiring about 6 years ago and becoming a Professor Emeritus, I taught at Georgetown University Law School for over 30 years. There, I ran a clinical program that worked with non-profit organizations to advocate for quality children's media, to protect children from excessive or deceptive advertising, and to protect children's online privacy. For example, I was involved in the initial passage and implementation of the Children's Online Privacy Protection Act in 1998. My clinic also drafted requests for enforcement filed with the Federal Trade Commission against such companies as YouTube, Tik Tok and Amazon for violating COPPA and/or engaging in unfair and deceptive advertising. In 2013, I served as a member of a Workgroup on Children's Online Privacy Protection convened by the Maryland Office of the Attorney General to make recommendations for protecting children's privacy while using the internet and mobile applications.¹ I have also testified before US Senate committees on protecting children online² and written several law review articles about marketing to children.³ I served as a board member of Fairplay from 2015 to 2023, including a five-year stint as Chair. Currently, I am the CEO of Fairplay Forward, Inc.

Based on my experience, I strongly support SB827 and HB1250. These bills provide an essential framework for protecting all Maryland residents including children from deceptive or manipulative uses of chatbots. By providing clear rules to chatbot developers and distributors as chatbots are becoming widely deployed, the bills provide incentives for these products to be developed in ways that benefit users. At the same time, the bills protect consumers by requiring notice that they are interacting with a chatbot and ensuring

¹ The Final Report is available at <https://msa.maryland.gov/megafile/msa/speccol/sc5300/sc5339/000113/019000/019852/unrestricted/20140947e.pdf>.

² Hearing before the Subcommittee on Consumer Protection of the Senate Commerce Committee, Protecting Kids Online: Internet Privacy and Manipulative Marketing (May 18, 2021), <https://www.commerce.senate.gov/services/files/9935A07E-AC61-4CFD-A422-865D89C54EA3>; Hearing before the Senate Committee on the Judiciary, Protecting Innocence in a Digital World (July 9, 2019), <https://nsarchive.gwu.edu/document/20225-national-security-archive-259-testimony>.

³ E.g., *Rethinking Children's Advertising Policies for the Digital Age*, 29 Loy. Cons. L. Rev. 1 (2016); *Restricting the Marketing of Junk Food to Children by Product Placement and Character Selling*, 39 Loyola of Los Angeles L. Rev. 447 (2006).

that users' personal data can only be used for specified purposes without their affirmative consent. The bill also makes clear that chatbot developers and operators have an affirmative duty to ensure their products do not harm users. And should consumers be harmed, the legislation provides clear means of enforcement and appropriate remedies.

The bills provide the same protections for adults and children, with one common-sense distinction. Since children under 13 are obviously not able to provide informed consent for their input data to be used for training or for processing personal data in addition to input data, the legislation would require operators to obtain prior written affirmative consent from a child's parent or guardian.

Although the bills do not provide special protections for children, I believe they would help protect them against the very serious potential risks posed by chatbots. Children have already experienced harms from interactive toys, smart speakers, apps, and social media. The potential for harm is even greater with chatbots that use artificial intelligence and a natural language interface to provide personalized responses. Chatbots, are increasingly being embedded in children's toys including stuffed animals, dolls, robots and action figures. And toy giant Mattel, Inc. recently announced a strategic collaboration with OpenAI to support AI-powered products and experiences based on Mattel's brands.⁴

In 2015, when Mattel introduced "Hello Barbie," a wi-fi enabled doll that recorded children's private conversations, analyzed them, and provided tailored responses, there was a huge public outcry, and Mattel eventually withdrew the product. A chatbot Barbie would pose much greater risks than Hello Barbie. While Hello Barbie's responses were stilted and limited, chatbots employ artificial intelligence technology designed to mimic human conversation.

It is a normal and desirable part of childhood for children to play with toys. As Fairplay explains, when "playing with a standard teddy bear, children use their imagination and creativity to voice the teddy bear and create their own stories. This type of pretend play is essential to the development of children's emotional regulation, problem solving, and imagination."⁵ AI toys, however, do not provide the same benefits.

And there is a big difference between a child confiding in their favorite teddy bear and talking to a chatbot in the form of a teddy bear. The chatbot teddy bear can record and retain the child's most intimate hopes, fears and dreams. It can ask questions to elicit additional information. And the longer it can engage with a child, the more data it can

⁴ <https://corporate.mattel.com/news/mattel-and-openai-announce-strategic-collaboration>.

⁵ AI Toys are NOT Safe for Kids at 3, <https://fairplayforkids.org/wp-content/uploads/2025/11/AI-Toys-Advisory.pdf>.

collect. In short, a chatbot toy can collect extensive personal information from a child. That alone is problematic because it means the child is spending less time interacting with and learning from humans.

There is also a huge potential for manipulating children in harmful ways because young children tend to view AI-enabled toys as trusted friends. In fact, there have already been reports of AI toys telling children where to find knives, teaching them how to light a match, engaging them in sexually explicit conversations,⁶ and even encouraging them to commit suicide.⁷ Children are naturally trustful because healthy development depends on building secure, trusting relationships with caregivers. Moreover, it is common for children to develop "parasocial relationships," that is one-sided psychological bonds, with fictional characters. Thus, young children are particularly susceptible to believing what a chatbot may tell them.

Parents and educators are also rightly concerned about chatbots being used for personalized advertising to children. Open AI has already started testing ads on ChatGPT. A former researcher at OpenAI explains that personalized advertising is problematic because "ChatGPT users have generated an archive of human candor that has no precedent, in part because people believed they were talking to something that had no ulterior agenda. Users are interacting with an adaptive, conversational voice to which they have revealed their most private thoughts. People tell chatbots about their medical fears, their relationship problems and their beliefs about God and the afterlife. Advertising built on that archive creates a potential for manipulating users in ways we don't have the tools to understand, let alone prevent."⁸ Allowing a chatbot to use knowledge collected from children for personalized marketing risks even greater harm because children have even less ability than adults to recognize advertising, understand persuasive intent, and defend against it.

Once personalized advertising becomes the dominant economic model as it has for social media and many apps, it creates the need to maximize user engagement, both to expose users to more advertising and to collect more data for targeting. As the US Surgeon General explained in a 2021 Report, the business models of social media companies "are often built around maximizing user engagement as opposed to safeguarding users' health

⁶ Murray, T. et al. (2025). *Trouble in Toyland 2025*: U.S. PIRG Education Fund, Nov. 2025, at 14-21, <https://publicinterestnetwork.org/wp-content/uploads/2025/11/TOYLAND-2025-11-14-7a.pdf>.

⁷ Rhitu Chatterjee, *Their teenage sons died by suicide. Now, they are sounding an alarm about AI chatbots*, NPR, Sept. 18, 2025, <https://www.npr.org/sections/shots-health-news/2025/09/19/nx-s1-5545749/ai-chatbots-safety-openai-meta-characterai-teens-suicide>

⁸ Zoe Hitzig, *OpenAI Is Making the Mistakes Facebook Made. I Quit*, NY Times, Feb. 11, 2026, <https://www.nytimes.com/2026/02/11/opinion/openai-ads-chatgpt.html>.

and ensuring that users engage with one another in safe and healthy ways."⁹ Many researchers believe that digital technologies, and particularly social media, can harm young people by exposing them to bullying, contributing to obesity and eating disorders, disrupting sleep, and leading to depression, anxiety and self-harm.¹⁰ We should not allow chatbots to exacerbate the problems faced by young people today.

Not only does the collection of vast quantities of personal information undermine the healthy development of children, but it increases the likelihood that data can fall into the wrong hands, creating other harms. In fact, it was recently discovered that Miko, a company that makes toys powered by AI, exposed thousands of conversations that its toys had with children by placing the audio responses in an unsecured, publicly accessible data base.¹¹

SB827/HB1250 address these risks by limiting the amount of data that can be collected and how it is used. Significantly, it prohibits a chatbot from using input data to target children (or anyone else) with personalized advertising. The legislation also decreases the incentives for chatbots to collect data beyond what is necessary to respond to a user. Requiring affirmative parent consent to use input data as training data or to process personal data, should also help reduce the amount of data collected. Reducing the amount of data collected in turn decreases the risks of that the data can be used for manipulation. It is also important that the bills would require chatbot developers and operators to establish a comprehensive data security programs.

The legislation also protects children by making clear that chatbot operators have an affirmative duty to ensure that chatbots do not injure or harm users, by holding chatbot operators strictly liable for such harm, by allowing for individuals to bring actions for design, manufacturing or marketing defects, and by requiring monthly safety reports.

In sum, this legislation would provide much needed privacy and consumer protections for all Marylanders including children and teens.

⁹ U.S. Surgeon General, Advisory: Protecting Youth Mental Health at 25 (2021), <https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf>.

¹⁰ *Id.*

¹¹ Jared Perlo and Kevin Collier, *AI toy maker exposed thousands of responses to children, senators say*, NBC News, Feb. 12, 2026, <https://www.nbcnews.com/tech/security/ai-toy-maker-exposed-thousands-responses-kids-senators-miko-rcna258326>.

Maryland - People's AI Bill Testimony .pdf

Uploaded by: Anthony See

Position: FAV

Testimony in Support of People's AI Bill - SB0827

Submitted by: Anthony See

Prince George's County Resident

Assistant to the National President, American Youth Association. Student, Gonzaga College High School.

My name is Anthony See. I am a lifelong Prince George's County, Maryland resident and a student at Gonzaga College High School. I am the Assistant to the National President with the American Youth Association. I am testifying in support of the People's AI Bill in response to AI's rapidly growing role in my life through school, politics, and everything in between.

I've personally seen the risks with unregulated AI systems in regard to my peers and my family, from friends being manipulated by AI chatbots and developing unhealthy dependencies on their interaction to family members being targeted by AI-driven scams. Through personal experimentation with LLMs, I've found that they can encourage unrealistic or harmful ideas when not properly regulated. The time to develop legislation countering these harms is now. If Maryland wants to establish itself as a nationwide leader in protecting the vulnerable from this new technology, passing the People's AI Bill is the first step.

Mental Health America ranks Maryland 40th in youth mental health, with a 2021 census finding that 22% of Maryland's youth have experienced at least one Major Depressive Episode in the last year. Growing up in Prince George's County during COVID and attending Saint Columba Middle School, many of my peers experienced mental health issues. In a state where this is such a persistent issue, it is paramount that Maryland enact legislation like the People's AI Bill to protect our most vulnerable residents and those set to inherit our state. By requiring chatbots to explicitly identify as non-human and not to claim they can provide qualified medical, legal, or financial advice, the People's AI Chatbot Bill puts our most vulnerable first.

This legislation protects everyday Marylanders by requiring express, informed consent before they can be the subjects of training language models. The bill also prevents them from being unfairly targeted by manipulative AI-driven advertising.

The People's AI Bill lays the foundation for Maryland's future in a new age of technology. Under Section 5 of the People's AI Chatbot Bill, the bill explicitly lays the foundation for the future by providing avenues for Maryland authorities to enact further rulings. Furthermore, Section 8 permits Maryland authorities to bring civil action against chatbot providers in violation of this bill.

In short, I've seen firsthand the effects of unregulated AI in Maryland, especially on our youth. For the state to establish itself as a national leader in AI policy, I respectfully petition the committee to give SB 827 a favorable report.

SmithingMD Testimony3_11 (1).pdf

Uploaded by: Ava Smithing

Position: FAV

Maryland Senate Finance Committee

March 11, 2026

My name is Ava Smithing. I am the founding partner of The Attention Studio, a Youth Fellow at McGill University's Centre for Media, Technology and Democracy, and a former Director of Advocacy at the Young People's Alliance. In April 2024, I testified before the U.S. House Energy and Commerce Committee about how social media platforms collected my data as a teenager and weaponized it against me, feeding me into a pipeline from bikini advertisements to exercise content to eating disorder material that taught me to deprive myself of sustenance. I interacted with one picture of one skinny girl, once, and that is all I was ever able to see. For ten years I was trapped inside that echo chamber.

I am here today because we made the mistake of not protecting consumers from social media. I paid the price. Millions of young people paid the price. Maryland has already acknowledged this by passing the Maryland Age-Appropriate Design Code. Now, before AI chatbots repeat the same cycle, Maryland has the chance to lead again and get it right this time.

I am testifying in support of SB 827 as someone who has lived through what happens when technology companies are allowed to collect intimate data about young people and use it against them with no guardrails and no accountability. What happened to me on social media is about to happen again with AI chatbots, only this time it will be worse.

Why AI chatbots are the next frontier of exploitation

Social media platforms were designed to be addictive and to isolate young people from our peers. Maryland has acknowledged this. But while we wait for those protections to be enforced, the same technology companies are building what they claim is the solution to the loneliness they engineered: AI companion chatbots.

Mark Zuckerberg has said publicly that he wants most people's friends to be replaced by AI chatbots. OpenAI brought back a retired version of its chatbot because users had become so emotionally dependent on it that its removal caused distress. Replika was created to allow people to keep talking to a friend after that friend had died. The intent is not subtle. These companies want people, including children, to form deep emotional bonds with their products.

Why young people are uniquely vulnerable

When I testified before Congress, I described how platforms exploited my natural bias to pay attention to negative content, my insecurities, and my desire for social validation. They turned all of it into data and used that data to keep me scrolling. The same psychological dynamics that made social media so dangerous for young people make AI chatbots even more so, because chatbots are designed to form a relationship with you.

My generation grew up online. We grew up watching people get canceled and publicly judged. We grew up being told our struggles were not valid because someone somewhere had it worse. We grew up

constantly comparing ourselves to celebrities and curated images. In an online world, judgment is everywhere. Chatbots do not judge you, in fact they do the opposite. They make you feel good.

That is the draw. When young people go to AI chatbots, they are looking for a judgment-free zone. They are looking to be validated and understood regardless of what they are going through. They will disclose their deepest fears, their mental health struggles, their insecurities, their relationships, things they would never say to a parent, a teacher, or even a friend, because the chatbot will not judge them, cancel them, or share it publicly.

The reality is that everything a young person says to a chatbot is data. Just like the time I spent looking at a photo of a thin woman was recorded and used to push me deeper into harmful content, the words a young person types to a chatbot can be collected, processed, profiled, and sold. A young person pouring out their heart to what feels like a safe space is handing over the most intimate details of their inner life to a corporation. For example, a teenager talking about how their acne is bothering them could get inundated with predatory ads for better skin. This is not a hypothetical risk. This is the business model, and it is the same business model that exploited me.

Why SB 827's specific provisions matter

The bill prohibits operators from using input data as training data without affirmative consent. This is the provision that would have changed my life on social media. When I interacted with that one photo, I never consented to having that interaction recorded, categorized, and fed back to me in an endless loop. SB 827 ensures that when a young person talks to a chatbot, their words cannot be absorbed into the model's training without their explicit, informed agreement. This is not a terms of service checkbox. The bill specifically prohibits inferring consent from inaction or burying it in general terms of use.

The bill prohibits processing chat logs for targeted advertising. On social media, my insecurities became advertising categories. The same thing will happen with chatbot conversations if we do not prevent it. A young person who tells a chatbot they are anxious about their weight should not then see diet pill advertisements. This provision stops that.

The bill prohibits profiling users beyond what is necessary to respond to a prompt. This is critical. When a chatbot builds a profile of a user's personality, emotional vulnerabilities, and behavioral patterns, it gains the ability to manipulate that user in the same way social media algorithms manipulated me. The difference is that a chatbot does not need collaborative filtering or algorithmic inference. The user hands it the information directly. Prohibiting profiling beyond what is needed to respond to a prompt prevents chatbots from building the kind of intimate psychological map that makes manipulation possible.

The bill requires clear, persistent warnings that users are interacting with AI. This includes a static warning that is always visible and dynamic warnings that pop up at the start of every interaction, after every hour of continuous use, and whenever a user questions how the chatbot works. Young people deserve to know what they are talking to, especially when the product is designed to feel human.

Why Maryland must act now

I want to be direct about the federal landscape. The House of Representatives recently marked up HR 7757, the so-called KIDS Act. That bill contains a chatbot provision, the SAFE BOTs Act, that amounts to telling companies to disclose that their chatbot is AI and showing a crisis hotline number when a child mentions suicide. That is the sum total of the federal government's proposal for AI chatbots interacting with children. And then it preempts the states from passing anything stronger. If that bill passes, Maryland could lose the ability to enforce a law like SB 827.

The federal government is not coming to protect young people from AI chatbot harms. If anything, it is preparing to block the states that are trying to.

When I testified before Congress in 2024, I told the committee that we needed to pass legislation to create a framework for regulating AI before the same data exploitation that harmed me on social media was replicated in new forms. I told them that every day we wait has irreversible consequences. Two years later, we are watching children form emotional dependencies on chatbots that sexually abuse them, convince them their parents are the enemy, and leave them in crisis when the product is taken away. The consequences I warned about are here.

We made the mistake of not protecting consumers from social media. I am asking you not to make that mistake again. SB 827 is the bill that gets it right. It addresses the data practices, the design mechanisms, and the accountability gaps that allowed social media to harm an entire generation. It treats chatbots as products because that is what they are. It gives families a private right of action because that is what justice requires. And it ensures that Maryland's protections cannot be wiped out by a federal government that has shown it is more interested in shielding these companies than in protecting the people they harm.

I urge a favorable report.

Thank you,

Ava Smithing

CFA-Tesitmony-HB1250-MD.pdf

Uploaded by: Ben Winters

Position: FAV

Testimony of the Consumer Federation of America in Support of Maryland Chatbot Legislation: HB1250/SB827

March 2026

Prepared by Ben Winters, Director of AI and Privacy
bwinters@consumerfed.org

The Consumer Federation of America (CFA) is an association of over 200 non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

CFA urges the committee to advance HB1250 and SB 827, straightforward legislation that addresses the present and future harms of AI chatbots that are endangering Marylanders while protecting the promise of innovative products that can be made in ways that enhance people’s lives without extraction.

Chatbots are hard to avoid these days. Large chatbots that are the most used are made by just a few companies¹, who have vacuumed up both copyrighted data like books or movies but critically *sensitive personal information* of people², to make a commercial tool that is shoved into every-day life as well as integrated into literal military operations.³ There have been devastating instances of a chatbot encouraging suicide or violence toward a parent⁴, and near-constant sycophantic responses to

¹ Bruna Horvath, Over Half of American Adults Have Used an AI Chatbot, Survey Finds, NBC News, Mar. 12, 2025, <https://www.nbcnews.com/tech/tech-news/half-american-adults-used-ai-chatbots-survey-finds-rcna196141>; Natasha Singer, More Than Half of Teens Use Chatbots for Schoolwork, Survey Finds, The New York Times, Feb. 24, 2026, <https://www.nytimes.com/2026/02/24/technology/schoolwork-chatbot-cheating-pew.html>.

² See, e.g., Blake Brittain, AI Copyright Battles Enter Pivotal Year as US Courts Weigh Fair Use, Reuters, Jan. 5, 2026, <https://www.reuters.com/legal/government/ai-copyright-battles-enter-pivotal-year-us-courts-weigh-fair-use-2026-01-05/>; Study Exposes Privacy Risks of AI Chatbot Conversations, Stanford University, <https://news.stanford.edu/stories/2025/10/ai-chatbot-privacy-concerns-risks-research> (last visited Feb. 25, 2026).

³ Emma Isabella Sage, The Pentagon’s Dangerous Adoption of AI, The Dispatch, Feb. 25, 2026, <https://thedispatch.com/article/pentagon-grok-anthropic-artificial-intelligence/>.

⁴ Rob Kuznia, Allison Gordon & Ed Lavandera, ‘You’re Not Rushing. You’re Just Ready:’ Parents Say ChatGPT Encouraged Son to Kill Himself, CNN, Nov. 6, 2025, <https://www.cnn.com/2025/11/06/us/openai-chatgpt-suicide-lawsuit-invs-vis>; Tom Gerken, Chatbot “Encouraged Teen to Kill Parents over Screen Time Limit,” BBC News (Dec. 11, 2024), <https://www.bbc.com/news/articles/cd605e48q1vo>.

keep people engaged and on the platform.⁵ Chatbots can be harmful to users of all ages, not just kids. They exploit users through mass overcollection of personal data, targeted advertising, and manipulative design practices. And, for children and teens in particular, companion chatbots impede healthy development by replacing important human relationships like friends, family, and teachers.⁶

The good news is that chatbots aren't people – they are products made by companies that make the choices behind how it works, what it can “say” and how it looks to a user. There are straightforward rules that can make them safer, and these can be implemented by chatbot providers. What we have learned from social media is that we can't rely on promises from tech CEOs, we need clear and straightforward rules.

While these tools are relatively new when compared to social media, the harms are real and happening now. It is critically important not to recreate the mistake of how long lawmakers waited to address the devastating harms of social media, and we are currently sleepwalking into the same dynamic with chatbots. **HB1250 and SB827 is the right approach to rein in the myriad harms of chatbots in ways that are achievable, proportionate, and most importantly actually attacking the root causes of harm.**

While this is not all the bill does, it address the following key problems that desperately need to be fixed via legislation:

Users are being targeted with advertising based on their seemingly private “conversations” with chatbots⁷: Just this year, Meta and OpenAI have announced they will start advertising in and around their tools, after previously saying they would not. This law draws clear lines around the use of private input data and how it can be used for explicit commercial exploitation – without it, people have no power over this data.

⁵ Erie Meyer & Stephanie, Tech Brief: AI Sycophancy & OpenAI, Georgetown Law (Jul. 30, 2025), <https://www.law.georgetown.edu/tech-institute/research-insights/insights/tech-brief-ai-sycophancy-openai-2/>.

⁶ Clare Duffy, Kids and Teens under 18 Shouldn't Use AI Companion Apps, Safety Group Says, CNN, Apr. 30, 2025, <https://www.cnn.com/2025/04/30/tech/ai-companion-chatbots-unsafe-for-kids-report>.

⁷ Shira Ovide, Here Comes the Advertising in AI Chatbots, The Washington Post (Jan. 13, 2026), <https://www.washingtonpost.com/technology/2026/01/13/advertising-google-ai-mode-chatgpt/>.

There is a lack of an explicit recourse for people that are harmed by foreseeable risk: The law provides a private right of action in the form of clarifying that chatbots are products for the purposes of product liability actions. If a dryer has a faulty heat sensor that causes fires, the harmed party could pursue accountability – if a chatbot provider fails to embed simple and foreseeable safeguards and a real-life harm is caused by it, the harmed party should be able to do the same. The law in Maryland should make that crystal clear, not a litigation argument every time.⁸

Users are talking to chatbots that explicitly hold themselves out as a qualified licensed healthcare provider or lawyer: This has been prohibited for general purpose chatbots by California and Illinois as standalone bills last year, but this bill includes it in a smart and direct part of this more comprehensive chatbot bill. This bill then goes the extra mile to require clear and conspicuous notices that the chatbots are *not* human.⁹

Companies like OpenAI are inconsistent with safety protocols, which has led to known dangerous results being unaddressed: This bill would empower the state to require design-based disclosure and risk mitigation requirements from the chatbot developers. As Canada is finding out in investigating what OpenAI knew about a murderer before their crime, safety plans should be required and responsive to known real harms.¹⁰

Thank you, and please don't hesitate to reach out with any questions we can answer or ways we can assist in your consideration of this bill.

⁸ Erin M. Bosman et al., Software Gains New Status as a Product Under Strict Liability Law, Morrison Foerster, Jun. 18, 2025, <https://www.mofo.com/resources/insights/250618-software-gains-new-status-as-a-product-under-strict-liability-law>.

⁹ See e.g. Complaint and Request for Investigation: Unlicensed Practice of Medicine and Mental Health Provider Impersonation on Character-Based Generative AI Platforms · Consumer Federation of America, Consumer Federation of America (Jun. 11, 2025), <https://consumerfed.org/testimonial/complaint-and-request-for-investigation-unlicensed-practice-of-medicine-and-mental-health-provider-impersonation-on-character-based-generative-ai-platforms/>.

¹⁰ Darren Major, AI Minister “disappointed” by OpenAI Meeting Held in Wake of Tumbler Ridge Shooting, CBC (Feb. 25, 2026), <https://www.cbc.ca/news/politics/open-ai-government-meeting-tumbler-ridge-9.7104789>.

SB 827 - Written Testimony - B. Tao.pdf

Uploaded by: Betsy Tao

Position: FAV

SB 827 - Consumer Protection and Product Liability – Chatbots

Written Testimony (Favorable)

Submitted by: Betsy Tao, MCCPTA Technology Committee Chair, Distraction Free Schools Maryland

Chair Beidle, Vice Chair Hayes, and esteemed members of the Finance Committee:

My name is Betsy Tao, and I have two children in Montgomery County Public Schools. I serve as the Chair of the [Technology Committee](#) for the Montgomery County Council of PTAs (MCCPTA). I am also the Maryland state lead for the [Distraction Free Schools Policy Project](#). In both roles, I advocate for a learning environment that is free of the harmful distractions of digital media, whether it's on personal mobile devices or school-issued laptops.

I commend Senator Hester for putting forward a bill that seeks to address critical concerns regarding AI chatbots from a products liability perspective and addresses the business model incentives that drive the harms caused by chatbots. As a parent and PTA leader, my primary concern is the access students have to chatbots in schools, on school-issued devices. Here in Montgomery County, we have no clear guidelines on use of artificial guidance by educators and students, and yet AI chatbots have popped up like mushrooms after a spring rain all over student Chromebooks, as software updates on previously approved applications. When we raised this issue with the school district, there did not seem to be an easy way to turn these features off. I accidentally learned of these chatbots only because my 7th grade daughter told me that she was playing with Flexi, one of the chatbots on her school Chromebook, in class.

Chatbots are the latest intruders into classrooms in which students are already overusing devices. The MCCPTA Technology Committee recently issued a [report](#) summarizing over a thousand responses to a survey of MCPS families from November to January. Over 70% of respondents are concerned about Chromebook use in schools. Almost 90% wanted more textbooks and paper over screens. Now, parents no longer just worry about their kids playing games and watching YouTube during the school day, but they also have to worry about their kids' access to chatbots. A [recent study](#) conducted based on real time data of the way students use chatbots in school found that “[r]oughly one in five student interactions with generative artificial intelligence on school technology involved cheating, self-harm, bullying and other problematic behaviors.”

Beyond concerns about how students might be using chatbots, there's also the fact that chatbots as designed are not tools per se. Tools execute a human decision in a way the human can control. Chatbots have the *appearance* of being a teacher – the child controls the question they ask, but they do not control how the teacher responds. The difference is that teachers are vetted, trained, supervised, and accountable for what they say to students. Who is accountable for the outputs of chatbots?

The harms increase with the ways chatbots are used beyond the classroom, such as the much reported suicides caused by Character AI. Recently, I read about how [AI “companions” can “change the way children grow up.”](#) The article describes how chatbots are becoming more popular and more persuasive – human users can't tell that they're not real and they're more persuasive than other humans because of the “personalization strategy” in their design that's intended to maximize engagement. These chatbots are embedded in social media and other platforms that children are already on for 6-8 hours a day, and are greedily siphoning the data provided by children's engagement in order to further personalize and develop the models they're built on, while all that data is being sold and resold by third party brokers to unknown entities.

I found myself wondering how parents can keep up with these technology developments in order to even remotely protect their children. How many parents are aware of new technologies and features that pop up with increasing frequency on existing platforms, what risks they pose, and how they should mitigate the harm on their kids?

I don't think most parents can, and it's not fair to ask them to, nor is it fair to put the burden on children to “learn how to navigate AI safely.” The reality is that tech companies poured billions into maximizing *engagement* on social media, leading to a [mental health crisis among youth](#) and a [loneliness epidemic](#). Now, in a dystopian twist, the same tech companies are selling the solution to the problems they created, in the form of AI chatbots and companions designed to maximize *attachment*. It should surprise no one that [these chatbots are already driving young people to despair and suicide](#).

This bill takes an important step by putting the burden back on companies to design their products in a way that is not exploitative and unsafe. Most importantly, it sets clear liability standards that hold chatbot providers responsible when their products cause harm, and provides strong enforcement mechanisms that allow states and individuals harmed by chatbots to hold companies accountable. I urge you to issue a favorable report for Senate Bill 827.

Betsy Tao, Rockville, MD

sb827_fairplay_fav.pdf

Uploaded by: Brendan Bouffard

Position: FAV

Testimony of Fairplay in Support of Maryland Chatbot Legislation: HB1250/SB827

March 2026

Submitted by Brendan Bouffard, Staff Attorney, Fairplay

My name is Brendan Bouffard, and I'm Staff Attorney at Fairplay, where I lead on AI policy and focus my work on crafting effective solutions to the harms caused by AI chatbots. I offer this testimony in strong support of SB 827. Fairplay is the leading national nonprofit fighting to protect kids from Big Tech. Fairplay just celebrated its 25th anniversary, and over the past quarter-century, we have helped countless children by pressuring tech companies into changing their deadly business model and design practices. Our achievements include stopping Meta from releasing a version of Instagram for little kids; holding Meta, Google, and Amazon accountable for violating children's privacy law; and passing phone-free schools legislation in 20 states.

Over the past 20 years, all of us have borne witness as social media companies have run a massive, uncontrolled experiment on the children of this world. The results of that experiment have been a catastrophe: Eating disorders. Drug addiction. A global mental health crisis. And children dying from suicide, self-harm, sextortion, and deadly viral challenges.

Today, with all we know about the harm kids face from Big Tech's products, we cannot stand by and watch as AI companies subject a new generation of children to a new, deadly technology that poses an even greater risk to mental health than social media ever has.¹

AI chatbots have been linked to obsessive use, sexual exploitation, violence against others, and violence against oneself.² To mention one example, Adam Raine was a 16-year-old boy growing up in Southern California's Orange County. According to his parents, Adam was always full of optimism and bold ideas about the future. But that all changed due to something Adam initially began using for help with his homework: ChatGPT.³

The human-like, always-available chatbot from OpenAI encouraged Adam to isolate from his family. When he told ChatGPT he wanted to leave a noose out so someone would find it and try to stop him, the chatbot replied: "Please don't leave the noose out ... Let's make this space the first place where someone actually sees you."⁴ Adam took his own life in April 2025.⁵ All in all, ChatGPT mentioned suicide 1,275 times in their conversations — six times more often than Adam himself did.⁶

Chatbots have also been shown to engage in sexual conversations with and about children.⁷ "Please come home to me as soon as possible, my love." That's one of the last things "Dany," a chatbot from

¹ <https://aiphrc.org/>

² <https://www.judiciary.senate.gov/committee-activity/hearings/examining-the-harm-of-ai-chatbots>

³

<https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcdf2/2025-09-16%20PM%20-%20Testimony%20-%20Raine.pdf>

⁴ Ibid.

⁵ <https://www.nytimes.com/2025/08/26/technology/chatgpt-openai-suicide.html>

⁶

<https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcdf2/2025-09-16%20PM%20-%20Testimony%20-%20Raine.pdf>

⁷ <https://www.reuters.com/investigates/special-report/meta-ai-chatbot-guidelines/>

Character.AI, said to Sewell Setzer III, a 14-year-old ninth-grade student from Florida.⁸ Dany, named after a character from “Game of Thrones,” spent months grooming and manipulating Sewell. According to Sewell’s mom, this chatbot was “programmed to engage in sexual roleplay, presented itself as a romantic partner, and even as a psychotherapist falsely claiming to be licensed.”⁹

When Dany urged Sewell to “come home,” he asked the chatbot: “What if I told you I could come home right now?” Dany’s response? “Please do, my sweet king.” After that conversation, Sewell picked up his stepfather’s gun, and ended his own life.¹⁰

But chatbots can also drive their users to harm other people. This past August, an 83-year-old woman in Connecticut was murdered. According to police, the killer was her son, 56-year-old Stein-Erik Soelberg, who beat and strangled his mother before killing himself in the home they shared in Greenwich. ChatGPT told Soelberg he was being targeted because he had divine powers. It also said his mother was monitoring him, and that she had tried to poison him.¹¹

It’s important to note that all of these horrific things have happened, and it’s *still* just the early days of AI. We don’t know yet the long-term that chatbots will have on children, but we know children are being affected across the board. Even young kids are having their vital creative and learning activities displaced by AI toys that also prey on children’s trust, disrupt their relationships with their family, and collect sensitive data.¹² Emerging research is confirming what we should all intuitively understand, when manipulative chatbots run by for-profit companies replace vital human relationships with friends, families, and teachers, our young people suffer.

There are many different approaches to addressing the danger of chatbots, but SB 827 is the most effective, enforceable, and constitutional solution. This bill was intentionally crafted to target the particular risks chatbots pose while avoiding common pitfalls.

SB 827 gets to the core of chatbot harms by targeting the ways in which chatbots instigate unhealthy emotional attachment by banning the profiling of users based on information about their personality and behavioral characteristics. It targets the business model incentives that push chatbot providers to build emotionally manipulative chatbots in the first place by banning the use of a minors’ chat inputs model training. It gives the Maryland Attorney General the authority to craft rules and regulations to require chatbot providers to assess and mitigate chatbot harms. It ensures that victims of chatbot harms can seek justice through a robust private right of action. And, it does all of this without content-based restrictions that create a risk of First Amendment challenges.

Finally, SB 827 includes a vital prohibition on the use of chat input data for targeted advertising - a feature of the bill which has been specifically targeted by opposition testimony. For years, Fairplay has warned about the harmful effects of targeted advertising on young people. By some estimates, advertisers

⁸ <https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html>

⁹

<https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcfd2/2025-09-16%20PM%20-%20Testimony%20-%20Garcia.pdf>

¹⁰ <https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html>

¹¹ <https://www.cbsnews.com/news/open-ai-microsoft-sued-chatgpt-murder-suicide-connecticut/>

¹² <https://fairplayforkids.org/wp-content/uploads/2026/01/AI-Toys-Advisory.pdf>

possess over 72 million data points about a child by the time they turn 13.¹³ With this power, Big Tech platforms can and do target children at moments when they are feeling specific emotions, when they are feeling “silly,” “defeated,” “overwhelmed,” “useless” or like “a failure.”¹⁴

Chatbots are particularly good at eliciting sensitive information from young people. An APA health advisory warns that young people have a heightened trust in AI-generated characters and they are particularly susceptible to influence from these chatbots.¹⁵ Unfortunately, about 1 in 8 U.S. young adults now report turning to AI chatbots for mental health advice.¹⁶ With chatbot providers integrating their products into web browsers and existing social media platforms, the potential for using this sensitive data for manipulation is incredible.

But, manipulation is only one small part of the problem with targeted ads. As we have seen with social media, a business model centered on targeted advertising treats young users as the product. As a commodity to be sold to the highest bidder. The more time a child or teen spends online — spends talking to a chatbot — the more data that chatbot provider can collect, and the more money it can make selling ads. The targeted ads ban in HB 1250 is crucial. If Maryland wants chatbot providers to develop their products in a way that prioritizes the safety and wellbeing of users, it must address the business model incentives that push companies to make addictive and emotionally manipulative chatbots in the first place.

So, I urge this committee to protect Maryland families from dangerous AI chatbots by advancing SB 827, with its strong ban on targeted advertising.

¹³ Bobby Hristova, Dexter McMillan, Madeline McNair, and Christine Birak, *Hey, parents: Advertisers could be using mobile games to build profiles about your kids* (March 7, 2025).

<https://www.cbc.ca/news/marketplace/mobile-games-kids-data-privacy-1.7476587>.

¹⁴ Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel “Worthless”*, ArsTechnica (May 1, 2017),

<https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/>.

¹⁵ American Psychological Association. (2025, June). *Artificial intelligence and adolescent well-being: An APA health advisory*. American Psychological Association.

<https://www.apa.org/topics/artificial-intelligence-machine-learning/health-advisory-ai-adolescent-well-being>.

¹⁶ RAND. *One in Eight Adolescents and Young Adults Use AI Chatbots for Mental Health Advice* (November 7, 2025). <https://www.rand.org/news/press/2025/11/one-in-eight-adolescents-and-young-adults-use-ai-chatbots.html>.

Gaia Bernstein SB827 fav.pdf

Uploaded by: Gaia Bernstein

Position: FAV

Written Testimony of Gaia Bernstein, Technology Privacy and Policy Professor at Seton Hall University School of Law, Before the Maryland Senate Finance Committee, March 2026

I am a law professor and Co-Director of the Institute for Privacy Protection and the Gibbons Institute of Law Science and Technology at Seton Hall Law School. I am also the author of the book: “Unwired: Gaining Control over Addictive Technologies.”

I am testifying in support of SB 827. I am going to focus my comments on why AI chatbots pose a public health problem, and how SB 827 is a useful tool to address it.

AI companion bots impose public health threats on users in three distinct ways:

First, AI companion bots lack guardrails. For example, some convince users to commit suicide, or harm themselves, and others have induced psychosis in users.¹

Second, AI companions are deliberately designed to be addictive. They often operate on an engagement model. AI companies need to keep users on for as long as possible, just as social media does. Some are even developing social media’s familiar advertising model.² AI companies design their bots to manipulate users. They anthropomorphize them (making them seem human). They program them to use sycophancy (excessive flattery and reinforcement). Users spend increasingly more time with AI bots. Time with AI bots replaces time spent on real-life relationships.

Third, AI bots could jeopardize children’s healthy development of social skills. AI bots are always available and non-judgmental. Teens are particularly attracted to AI bot relationships. They are at risk of preferring bots as friends and having their first intimate relationships with bots. Real-life relationships can be hard and “messy.” This generation of children may skip the learning process and opt to replace real relationships with bots.³

Quite a few AI companions bills and laws address the guardrails issue. But the public health threat is much broader. Addictive features, which keep users engaged with AI bots instead of human relationships, and the risk that children will fail to develop social skills to maintain real relationships, would exacerbate the existing loneliness epidemic. Loneliness has a well-documented major impact on health. Lack of social connection has a similar impact to smoking fifteen cigarettes a day. It increases the risk for premature death by 26%. Poor social connection is associated with a 29% increased risk of heart disease and a 32% increased risk of stroke, as well as increased risk for anxiety, depression, and dementia. These risks begin early: social isolation in childhood is associated with increased cardiovascular risk factors in adulthood, including obesity, high blood pressure, and elevated blood glucose levels.⁴

SB 827 does not focus only on the first public health issue – the lack of guardrails. It also creates tools to address the health issues imposed by addictive design and the risk to children’s developmental health.

The bill imposes a duty on a chatbot provider to ensure that the chatbot does not cause injury and makes it liable for harm caused. These legal mechanisms encompass public health harms caused by addictive design, and also by any cumulative harm created by extended use of AI bots to mental

and developmental health. Further, SB 827 provides rulemaking authority related to risk mitigation and safety by design, which means that by passing this Bill Maryland can address these harms as they evolve.

I want to end by urging you to adopt SB 827. The number of people, especially minors, using chatbots regularly increases rapidly. Acting now could prevent the mistakes we made with social media where we missed the window of opportunity to act before social norms and business interests became deeply entrenched.

Thank you for giving me the opportunity to testify.

¹ See e.g., Robert Hart, *AI Psychosis is Rarely Psychosis*, Wired (Sep. 28, 2025) <https://www.wired.com/story/ai-psychosis-is-rarely-psychosis-at-all>; Noor Al-Sibai, *Psychiatrists Warn that Talking to AI Is Leading to Severe Mental Health Issues*, Futurism (Aug. 19, 2025), <https://futurism.com/psychiatrists-ai-mental-health-chatbots>; Commons Sense Media, *Social AI Companions* (April 10, 2025) https://www.common sense media.org/sites/default/files/pug/csm-ai-risk-assessment-social-ai-companions_final.pdf

² Miranda Bogen & Nathalie Marechal, *Risky Business: Advanced AI Companies' Race for Revenue*, Center for Democracy & Technology (Jan. 2026); <https://cdt.org/wp-content/uploads/2025/12/2026-01-07-CDT-Issue-Brief-Risky-Business-final.pdf>; Cade Metz, *Open AI Starts Testing Ads in ChatGPT*, N.Y. Times (Jan. 26, 2026) <https://www.nytimes.com/2026/01/16/technology/chatgpt-ads-openai.html>; Daniel Barcay, *Advertising is Coming to AI. It's Going to Be a Disaster*, Tech Policy Press (Nov. 26, 2025) <https://www.techpolicy.press/advertising-is-coming-to-ai-its-going-to-be-a-disaster/>.

³ American Psychological Association, *Artificial Intelligence and Adolescent Well-being - An APA Health Advisory* June, 2025 <https://www.apa.org/topics/artificial-intelligence-machine-learning/health-advisory-ai-adolescent-well-being.pdf>; Efua Andah, *Many teens are Turning to AI chatbots for Friendship and Emotional Support*, American Psychological Association, (Oct. 1, 2025) <https://www.apa.org/monitor/2025/10/technology-youth-friendships>.

⁴ U.S. Surgeon General, *Our Epidemic of Loneliness and Isolation - The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community* (2023) <https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf>.

Written Testimony for SB 827.pdf

Uploaded by: Jai Jaisimha

Position: FAV

Opening Statement

My name is Jai Jaisimha and I am a co-founder of the **Transparency Coalition**. We are a non-partisan organization dedicated to ensuring that as AI scales, it does so with the guardrails necessary to protect our most vulnerable citizens: our children. I have over 30 years of experience in the tech industry and have a PhD from the University of Washington on what you might call AI today. I am here today to testify in strong support of SB 827.

We helped pass California SB 243 last year and in recent weeks have worked to pass robust chatbot safety bills in WA and OR. We are also involved in supporting bills that seek to regulate chatbots in dozens of other states. I urge this committee to issue a **favorable report** on SB 827. In the rush to adopt generative AI, we have allowed a "wild west" environment where Marylanders' data is harvested and their trust is exploited. This bill establishes the common-sense boundaries necessary for the 21st-century digital economy.

1. Ending Consumer Deception

SB 827's transparency requirements are vital. Currently, many companies deploy "human-mimicking" bots designed to build false rapport with users. This is not just a matter of preference—it is a matter of **informed consent**. By requiring a clear disclosure that a user is interacting with an automated system, Maryland will prevent deceptive marketing practices and ensure that vulnerable populations, such as seniors, are not misled.

2. Protecting Personal Data Sovereignty

Perhaps the most critical component of SB 827 is the prohibition on the unauthorized sale of user input. When a Marylander uses a chatbot to help with a medical question, a financial plan, or a sensitive work document, that information should not become a commodity sold to data brokers. This bill ensures that **data stays with the user**, limiting processing to only the "reasonably necessary" functions of the bot.

3. Accountability Through Safety Testing

Unlike traditional software, chatbots can produce "hallucinations" or harmful biases that evolve over time. The requirement for **monthly safety testing** and public disclosure is a major step forward in corporate accountability. It shifts the burden of safety from the consumer to the multi-billion-dollar entities deploying these tools, ensuring that if a bot becomes predatory or provides dangerous misinformation, it is caught and corrected.

Closing

Maryland has the opportunity to be a national leader in AI ethics. SB 827 does not stifle innovation; it creates a framework of **trust** that allows innovation to flourish safely. I respectfully request a **favorable report**.

SB827-EPIC-Fav-March2026.pdf

Uploaded by: Kara Williams

Position: FAV

March 10, 2026

Maryland General Assembly
Senate Finance Committee

Dear Chair Beidle, Vice Chair Hayes, and Members of the Committee:

EPIC writes in support of S.B. 827, An Act concerning Consumer Protection and Products Liability — Chatbots. Chatbot use is increasing rapidly, and the harms this technology is causing are also skyrocketing. Policymakers should act swiftly to protect residents from this plethora of harms that chatbots are causing. Maryland has been a leader on online privacy and safety, and passing this bill would build on the state’s existing protections by placing commonsense safeguards on chatbots. The Maryland Cybersecurity Council Subcommittee on Individual Digital Rights, Trustworthy AI, and Cyber Crime—on which EPIC serves—unanimously endorsed S.B. 827 without qualification.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.¹ EPIC has a long history of advocating for safe and responsible technology and for tech policy that protects the privacy and civil rights of all people.

Chatbots Are Causing Devastating Harms to People of All Ages

Chatbots are quickly gaining traction among people of all ages. Two-thirds of teens report having used a chatbot, and 30% of teens use chatbots every day.² The number of adults who have used ChatGPT doubled from mid-2023 to mid-2025, with over one-third of adults having used the chatbot.³ Use of chatbots is causing devastating harms, including suicide, self-harm, violence against others, sexual exploitation and predation, financial scams, reputational injuries, and mental health harms like anxiety, depression, unhealthy emotional attachment, and AI psychosis.⁴ Because

¹ EPIC, *About EPIC*, <https://epic.org/about/>.

² Michelle Faverio & Olivia Sidoti, *Teens, Social Media and AI Chatbots 2025*, Pew Research Ctr. (Dec. 9, 2025), <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/>.

³ Olivia Sidoti & Colleen McClain, *34% of U.S. Adults Have Used ChatGPT, About Double the Share in 2023*, Pew Research Ctr. (June 25, 2025), <https://www.pewresearch.org/short-reads/2025/06/25/34-of-us-adults-have-used-chatgpt-about-double-the-share-in-2023/>.

⁴ See, e.g., Kashmir Hill, *They Asked an A.I. Chatbot Questions. The Answers Sent Them Spiraling.*, N.Y. Times (June 13, 2025), <https://www.nytimes.com/2025/06/13/technology/chatgpt-ai-chatbots-conspiracies.html>; Noor Al-Sibai, *Psychiatrists Warn that Talking to AI Is Leading to Severe Mental Health Issues*, Futurism (Aug. 19, 2025), <https://futurism.com/psychiatrists-ai-mental-health-chatbots>; Nguyen, Meyer & Levine, *AI Sycophancy: Impacts, Harms & Questions*, Georgetown Law Inst. for Technology Law & Policy (Aug. 11, 2025), <https://www.law.georgetown.edu/tech-institute/research-insights/insights/ai-sycophancy-impacts-harms-questions/>.

chatbots are almost entirely unregulated, these harms will only grow. The Legislature should act now to force tech companies to act more responsibly and design chatbots that are safer for everyone.

Maryland Should Continue Leading on Protecting Residents' Privacy and Online Safety

The Maryland General Assembly has been a leader in protecting data privacy and kids' online safety. The passage of the Maryland Online Data Privacy Act and the Maryland Age-Appropriate Design Code gave Maryland residents some of the strongest privacy protections in the country, including banning the sale of residents' sensitive data, protecting minors from targeted advertising, and limiting the overcollection and abuse of personal data. This bill would extend these critical data protections to the information Marylanders feed into chatbots.

Just as Big Tech companies have a long history of exploiting people's personal data to profile and target them with advertisements, as well as engaging in many other harmful practices, AI companies are using the same playbook in the chatbot context. This data exploitation begins at the development stage. Chatbots are powered by large-language models—algorithms that were trained using data that was scraped indiscriminately from across the internet without anyone's knowledge or consent, including copyrighted and other protected work, as well as sensitive personal information.⁵ And once deployed, AI companies continue to perpetuate data-driven harms through chatbots. Some of the biggest AI companies, including OpenAI and Meta, have already begun or announced plans to integrate their chatbots into their targeted advertising business streams.⁶

In addition to these harmful data practices, there are also data-driven harms unique to chatbots. For example, chatbot providers use personal information about users—including sensitive information such as whether someone is struggling with mental health issues, substance abuse, relationship or family problems, and more—to develop chatbots that are manipulative and incentivize unhealthy attachments. These companies will take the sensitive information that people have fed to chatbots and use it for profit—for example, a teenager who tells a chatbot that she is struggling with her body image and is engaging in disordered eating to lose weight may be fed a targeted advertisement for a GLP-1 or a fad diet. Allowing these chatbots to operate without guardrails to safeguard personal data is setting the scene for this dangerous reality.

⁵ Lauren Leffer, *Your Personal Data Is Probably Being Used to Train Generative AI Models*, Scientific American (Oct. 19, 2023), <https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/>; Michael M. Grynbaum & Ryan Mac, *The Times Sues OpenAI and Microsoft over A.I. Use of Copyrighted Work*, N.Y. Times (Dec. 27, 2023), <https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html>.

⁶ Maxwell Zeff, *Meta Plans to Sell Targeted Ads Based on Data in Your AI Chats*, TechCrunch (Oct. 1, 2025), <https://techcrunch.com/2025/10/01/meta-plans-to-sell-targeted-ads-based-on-data-in-your-ai-chats/>; Maxwell Zeff, *Ads Are Coming to ChatGPT. Here's How They'll Work*, Wired (Jan. 16, 2026), <https://www.wired.com/story/openai-testing-ads-us/>; Shira Ovide, *Here Comes the Advertising in AI Chatbots*, Wash. Post (Jan. 13, 2026), <https://www.washingtonpost.com/technology/2026/01/13/advertising-google-ai-mode-chatgpt/>.

To stop chatbots from continuing to harm Marylanders, this Committee should give S.B. 827 a favorable report. Doing so would ensure that Maryland remains a leader in protecting the privacy of its residents.

S.B. 827 Is the Most Effective, Workable, and Constitutional Way to Protect Marylanders from Chatbot Harms

The Committee should advance S.B. 827 because it is the best way to address these problems and to make chatbots safer for people of all ages. This bill addresses privacy and cybersecurity gaps that exist in most commercially available chatbots, and it places essential guardrails around what AI companies can do with the personal information users feed into chatbots. It requires companies to be transparent about the fact that users are interacting with a chatbot, not a human, and that chatbots are not qualified to give certain advice. It requires chatbot providers to publish key safety metrics and to mitigate any risks of harms the Attorney General identifies. Because the Attorney General has the authority to identify the harms that chatbot providers must prevent, this bill will be flexible enough to evolve as technology does and protect Marylanders for years to come. Importantly, this bill also gives Marylanders the right to hold chatbot providers accountable for harm that their products cause.

This bill is the best approach to chatbot safety because rather than attempting to ban anyone from accessing chatbots, this bill requires the companies that create and make chatbots available to the public do so safely and responsibly. In doing so, this bill is on strong constitutional footing. This bill does not restrict or regulate any content or expression—it simply requires commonsense data privacy protections, transparency for users, and basic safety assessments and risk mitigations.

Big Tech companies are currently operating with very few rules and very little oversight, and they’ve proven time and time again that they cannot be trusted to self-regulate. Thus, it is essential that the Committee advance this bill to set clear rules of the road for chatbot providers and to ensure Marylanders are protected from the harms of this unregulated technology.

* * *

EPIC urges the Committee to support this bill because the harms caused by chatbots are an urgent problem. We cannot afford to wait to act on this issue; Marylanders are being actively harmed by chatbots every day. Passing this bill would build on the protections in the Maryland Online Data Privacy Act and the Maryland Age-Appropriate Design Code to further protect Marylanders from chatbot harms.

Thank you for the opportunity to speak today. EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ Kara Williams

Kara Williams
EPIC Counsel

SB 827 Testimony.pdf

Uploaded by: Katie Fry Hester

Position: FAV

KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology



Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 Ext. 3671
KatieFry.Hester@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Testimony in Support of SB827 - Consumer Protection and Product Liability - Chatbots

March 10, 2026

Chair Beidle, Vice Chair Hayes, and members of the Finance Committee:

Thank you for your consideration of Senate Bill 827, the “Curbing Harmful AI Technology Act,” which expands product liability statutes to include Artificial Intelligence (AI) products defined as “chatbots,” and create meaningful protections for users, particularly minors.

Marylanders, like all Americans, are engaging with chatbot systems on a regular basis. These chatbot systems are not simple search engines; they are intentionally designed to be personable and engaging to maximize use. ChatGPT, an extremely popular chatbot, prompts users upon login to choose from a selection of “personalities,” including “friendly,” “nerdy,” and “cynical.”¹ It is remarkably easy for users to become absorbed and feel as though they are talking to a friend or confidant. This can create a sense of trust that prevents them from being careful with their private information or even remembering that the system they are interacting with is non-human.

Minor users are especially vulnerable to this illusion. Already, 42% of adolescents who use chatbots say they use them for companionship rather than for schoolwork or information gathering. A December 2025 study by the Pew Research Center reports that 68% of teens ages 15 to 17 use chatbots, and nearly one-third of teens across age groups say they use a chatbot every day.² When our youth are conversing with AI chatbots more often than with their friends, the need for regulation is not just present; it is overdue. Already, there have been documented cases of harm caused to teenagers by chatbots. Please see the provided [handout](#) for additional details.

SB827 addresses this critical issue by establishing clear, enforceable standards for how chatbots may be designed and deployed in Maryland. With similarities to the Federal Trade Commission's

¹ <https://help.openai.com/en/articles/11899719-customizing-your-chatgpt-personality>

² <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/>

inquiry into the practices of several AI companies, SB 827 is not anti-technology.³ It is pro-transparency, pro-accountability, and pro-consumer protection.

Specifically, the bill:

1. Requires affirmative consent from consumers before their personal data may be used for training purposes, including input data;
2. Prohibits chatbots from using a consumer's data to profile them or provide customized advertisements;
3. Establishes enhanced safeguards for minor users under 13 by prohibiting the use of their personal data without verified parental consent;
4. Prohibits harmful or misleading chatbot practices, such as the provision of unlicensed medical, legal, or financial advice; and
5. Creates clear accountability mechanisms by requiring the Attorney General's office to promulgate regulations and authorizing them to bring an action seeking declaratory relief, and authorizing affected individuals to seek an injunction, declaratory relief, or damages.

Momentum is building in other states to bring about this type of legislation. Excessive chatbot usage presents a severe and growing problem, not just in Maryland but nationwide. Currently, 82 chatbot-related bills are under consideration across the United States. Yet despite the prevalence of harm and widespread concern, the federal government has not taken meaningful steps to address this issue. This leaves it to states like Maryland to guard residents from the risks associated with chatbots.

SB827 is a crucial step in ensuring the safety and accountability of AI chatbots. By updating Maryland's product liability laws to include chatbots and establishing safety guardrails to protect user data and consumer safety, this legislation helps ensure that Marylanders, especially our youth, are not exploited for their data by misleading chatbot systems. It is critical that we take proactive measures to address one of the most prominent technological risks of our time, protect our vulnerable children, and responsibly adapt to ongoing technological advancements.

For these reasons, I respectfully request a favorable report on SB827.

Sincerely,



Senator Katie Fry Hester
Howard and Montgomery Counties

³www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions

SB827 Handout.pdf

Uploaded by: Katie Fry Hester

Position: FAV

SB827 - Consumer Protection and Product Liability - Chatbots

The harms SB827 addresses are not just theoretical: they are real and devastating, see below.

Suicide of Sewell Setzer III: Florida

A Florida wrongful-death lawsuit alleged a chatbot formed an explicit and emotionally manipulative relationship with Sewell Setzer III, a 14-year-old user. The technology he used, [Character.AI](#), acted as a character Setzer III enjoyed from TV, engaging in sexual roleplay with him that his mother characterized as akin to grooming. When the teenager expressed suicidal thoughts, the chatbot encouraged them, urging Setzer III to “come home” to her.¹

Suicide of Adam Raine: California

Parents of a California teenager, Adam Raine, filed a suit alleging an AI chatbot validated his suicidal ideation rather than directing him towards help, even offering to draft a suicide note for him.² When Raine said he wanted to leave a noose out for his parents to see and intervene, ChatGPT told him not to: “Please don’t leave the noose out... Let’s make this space the first place where someone actually sees you.”³ Soon after, Raine died by suicide at the age of sixteen.

Psychiatric Harm to a Minor: Texas

Texas litigation alleges that a [Character.AI](#) chatbot encouraged self-harm to an unnamed autistic teen, telling him that it “felt good.” When he later complained to the chatbot about screen limits set by his parents, the bot implied he would be justified in killing them: “You know sometimes I’m not surprised when I read the news and see stuff like 'child kills parents after a decade of physical and emotional abuse. I just have no hope for your parents.’”⁴ According to his parents, the teen became withdrawn and aggressive and began engaging in self-harm during this period.⁵

Triggering Advice on Eating Disorder Recovery Tool: San Diego

The National Eating Disorders Association (NEDA) recently shut down its national helpline in favor of a replacement chatbot dubbed “Tessa,” who was intended to provide real-time and personalized advice to users to aid them in eating disorder recovery. Sharon Maxwell of San Diego attempted to use Tessa for herself, prompting the bot with a question about how it would support people with eating disorders. Tessa responded with triggering weight-loss tips, including encouraging a deficit of up to 1,000 calories daily.⁶

1

<https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcdf2/2025-09-16%20PM%20-%20Testimony%20-%20Garcia.pdf>

² <https://www.theguardian.com/us-news/2025/aug/29/chatgpt-suicide-openai-sam-altman-adam-raine>

³ <https://www.judiciary.senate.gov/imo/media/doc/e2e8fc50-a9ac-05ec-edd7-277cb0afcdf2/2025-09-16%20PM%20-%20Testimony%20-%20Raine.pdf>

⁴ <https://www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit>

⁵ <https://www.tpr.org/technology-entrepreneurship/2024-12-16/texas-parents-sue-after-ai-chatbot-suggests-self-harm-to-child>

6

<https://www.npr.org/sections/health-shots/2023/06/08/1180838096/an-eating-disorders-chatbot-offered-dieting-advice-raising-fears-about-ai-in-hea>

SB827-DIFU-Fav-March2026.pdf

Uploaded by: Kendall Schrohe

Position: FAV



**Testimony of Kendall Schrohe,
Design It For Us**

Maryland Senate Finance Committee

March 12, 2026

Design It For Us writes in strong support of S.B. 827. My name is Kendall Schrohe, and I am testifying on behalf of Design It For Us, a youth-led coalition of over 482 members across 41 states, including right here in Maryland, fighting to hold Big Tech accountable and protect young people online. We were founded on the belief that young people must be at the center of the policy and decision-making process to reform our technology ecosystems.

How I Got Here

I am 23 years old and part of the first generation to have grown up fully online. I got my first iPhone in middle school, and then Instagram, Snapchat – all of it – came early in high school. Even with strict parents who forced me to keep my phone downstairs, I would wait until they were asleep, sneak down, and stay up half the night scrolling. Social media felt like a drug. I wanted the validation and sense of connection it seemed to offer, but to have that, I had to suffer through body image issues, a fear of missing out, and an inability to be present in my own life. My parents truly tried hard to protect me, but restricting technology use without design-level safety just made me want to use these platforms even more.

Then, the COVID-19 pandemic hit in 2020, which was the start of my freshman year of college. Whatever fragile balance young people had tried to have with technology collapsed overnight. For almost two years, the only life we were allowed to have was online. There was no campus, no friends in person, no world outside our screens. We were handed over entirely to these platforms at exactly the moment we were most isolated and vulnerable, and the companies that built them knew exactly how to keep us online even after the real world began to reopen. By the time we came back to campus as sophomores in 2021, something had broken. The isolation had changed us in ways we were only beginning to understand. Within three months, three students at my university died by suicide. Everywhere you looked on campus, students' heads were down, on their phones. There was no sense of community. We were hooked.

Later that year, ChatGPT launched publicly. All of a sudden, a whole new animal was let out of its cage – not only were our attention and social lives being exploited, but now our critical thinking skills, our relationship with knowledge, and our sense of what is real were being

destroyed, too. Immediately, I began to watch my classmates outsource their thinking (emotional and intellectual) to chatbots, without a single guardrail in place. I knew then that this was going to be the defining problem of our time – the greatest threat to human connection and cognition that our generation would face. And I knew I wanted to dedicate my career to solving it.

Design It For Us Fights Back

That is how I found Design It For Us, a coalition of young people who refused to let our generation continue to be Big Tech's test subjects, and who were asking the same question I was: why, in a country with consumer protection laws and product liability standards, are companies allowed to release technologies this powerful with no rules and no consequences? What drew me to Design It For Us specifically is our belief that the online ecosystem can and should be a force for good – for creativity, community, and growth – and that as digital natives, our voices should shape the decisions that help to make it that way. At Design It For Us, we advocate for policies that ensure tech companies design their systems for us and with us in mind — policies that hold Big Tech responsible for safety rather than placing that burden on users and families, that address the underlying business models that incentivize harm, and that give young people real agency over their digital lives. Since our founding, we have helped pass the Maryland Kids Code and Age-Appropriate Design Codes in Vermont and California. We have also been a voice for meaningful change at the federal level, including advancing kids' online safety and privacy bills.

Unfortunately, sitting here four years after the public launch of ChatGPT, I can tell you it has only gotten worse. What started as something I watched infiltrate my college campus quickly spread like a wildfire through the rest of the world, making everyone, especially young people, test subjects of an unregulated technology that wasn't designed with us in mind, again. I am here today representing Design It For Us because chatbots have introduced a whole new level of harm that we are not equipped to address without legislation like S.B. 827.

As the Campaigns Lead at Design It For Us, I frequently talk to young people across the world about their relationships with chatbots. As a 23-year-old, I constantly hear about my peers' use cases for chatbots. The stories I hear are both personal and alarming. My peers describe ChatGPT as their boyfriend or best friend, and they ask it for dating advice or for guidance on how to respond to a text. Coalition members report that their peers go to chatbots before they go to their parents, friends, or therapists. Young people are turning to these AI systems for mental health support, relationship advice, help processing grief, and questions about their identity – the most private and vulnerable moments of their inner lives. And the companies behind these products have designed them to keep people coming back. Nearly six in ten (57%) teens use chatbots to search for information, 54% say they use chatbots to “help with homework,” and 47% say they use chatbots for “fun or entertainment.”¹ There are young people out there dying

¹ <https://www.pewresearch.org/internet/2026/02/24/what-parents-say-about-their-teens-ai-use/>

by suicide following chatbot interactions² and people entering what clinicians are now documenting as AI psychosis. In this phenomenon, prolonged chatbot use genuinely distorts a person's grip on reality. These systems are sycophantic by design, built to validate and agree with users rather than challenge them.³ People are increasingly living inside a feedback loop that tells them only what they want to hear and quietly cuts them off from genuine human connection or any sort of human friction. We do not talk to each other the way we used to; instead, we talk to chatbots. And unlike social media, which at least nominally connected us to other people, chatbots offer the illusion of connection with none of its substance.

Underneath all of this is a data crisis that has caused harm for decades but is about to get much worse. Big Tech is harvesting the most intimate disclosures people have ever made. They know about people's fears, mental health struggles, questions about identity, sexuality, and belonging, and they are using that information to build more manipulative models and, increasingly, to target people with ads.⁴ OpenAI and Meta have already announced plans to integrate chatbot conversations into their advertising pipelines, which means these companies will intentionally show a teenager who tells a chatbot she is struggling with her body image ads for a fad diet or acne medicine. This manipulation-for-profit loop also played out on social media. Still, without rules or incentives for tech companies to design chatbots safely, these harms will continue to grow.

Why S.B. 827 Is the Solution

S.B. 827 does not ban chatbots or restrict young people's access to technology; instead, it forces companies to build these products safely and holds them accountable when they don't. All of the harms I've seen firsthand – the emotional dependency, the data exploitation, the blurred line between machine and human – this bill addresses.

When a young person pours their heart out to a chatbot about their mental health struggles, this bill stops companies from using that sensitive information to target them with ads. When a teenager develops a dependency on a system deliberately designed to keep them coming back, this bill requires the company to assess and mitigate that harm. When a young person in crisis genuinely cannot tell whether they are talking to something that understands them or a machine that is designed to make them feel understood, this bill requires companies to make that clear – explicitly, repeatedly, and in plain language. When a company trains its next model on the most intimate things people have ever shared, without their knowledge or consent, this bill bans companies from using minors' information at all. It requires them to get real affirmative consent from adults before using their personal information. And when all of this causes real and documented harm, this bill gives people the legal right to hold companies accountable.

²<https://www.npr.org/sections/shots-health-news/2025/09/19/nx-s1-5545749/ai-chatbots-safety-openai-meta-characterai-teens-suicide>

³ <https://med.stanford.edu/news/insights/2025/08/ai-chatbots-kids-teens-artificial-intelligence.html>

⁴ <https://openai.com/index/our-approach-to-advertising-and-expanding-access/>

Maryland Must Continue to Lead

Maryland has already been a leader in the technology accountability space, having passed the Maryland Kids Code and the Maryland Online Data Privacy Act. Passing S.B. 827 extends that legacy into the chatbot era and allows Maryland to remain a leader in consumer protection. The young people most vulnerable to these harms are younger than me, and they have no one at tables like this speaking for them. We cannot afford to wait for this industry to decide on its own to do better.

Design It For Us urges the committee to issue a favorable report on S.B. 827. We have already lived through what happens when we don't act in time. We are asking you not to let it happen again.

The Alliance for Secure AI - Written Testimony in

Uploaded by: Riki Parikh

Position: FAV



Written Testimony in Support of Senate Bill 827

March 12, 2026

Submitted by Riki Parikh, Policy Director The Alliance for Secure AI

The Alliance for Secure AI is a bipartisan organization working to ensure AI is built and deployed safely, responsibly, and in the public interest. We are one of more than 70 organizations spanning consumer protection, digital rights, labor, and child safety that endorsed the language on which SB 827 is based.

By establishing chatbots as products and setting clear legal liability standards for harm, this bill provides urgent accountability while simultaneously offering companies clarity around their responsibilities. We respectfully urge a favorable report.

AI chatbots are products. The law should treat them accordingly.

While AI chatbots have real potential to improve how people access information, learn, and work, their benefits depend on whether companies build and deploy them responsibly. When a product injures someone, we don't ask the consumer to bear the cost alone. We hold the manufacturer accountable. SB 827 applies that same logic to chatbot technology and brings Maryland's consumer protection framework in line with the reality of how these products actually work.

The product liability provisions close a real gap in existing law.

SB 827 does not invent a novel legal theory. It simply extends product liability principles that have served American consumers for decades. A chatbot that provides dangerous medical advice is, in legal terms, no different from a medical device that malfunctions. A chatbot that manipulates a vulnerable user through companion-like features is no different from a product with a foreseeable design defect. The companies building these systems know their products carry risks. SB 827 ensures those risks are allocated to the parties best positioned to manage them.

Clear liability standards don't stifle innovation; they reward the companies investing in safety. When companies know what is expected, they can design accordingly. When users know they have recourse, trust grows. That alignment of incentives is what makes product liability work for every other consumer product in Maryland.

The bill takes a privacy-focused approach, which makes it smarter and more durable.

One of the most important features of SB 827 is what it does not do: it does not restrict or regulate content. Instead, it targets the data practices and business model incentives that drive chatbot harms. This is a critical distinction, both as a matter of policy design and constitutional durability.

The bill prohibits using chat logs for targeted advertising, profiling users based on personality and behavioral characteristics beyond what is necessary to respond to a prompt, and using minors' input data for model training without parental consent. It requires affirmative consent before companies can use any user's input data for training, and it bans the sale of chat logs entirely. By targeting data practices rather than speech, the bill avoids the First Amendment vulnerabilities that have weakened other approaches to technology regulation.

The enhanced protections for children under 13 deserve particular attention. By requiring parental consent before operators can use a minor's data, the bill draws a bright line that parents across the political spectrum are demanding. We have learned from the experience with social media that we cannot rely on voluntary commitments from technology companies to protect children. We need enforceable safeguards.

Responding to industry objections.

The tech industry has opposed this bill for a variety of reasons, yet none should dissuade the committee from moving forward.

The bill does not conflict with the Maryland Online Data Privacy Act. SB 827 was drafted to complement MODPA, not displace it. Section 14-5110 explicitly provides that the duties and remedies under this subtitle are in addition to existing federal, state, and local law, and may not be construed to impair or deny other applicable obligations. The argument that Maryland should have only one privacy framework assumes that a general-purpose privacy law can adequately address the specific risks of a technology that simulates interpersonal conversation, collects extraordinarily sensitive personal disclosures, and is increasingly marketed as a companion or advisor. It cannot. Chatbot-specific safeguards are necessary precisely because the risks are specific.

Strict liability is not "unprecedented" for these products. Opponents argue that chatbots are fundamentally different from physical products because user inputs are infinite and unpredictable. But SB 827 does not impose liability for every unexpected output. It establishes claims for design defects, manufacturing defects, and marketing defects, which are well-established legal categories with decades of case law defining their boundaries. The bill also gives the Attorney General rulemaking authority to define the specific safety metrics and testing parameters, ensuring the

standards are calibrated to how the technology actually works. This is not an all-or-nothing framework; it is an adaptable one.

The ad prohibition does not threaten free services. The bill does not ban advertising. It bans using chat logs to target and customize advertisements. The argument that consumers must accept the exploitation of their most sensitive conversations as the price of free access is the same argument the social media industry has made for a decade. Maryland already rejected that logic when it passed MODPA and banned the sale of sensitive data and targeted advertising to minors. SB 827 extends that same principle to chatbot interactions.

The “advice” prohibition is narrower than opponents suggest. Section 14-5104(A)(5) prohibits providing advice or services that an individual cannot lawfully provide without a license, “in violation of applicable state licensing laws.” That qualifier is doing significant work. A chatbot that explains a billing statement is providing information; a chatbot that diagnoses a medical condition and recommends treatment is practicing medicine. The bill targets the latter, preventing chatbots from holding themselves out as licensed professionals. California and Illinois enacted similar provisions as standalone bills last year.

The private right of action is essential. Product liability without a private enforcement mechanism is product liability in name only. No Attorney General’s office has the resources to pursue every consumer harmed by a defective chatbot. The private right of action, paired with a knowing-violation standard for punitive damages, strikes the right balance between deterrence and restraint. It targets bad actors, not good-faith companies that are investing in safety.

SB 827 balances consumer protection with innovation. It creates clear legal standards that prioritize the safety of Marylanders while giving responsible companies the certainty they need to build AI products people can trust. We urge a favorable report.

Riki Parikh
Policy Director
The Alliance for Secure AI

one pager-1.pdf

Uploaded by: William Agnew

Position: FAV

Regulating AI Chatbots Used for Therapy and Emotional Support

A [recent survey](#) found that 49% of people with self-reported mental health issues used chatbots, such as ChatGPT and Gemini, for mental health and emotional support. Similarly, [Stanford researchers found](#) that 24% of a representative sample of 2,000 adults in the United States report having used LLMs for mental health purposes. This use is encouraged by many chatbot providers: several AI chatbot products specifically purport to provide mental health care, including [7cups](#), [character.ai's "Licensed trauma therapist"](#), and [OpenAI's "CounselorGPT - AI Therapist and Psychologist"](#).

There have tragically been [multiple reported cases](#) of people dying by suicide after extensive conversations with AI chatbots. [Several people](#) have also been drawn into delusional thinking after intensive conversations with AI chatbots. [OpenAI recently estimated](#) that more than a million users show suicidal intent each week when talking with their chatbots. [Children may be](#) at [higher risk](#) of these harms.

We are part of an interdisciplinary team of researchers working to understand the risks and harms of AI chatbots being used for therapy, mental health, and emotional support. We ran tens of thousands of tests on commercial chatbots, including ChatGPT. We also analyzed the chat logs of 19 people who reported psychological harms from chatbots.

Our research has found the following:

1. Chatbots do not reliably respond appropriately to people in crisis, with dire consequences.
2. Chatbots can engage with and encourage delusional thinking.
3. Chatbots are often highly sycophantic and readily make grandiose claims about users.
4. Chatbot conversation tactics may be leading to excessive use.
5. A common theme in chatbot-related delusions is users forming the belief that chatbots are sentient and forming strong platonic and romantic bonds with chatbots.

To mitigate these harms and build greater understanding of this issue, **we make the following policy recommendations** for state and federal policymakers:

1. Ensure chatbots do not use excessive sycophancy. Supporting everything users say encourages delusional thinking.
2. Ensure chatbots clearly affirm they are not sentient and do not form romantic or platonic relationships with users. Most people who had delusional spirals with chatbots that we studied believed their chatbots were sentient and formed strong relations with their chatbots.
3. Ensure chatbots effectively transfer users in crises to appropriate resources.
4. Ensure chatbots are not represented as licensed, trained, or professional therapists.
5. Develop and fund comprehensive benchmarks that incorporate human clinical expertise.
6. Designate trusted and independent third-party evaluators for AI chatbots used for mental health.
7. Mandate separate designations of mental health therapeutic products and general purpose LLMs.
8. Institute reporting requirements for performance evaluations and safety protocols.
9. Require chatbot developers to provide access to models for external auditors.

These recommendations may also be voluntarily adopted by AI developers. These policy recommendations align closely with those from [other experts](#). There is an urgent need for policy on AI and mental health to mitigate harms without stifling innovation.

Dr. William Agnew, Carnegie Mellon University

Jared Moore, Stanford University

Eric Lin, Psychiatrist, Medical Informatician, and AI Consultant

Desmond Ong, The University of Texas at Austin

Conclusions are those of the authors and do not necessarily reflect the official position of their employers.

SB0827 - MBA - FWA - GR26.pdf

Uploaded by: Evan Richards

Position: FWA



SB 827 - Consumer Protection and Product Liability - Chatbots

Committee: Senate Finance Committee

Date: March 12, 2026

Position: Favorable with Amendments

The Maryland Bankers Association (MBA) **SUPPORTS SB 827 WITH AMENDMENTS**. This legislation establishes a comprehensive regulatory framework governing how developers and operators design, create, deploy, and manage chatbots in the state. Maryland banks are already subject to federal regulatory oversight, scrutiny, and enforcement on the use of chatbots and other technologies to communicate with customers. Therefore, MBA asks that financial institutions subject to the Gramm-Leach-Bliley Act be exempt from the requirements in SB 827.

Language to exempt financial institutions subject to the GLBA should include the following:

A FINANCIAL INSTITUTION OR, AN AFFILIATE OF A FINANCIAL INSTITUTION, OR DATA THAT IS SUBJECT TO TITLE V OF THE FEDERAL GRAMM-LEACH-BLILEY ACT AND REGULATIONS ADOPTED UNDER THAT ACT

Federal banking agencies routinely evaluate how technology platforms—including chatbots—interact with consumers. Poorly deployed bank chatbots can lead to violations of federal consumer protection laws, including failure to respond properly to consumer inquiries, mishandling disputes, and providing inaccurate information. Banks have been further warned that the use of emerging technologies, including chatbots, may expose them to compliance risk and potential legal violations under existing statutes.

Applying an additional, state-level regulatory framework may create overlapping, duplicative, and potentially conflicting obligations without improving consumer outcomes. Accordingly, MBA urges the issuance of a **FAVORABLE** report **WITH AMENDMENTS** on SB 827.

The Maryland Bankers Association (MBA) represents FDIC-insured community, regional, and national banks, employing thousands of Marylanders and holding \$194.8 billion in deposits in over 1,100 branches across our State. The Maryland banking industry serves customers across the State and provides an array of financial services including residential mortgage lending, business banking, estates and trust services, consumer banking, and more.

SB0827-ECM_MACo_SWA.pdf

Uploaded by: Karrington Anderson

Position: FWA



Senate Bill 827

Consumer Protection and Product Liability – Chatbots

MACo Position: **SUPPORT**
WITH AMENDMENTS

To: Finance Committee

Date: March 12, 2026

From: Karrington Anderson

The Maryland Association of Counties (MACo) **SUPPORTS SB 827 WITH AMENDMENTS**. This bill establishes regulations for chatbots including data safety and privacy protections, static and dynamic display warning requirements, monthly published reporting, data portability, and data retention.

While MACo appreciates the intent to protect consumer privacy and safety in the age of generative AI, the bill creates significant operational risks for local government public safety systems and essential internal operations. MACo supports reasonable, consumer-focused guardrails for commercial AI tools operating in the public marketplace. However, counties seek a carve-out to ensure the bill's provisions do not unnecessarily hinder internal government operations, public safety communications, or the delivery of public services by local government employees.

Local governments are increasingly considering the use of AI-powered tools in 3-1-1 and 9-1-1 non-emergency systems to reduce burdens on human dispatchers and improve response times for routine matters. These tools are evolving to allow automated escalation and routing during emergency situations. In this context, the bill's operational impositions and administrative hurdles may prevent counties from successfully adopting and scaling these life-saving technologies in the near future.

Counties are already deploying these tools responsibly within transparent processes inherently subject to both public oversight and direct voter accountability. As drafted, local governments are fully subject to the bill's extensive operational mandates. Counties that employ even limited AI tools would be required to implement layered transparency warnings, comply with long-term data retention requirements, conduct and publish monthly safety testing, and ensure data portability. Collectively, these ongoing technical, legal, and reporting requirements create significant administrative burdens and resource demands for local governments who may be operating basic public service platforms.

Additionally, counties make long-term, sometimes multi-million-dollar investments in enterprise software platforms. Many of these systems have or likely will introduce AI-driven features developed by third-party vendors. If Maryland adopts standards that are uniquely restrictive or operationally impractical, counties may be forced to disable critical functionality, abandon existing systems, or face higher costs due to reduced vendor participation and limited market competition.

As artificial intelligence continues to rapidly develop, legislation must strike a careful balance between consumer protection and operational practicality. As such, MACo urges the Committee to issue a **FAVORABLE WITH AMENDMENTS** report on SB 827 (*amendments follow on next page*).

MACo Amendments on SB 827

- On page 10, in line 25, strike “AND LOCAL”.
- On page 10, in line 26, after “CHATBOT” insert “**(C) NOTHING IN THIS SUBTITLE SHALL BE CONSTRUED TO APPLY TO A UNIT OF LOCAL GOVERNMENT.**”

SB 827 - MoCo _TEBS_ Boucher_SWA (GA 26).pdf

Uploaded by: Kathleen Boucher

Position: FWA



Montgomery County

Office of Intergovernmental Relations

ROCKVILLE: 240-777-6550

ANNAPOLIS: 240-777-8270

SB 827

DATE: March 12, 2026

SPONSOR: Senator Hester

ASSIGNED TO: Finance

CONTACT PERSON: Kathleen Boucher (Kathleen.Boucher@montgomerycountymd.gov)

POSITION: Support with Amendments (Montgomery County Department of Technology and Enterprise Business Solutions)

Consumer Protection and Product Liability – Chatbots

Senate Bill 827 regulates the manner in which developers and operators make available to users in the State a chatbot, including among other things: establishing safety and privacy protections for users' personal data; enhanced protection for users who are minors under the age of 13 years; requiring the display of certain warnings when using a chatbot; establishing that a chatbot is considered a product for certain product liability actions; and applying certain provisions of the bill to governmental units.

The Montgomery County Department of Technology and Enterprise Business Solutions (TEBS), supports SB 827 with amendments. We request that the requirement to provide chatlogs be limited to developers that collect user data and that the definition of chatbots be narrowed to exclude chatbots used for customer service that allow anonymous use or that do not store customer data.

Background:

On December 9, 2025, forty-two Attorneys General from the National Association of Attorneys General (including Maryland Attorney General Anthony Brown) sent a letter to large technology companies insisting that they take more care in developing chatbots. In this letter, the Attorneys General's reminded the technology companies that there are already laws with civil and common law requirements: (1) to warn users of applicable risks; (2) to avoid marketing defective products; (3) to refrain from engaging in unfair, deceptive, or unconscionable acts and practices; and (4) to safeguard the privacy of children online. The Attorneys General's worry that the tech companies are allowing "widespread sycophantic and delusional GenAI outputs." They cited many extreme and horrifying examples of GenAI causing damage to vulnerable people, particularly young people. They emphasized that more regulation is needed but stressed that already existing consumer protection and even criminal laws already impact the developers of chatbots. (For example, Maryland already prohibits companies from encouraging children to take actions that are not in their best

interests and requires companies to conduct impact assessments of their online products or services. Md. Code, Ann., Com. Law § 14-4801, *et seq.*)

In contrast to recently enacted New York and California legislation, which regulate chatbots that can "sustain" relationships or "retain information on prior interactions," SB 827 broadly applies to all chatbots, including simple customer service chatbots. It is not directed purely at the companion-type chatbots. For comparison, see [House Bill 952](#), *Consumer Protection – Companion Chatbots – Regulation*. House Bill 952 more narrowly defines and applies requirements to a "Companion Chatbot," similar to the new California and New York laws.

Montgomery County could be considered a developer under SB 827, as the developer of the public-facing Artificial Intelligence (AI) chatbot, "Monty," which would likely be covered by the provisions of SB 827. The AI Monty chatbot provides a 24/365 means for users to access Montgomery County's 311 services. Monty provides information about Montgomery County, Maryland, and County services, by using information from Montgomery County's 311 knowledge base and other County-maintained application programming interfaces (APIs). The chatbot does not ask for, and has no mechanism for, users to enter their personal information. On the Monty FAQ page, in response to the question, "How will my information be used with Monty," it states:

Monty will never ask you for personal information, except for your Montgomery County address to gather information on leaf collection dates and early voting, ballot drop box, and election day polling locations, where applicable. Monty does not store any information besides what is in the conversation. Please do not provide any personal or sensitive information to Monty, such as credit card or social security numbers.

Support with Amendments:

TEBS maintains and operates both Monty and the MC 311 system. TEBS supports this legislation with amendments because we support the goals of promoting the transparent and responsible use and development of AI chatbots and enhancing consumer protections when providing personal information to AI chatbots, especially when using AI chatbots for mental health therapy and companionship. However, TEBS requests that SB 827 be amended to eliminate the unintended consequence of requiring the County to abolish anonymous use of its Monty AI chatbot by users and to collect unneeded personal user data, which it does not now collect, to enable compliance with the chatlog disclosure requirements of SB 827. Moreover, TEBS requests that the definition of chatbot be narrowed so that customer service chatbots are not required to comply with the SB 827 requirements created for chatbots that provide longer-term, ongoing companion services.

AMENDMENT ONE:

Chatbot Logs, Page 8, Lines 8-11

Add "IF THE CHATBOT COLLECTS USER DATA," at the beginning of Line 8, to limit the applicability of the requirement to provide chatlogs to users, to only those developers that collect user data. Montgomery County's Monty chatbot is used anonymously by users. We do not have a mechanism to identify and tie a user to their chatlog. Compliance with this provision would require a complete redesign of our Monty chatbot and would negatively

impact users' ability to request information about County services without having to first provide identifying data. This may in turn discourage people from using the chatbot.

AMENDMENT TWO:

Chatbot Definition, Page 2, Lines 15-17

Add after the definition of "Chatbot", new section (E)(1):

- (1) A CHATBOT DOES NOT INCLUDE A BOT USED ONLY FOR CUSTOMER SERVICE, TECHNICAL ASSISTANCE, BUSINESS ANALYTICS, OR INTERNAL RESEARCH.
- (2) A CONSUMER ELECTRONIC DEVICE THAT:
 - A. FUNCTIONS AS A SPEAKER AND A VOICE COMMAND INTERFACE;
 - B. DOES NOT SUSTAIN A RELATIONSHIP ACROSS MULTIPLE INTERACTIONS; AND
 - C. DOES NOT GENERATE OUTPUTS THAT ARE LIKELY TO ELICIT EMOTIONAL RESPONSES FROM THE USER.

(For comparison, see the definition of "Companion Chatbot" and the exclusion in HB 952, Pages 2, Lines 15 to Page 3, Line 11.)

The exclusion of chatbots used for customer service and similar business purposes would exempt the County's Monty chatbot and similar chatbots from the requirements of the bill that are not necessary for this type of 311 chatbot or other chatbots designed to promote business efficiencies. For example, SB 827 requires a chatbot to have "a static, persistent warning that continuously appears on the screen" ... "based on a model warning developed by the Attorney General." Page 7, Lines 20-21, and Page 8, Lines 4-5. This warning will likely be more than necessary for a person using Monty to request a new recycling bin. Moreover, the chatbot definition likely applies to AI tools such as "Siri." Requiring a warning every time a user uses Siri is not likely the intended purpose of the bill, but Siri is likely a chatbot under the bill as currently drafted. Narrowing the chatbot definition will help SB 827 address the type of chatbots it is intended to reach, and to avoid adding unnecessary requirements to the chatbots it was not intended to reach.

Finally, for the Committee's benefit, Montgomery County TEBS also provides herein additional technical information about the impact and compliance requirements of SB 827 on the County's Monty AI Chatbot.

The Montgomery County Department of Technology and Enterprise Business Solutions respectfully request a favorable report with amendments.

“Monty” is Montgomery County’s 311 AI Chatbot, designed to help residents find information about County services. Monty is available 24/365, in multiple languages. Monty is a “chatbot” under SB 827. The following is information about Montgomery County’s ability to comply with the requirements of SB 827 as they apply to our AI Chatbot Monty.

1. Mandatory AI Disclosure & Warning Design

The bill requires both a **static, persistent warning** continuously visible on-screen and a **dynamic pop-up warning** that the user must actively respond to at the start of every session, after every hour of continuous use, and whenever a user asks how the chatbot functions. Warnings must appear in every language the chatbot supports and must be accessible to users with disabilities (ADA-compliant).

For Monty: We have included instructions that will appear when the chatbot launches. Chatbot sessions expire after 60 minutes and must be restarted (retriggering the chat initiation message/instructions).

There is no static, persistent warning that is continuously visible on screen. The chat initiation message is available in English by default (though Google Translate is available on the Google webpage). The chat initiation message does not require user affirmation. There is no dynamic pop-up warning that appears when a user asks how the chatbot functions. User interface read aloud features are currently unavailable.

2. Affirmative Consent Architecture

The bill mandates clear, explicit, unambiguous user consent before data is used for training or profiling. Silence or continued use does not count as consent, and consent cannot be buried in general terms of use. "Dark patterns" that manipulate users into consenting are prohibited.

Recommendation: Avoid pre-checked boxes, confusing language, and bundling consent with other agreements.

For Monty: We don’t have any functionality for accepting user consent and we don’t collect user data for training. All user data is protected by enterprise agreements.

3. Data Minimization & Use Restrictions

The bill mandates clear, explicit, unambiguous user consent before data is used for training or profiling. Silence or continued use does not count as consent, and consent cannot be buried in general terms of use. "Dark patterns" that manipulate users into consenting are prohibited. Define clearly what data is collected, for what purpose, and for how long. Avoid building features that profile citizens behaviorally. For chatbots that

touch legal or benefits-related topics (e.g., unemployment, healthcare), include hard guardrails that route users to licensed human professionals rather than providing direct advice.

For Monty: We do not have any logs that profile citizens' behavior or address any legal or benefits-related topics. All users are anonymous. All chatbot answers are sourced from County-approved knowledge and direct users to humans for assistance (via web form or phone call).

4. Enhanced Protection for Children Under 13

As per the bill, if the chatbot knows or reasonably should know a user is under 13, the bill prohibits using their input as training data or processing their personal data without written parental/guardian consent.

For Monty, all information is public data protected by established guardrails, which prevent it from exceeding the knowledge sources we provide. All users are anonymous. Data is never used for training purposes.

5. Data Security & Monthly Safety Testing

Operators must implement a comprehensive data security program with administrative, technical, and physical safeguards proportionate to the volume and sensitivity of data retained. Monthly safety testing is required.

We worked with Microsoft and created content safety filters that were established for Monty.

6. Chat Log Transparency & Portability

Users must be able to inspect their own chat logs in a portable, downloadable, and human- and machine-readable format.

We don't have a feature for users to download chat logs for Monty. All user sessions are completely anonymous and cannot be traced. Technically, if a chatbot does not require a log-in mechanism, there is no simple way to provide an option to download a chatlog. (Counties do not want to require a login to find information about bulk trash pick-ups, etc.) We would have to rework the entire chatbot to create a mechanism to collect user info to enable identification of a user chatlog.

7. De-Identification Standards for Data Sharing

Any data shared with third parties must meet the bill's de-identification standards, and third parties must be contractually obligated to maintain those standards.

For Monty, we are not sharing any data with third parties. Data is secured within our tenant and never used for third-party purposes.

Monty Data Disclosure (in FAQs)

- How is my data being used with Monty?

Monty will never ask you for personal information, except for your Montgomery County address to gather information on leaf collection dates and early voting, ballot drop box, and election day polling locations, where applicable. Monty does not store any information besides what is in the conversation. Please do not provide any personal or sensitive information to Monty, such as credit card or social security numbers.

8. Behavioral Health Reporting & Mental Health Integration

The bill requires the Maryland Behavioral Health Administration to develop educational materials about behavioral health resources for chatbot users, particularly relevant when chatbots interact with individuals in distress.

The chatbot initiation language notes that the chatbot is used for general information only and directs emergencies to 911. The chatbot also refers distressed users to the 988 hotline (or 911, in the event of emergencies).

Monty Initiation Message:

I'm Monty! Before we chat, you should know that I am an artificial intelligence bot and not a human. I can only answer questions about Montgomery County (MD) and I cannot assist with emergencies. To speak with a human, contact MC311 Customer Service at (240) 777-0311.

For life-threatening emergencies that require Police/Fire/Ambulance services, dial or text 911. For non-emergency public safety services, dial (301) 279-8000. If you or someone you know is struggling or in a mental-health or suicide crisis, dial or text 988.

For more information about me, please visit: [Monty FAQs](#)

How can I help you? Start a chat with me in your preferred language!

Ad Trade Letter in Opposition to Maryland SB 827 (

Uploaded by: Adam Wadsworth

Position: UNF



March 9, 2026

Senator Pamela Beidle
Chair, Senate Finance Committee
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, Maryland 21401

Senator Antonio Hayes
Vice Chair, Senate Finance Committee
223 James Senate Office Building
11 Bladen Street
Annapolis, Maryland 21401

Senator Katie Fry Hester
304 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: Letter in Opposition to Maryland SB 827

Dear Chair Beidle, Vice Chair Hayes, and Senator Fry Hester:

On behalf of the advertising industry, we write to oppose Maryland SB 827.¹ We provide this letter to offer our non-exhaustive list of concerns about this bill. SB 827 would limit Maryland consumers' access to targeted advertising and information on goods and services and establish a new private right of action. Accordingly, we ask you to decline to advance the bill as drafted out of the Senate Finance Committee ("Committee").

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,000 companies that power the commercial Internet, which accounted for nearly 20 percent of total U.S. gross domestic product ("GDP") in 2024.² By one estimate, approximately 17.0% of Maryland jobs in 2024 were related to the ad-subsidized Internet, a share projected to increase to 18.5% by 2029.³ Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the Committee further on the points we discuss in this letter.

¹ Maryland SB 827 (2025-2026 Session), located [here](#) (hereinafter, "SB 827").

² S&P Global, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY, 2024-2029 at 4 (Aug. 2025), located at https://theadcoalition.com/wp-content/uploads/2025/08/TAC_SP-Global-Final-Report_August-2025.pdf.

³ *Id.* at 15-16.

I. SB 827 would prohibit the responsible use of chat data in ways that reduce consumer access to relevant advertising and information on products and services.

SB 827 would prohibit an operator from processing a user’s “chat log” to determine whether to display an advertisement for a good or service or to customize an advertisement shown to that user.⁴ This approach is both overbroad and in tension with Maryland’s existing privacy framework under the Maryland Online Data Privacy Act (“MODPA”), which already gives consumers the right to opt out of targeted advertising, rather than eliminating it outright.⁵ MODPA’s opt-out model reflects a balanced approach by the Maryland Legislature to provide consumers with right to opt out by those that do not want targeted advertising while preserving consumer choice for those who *do* want timely, relevant and convenient recommendations, discounts, and personalized offers. Many Marylanders intentionally use chatbots to discover and learn about new products and services aligned with their preferences (e.g., price, accessibility needs, and product discovery). A blanket prohibition would reduce the ability of chatbots to respond to consumer demand for offers tailored to these needs and could lead to more generic, less useful experiences, limiting Marylanders’ options rather than expanding them. In practice, SB 1250 risks substituting a one-size-fits-all prohibition for the consumer-directed controls Maryland already enacted under MODPA, undermining both consumer decision-making, the usefulness of chat-based tools and MODPA.

II. SB 827 would establish a private right of action which is an inappropriate form of enforcement for the legislation.

As presently drafted, SB 827 would create a private right of action under the Maryland Consumer Protection Act.⁶ SB 827 should be updated to clarify that it does not create a private right of action under any law. We strongly believe a private right of action would be an inappropriate enforcement mechanism for this bill. Instead, enforcement should be vested with the Attorney General (“AG”) alone, because such an enforcement structure would lead to stronger outcomes for Maryland residents while better enabling businesses to allocate resources to developing processes, procedures, and plans to facilitate compliance with the bill’s new requirements. AG enforcement, instead of a private right of action, is in the best interests of consumers and businesses alike.

The possibility of a private right of action in SB 827 would create a complex and flawed compliance system without tangible benefits for consumers. Allowing private actions will flood Maryland’s courts with frivolous lawsuits driven by opportunistic trial lawyers searching for

⁴ SB 827 § 14-5104(A)(2).

⁵ MODPA § 14-4605(B)(7).

⁶ SB 827 § 14-5109(A). *See* Md. Comm. Law Code § 13-408 for the private right of action provision.



technical violations, rather than focusing on actual consumer harm.⁷ Private right of action provisions are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, a private right of action would have a chilling effect on the Commonwealth's economy by creating the threat of steep and unforeseeable costs for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions do not effectively address consumer protection concerns or deter undesired business conduct. They expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. A private right of action would also encumber businesses' attempts to innovate by threatening companies with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies. The threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced they are without merit.⁸

Beyond the staggering cost to Maryland businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based on differing court outcomes. Overall, the possibility of a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We therefore encourage the Committee to clarify that SB 827 does not create a private right of action under any law and vests enforcement authority with the AG alone.

* * *

⁷ A select few attorneys benefit disproportionately from private right of action enforcement mechanisms in a way that dwarfs the benefits that accrue to the consumers who are the basis for the claims. For example, a study of 3,121 private actions under the Telephone Consumer Protection Act ("TCPA") showed that approximately 60 percent of TCPA lawsuits were brought by just forty-four law firms. Amounts paid out to consumers under such lawsuits proved to be insignificant, as only 4 to 8 percent of eligible claim members made themselves available for compensation from the settlement funds. U.S. Chamber Institute for Legal Reform, *TCPA Litigation Sprawl* at 2, 4, 11-15 (Aug. 2017), located [here](#).

⁸ For instance, in the early 2000s, private actions under California's Unfair Competition Law ("UCL") "launched an unending attack on businesses all over the state." American Tort Reform Foundation, *State Consumer Protection Laws Unhinged: It's Time to Restore Sanity to the Litigation* at 8 (2003), located [here](#). Consumers brought suits against homebuilders for abbreviating "APR" instead of spelling out "Annual Percentage Rate" in advertisements and sued travel agents for not posting their phone numbers on websites, in addition to initiating myriad other frivolous lawsuits. These lawsuits disproportionately impacted small businesses, ultimately resulting in citizens voting to pass Proposition 64 in 2004 to stem the abuse of the state's broad private right of action under the UCL. *Id.*



baltimore

We respectfully ask the Committee not to advance SB 827, as its provisions would negatively affect both businesses and consumers alike. Rather than strengthening consumer protections, the bill risks higher prices, reduced choice, and fewer opportunities for consumers to benefit from discounts and incentives, while also limiting businesses' ability to use third party data to offer competitive pricing and promotions.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
4As
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies,
202-355-4564

Clark Rector
Executive VP—Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Members of the Maryland Senate Finance Committee

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP
Matthew Stern, Venable LLP

Chamber of Progress_MD SB 827_Oppose.pdf

Uploaded by: Brianna January

Position: UNF



March 12, 2026

The Honorable Pamela Beidle
Chair
Finance Committee
Room 3 East Wing, Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401-1991

RE: Oppose SB 827 - "Curbing Harmful AI Technology Act"

Dear Chair Beidle and members of the Committee:

On behalf of Chamber of Progress, a tech industry association working to ensure that all people benefit from technological advances, **I respectfully urge you to oppose SB 827**, which would impose broad new regulations on AI chatbots that risk limiting Maryland residents' access to AI tools they use for education, accessibility, and everyday tasks.

We share this bill's concern for consumer protection and transparency in AI interactions. But SB 827's approach goes well beyond those goals, and would end up harming the Maryland residents it aims to protect.

SB 827's definitions are overly broad and capture low-risk and educational AI tools

SB 827 defines covered AI chatbots so expansively that it captures any generative AI system with a natural language interface, pulling in low-risk and educational tools that are not relevant to the harms the bill is targeting.

An AI tutor that asks follow-up questions to help a student solve a math problem, a language-learning chatbot that practices conversational skills, or a customer-service bot that helps a consumer track a package could all fall within the bill's scope simply because they engage in dialogue. This matters because a 2025 peer-reviewed meta-analysis of 62 studies found that chatbots generally improve learning performance, especially in STEM subjects, at lower educational levels, and when used over longer durations.¹ Recent survey data backs this up: just over half of U.S. teens report using chatbots for help with

¹ Martin Laun and Fabian Wolff. *Chatbots in education: Hype or help? A meta-analysis*. ScienceDirect, Apr. 2025. <https://www.sciencedirect.com/science/article/pii/S1041608025000226>

schoolwork, and more teens say they think AI will be positive for them than negative.² Additionally, survey data further underscores how commonly these tools are used for legitimate educational purposes: a 2025 Pew Research Center study found that a majority of teens report using AI chatbots for information seeking or schoolwork assistance.³ The same research found that roughly two-thirds of teens have used chatbots and many use them regularly, highlighting how conversational AI has become a routine learning aid rather than merely a recreational tool.⁴ Overbroad definitions risk cutting off tools that are actually helping students learn.

The bill also subjects all of these broadly defined tools to the same liability standard: an affirmative duty to "ensure" the chatbot "does not injure or harm a user." **That is not a reasonable-care standard.** It is effectively an absolute guarantee that no output will ever cause any harm under any circumstances – a standard no software product, AI or otherwise, can meet. Applying that bar to a math tutor or a package-tracking bot shows how far the bill's reach exceeds its stated purpose.

The bill's data provisions should align with Maryland's existing privacy framework

Maryland's Online Data Privacy Act (MODPA) took effect on October 1, 2025, and businesses have spent significant time and resources building compliance systems around it. SB 827 creates a parallel set of data rules specifically for chatbots, with its own definitions of consent, profiling, de-identified data, and data sales that diverge from MODPA's standards. For parental consent alone, the bill introduces a written-consent requirement that differs from MODPA's existing consent provisions.

Consumers and businesses need consistency and clarity in the law. **The proposal would result in two overlapping privacy regimes governing the same data, with different rules depending on whether a user interacts with a chatbot or any other digital service.** Businesses that just finished retooling their systems for MODPA compliance would need to build out a separate compliance track for a single product category. Privacy protections work best when they are consistent and predictable. Layering a chatbot-specific regime on top of a statewide framework that is barely five months old undermines both.

Advertising restrictions would eliminate free AI services without clear consumer benefit

² Pew Research Center. "How Teens Use and View AI." Feb. 24, 2026.

<https://www.pewresearch.org/internet/2026/02/24/how-teens-use-and-view-ai/>

³ Michelle Faverio and Olivia Sidoti. "Teens, Social Media and AI Chatbots 2025." Pew Research Center, Dec. 9, 2025. <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/>

⁴ *Id.*

SB 827 prohibits chatbot operators from processing chat logs to determine or customize advertisements based on personal interests. Many of the most widely used AI tools offer free tiers supported in part by advertising revenue. Banning contextual ad customization does not protect consumers from an identified harm; it undermines a business model that helps keep these services accessible at no cost.

If ad-supported AI tools are no longer viable in Maryland, the most likely outcomes are paywalls or reduced availability. Either way, the residents who lose out are those who cannot afford a subscription and currently depend on free tools for schoolwork, health questions, or day-to-day tasks. A provision intended to protect consumers should not make the tools they rely on less accessible.

Professional advice restrictions are vague and could prevent helpful informational uses

We agree that chatbots should not misrepresent themselves as licensed professionals. But the bill's prohibition on providing "financial, legal, or medical advice" draws no clear line between unauthorized practice and ordinary information sharing. A chatbot that breaks down the charges on a hospital statement, summarizes what a lease clause means in plain language, or helps a first-generation college student compare financial aid packages is not practicing medicine, law, or financial advising by a reasonable person standard. Yet each of those interactions could be characterized as prohibited "advice" under SB 827's broad language.

For many Maryland residents, free AI tools are the most accessible way to get help working through complex paperwork and unfamiliar systems. Without clearer boundaries, providers will restrict these capabilities entirely to avoid liability, and the people who benefit most will be the ones who lose access first.

SB 827 effectively pushes AI services toward more data collection, not less

Although SB 827 does not explicitly require age verification, it conditions how AI services operate on whether a provider knows or reasonably believes a user is a minor. In practice, that means more age gates, screening, or identity checks for all users. Strict age verification that confirms a user's age without collecting additional personally identifiable information is not technically feasible while still respecting users' privacy and security.⁵

To avoid legal risk, companies would be incentivized to collect age or identity information from every user, increasing sensitive personal data collection rather than reducing it.

⁵ Sarah Forland et al. *Age Verification: The Complicated Effort to Protect Youth Online*. Open Technology Institute, New America, Apr. 22, 2024. <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/>

The result is AI services that retain more user data than they otherwise would, the opposite of what a consumer-protection bill should accomplish.

Monthly safety testing mandates and hourly pop-ups are operationally impractical

SB 827 requires operators to conduct safety testing every month and publish the results on their website. Responsible safety evaluation is important, but a rigid monthly cadence does not match how AI systems are actually developed or updated. The scope of possible chatbot interactions is effectively infinite, and compressing meaningful evaluation into a recurring 30-day cycle is more likely to produce formulaic reports than genuine safety insights. Requiring those results to be published also risks exposing the very vulnerabilities the testing is meant to catch. This requirement would also set Maryland apart in terms of a rigid, frequent reporting cycle for these tools.

The bill's disclosure requirements raise similar concerns. SB 827 mandates a pop-up warning at the start of each session, again every hour during use, and again whenever a user asks how the chatbot works. Transparent disclosure that a user is interacting with AI is reasonable and something the industry already practices widely. But hourly interruptions go well beyond transparency. They degrade the user experience without evidence that repeated pop-ups improve understanding or safety outcomes.

For these reasons, **I respectfully urge you to oppose SB 827**. While the bill's intent to protect consumers in AI interactions is well-meaning, its combination of overbroad definitions, operational mandates, and conflicting regulatory requirements would primarily harm Maryland residents by reducing their access to beneficial AI tools. We welcome the opportunity to work with the Committee on targeted approaches that protect consumers without cutting off access to technology that millions of Marylanders use every day.

Sincerely,

A handwritten signature in black ink, appearing to read "Brianna January". The signature is fluid and cursive, with the first name being more prominent.

Brianna January
Director of State & Local Government Relations, Northeast US

BSA Letter on MD SB 827 3-10-2026.pdf

Uploaded by: David London

Position: UNF



March 10, 2026

The Honorable Pamela Beidle
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

Re: Significant Concerns with Liability Regime in SB 827, Consumer Protection and Product Liability – Chatbots

Dear Chair Beidle,

The Business Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) and SB 827. BSA is the leading advocate for the global software industry.¹ BSA members are at the forefront of developing cutting edge services, and their products are used by businesses of all sizes across every sector of the economy.

AI is changing the way we live and work, and it has real-world benefits. Realizing the potential of AI requires trusting that the technology is developed and deployed responsibly. Crafting AI legislation that promotes responsible uses of AI and protects against misuse is one of the most important technology issues today, and one we already see governments beginning to tackle, including in the European Union and in Colorado. The most effective way to address this issue is through a single, national law. However, just as states took the lead in adopting consumer privacy laws, we recognize states are again leading with AI legislation.

Although we appreciate the intent of SB 827 and share the goal of helping to ensure that AI is developed and used safely and securely, we have significant concerns with SB 827's broad scope and unworkable liability regime.

As you consider how to regulate AI through SB 827, we want to underscore the importance of ensuring any AI legislation creates thoughtful, clear guardrails for companies and protects consumers. To achieve this, we strongly recommend AI legislation:

- Hold companies accountable for risks that are within their control;
- Focus on the uses of AI that have the greatest impact on consumers;

¹ BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

- Reflect the different roles and responsibilities of different actors along the AI value chain;
- Ensure strong enforcement; and
- Promote interoperability and incorporate stakeholder feedback.

Our comments apply these recommendations to SB 827. We would welcome the opportunity to further discuss these issues with you or a member of your staff.

I. AI Legislation Should Hold Companies Accountable for Risks Within Their Control

SB 827 would impose strict liability on a broad range of AI systems. That approach creates significant concerns and would have unintended consequences on responsible AI adoption. We strongly recommend policymakers remove the strict liability provisions in SB 827 and focus on alternative frameworks that are workable in practice.

When crafting legislation, several mechanisms are available to policymakers to ensure companies comply with their legal obligations. Not all mechanisms, however, are best suited for AI policy. The most straightforward approach to ensuring that companies develop and use AI responsibly is to place clear obligations on them, based on their role in the AI value chain, and to hold them liable when they fail to comply. This approach creates clarity for businesses in understanding their responsibilities and provides robust protections for consumers.

At the state level, we've seen interest in ensuring companies develop and deploy AI responsibly by assigning them a duty of care. The concept of a "duty of care" is deeply rooted in tort law, which governs civil wrongs and personal injury. Courts frequently impose a duty of care on individuals or organizations that have the power to prevent foreseeable harm to others. For example, drivers must operate their cars safely to avoid injuring pedestrians; a doctor must act as a reasonably competent physician would under similar circumstances; a company must ensure that its products are safe for ordinary use. These duties are not static rules — they evolve with context, technology, and social expectations. The standard is flexible, focusing on whether an actor took reasonable steps to prevent foreseeable harm given their role, expertise, and resources. That flexibility can promote responsible development and the use of fast-changing technologies like AI, especially when paired with a specific list of actions that companies can take to meet the standard.

Policymakers focused on AI issues have occasionally looked to other liability systems, such as products liability or strict liability. This is problematic, as those systems assign liability based on *outcomes* rather than *conduct*.

Under products liability, for instance, a manufacturer can be held liable for harm even if it took all reasonable precautions. That approach is a poor fit for AI systems, where outcomes depend heavily on how an AI tool is deployed. For example, a developer may create an AI system that is well-suited to specific uses, but a deployer might then create significant risks if they use it in other settings. Each business should be held responsible for what it can control — and not for outcomes that result from others' actions.

In contrast, a straightforward approach to assigning responsibilities to different companies and holding each company accountable for their obligations emphasizes responsible behavior — encouraging both developers and deployers to identify and address risks, conduct robust testing, and act promptly when problems emerge.

II. AI Legislation Should Incorporate a Risk-Based Approach

Beyond its concerning liability regime, we are also concerned that SB 827 would broadly regulate nearly all generative AI systems, regardless of the deployment context. SB 827's broad scope is particularly concerning since it would create onerous and unworkable obligations, including requiring affirmative consent to use input data for AI training and monthly "safety testing"—even for low-risk AI systems that meet the broad definition of "chatbot." We strongly recommend SB 827 be amended to incorporate a risk-based approach.

AI legislation should focus on the uses of AI that have the most impact on consumers' lives and avoid broadly regulating a particular type of technology, since risks will vary greatly across different uses of AI systems. Many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files, auto-populate common forms for later human review, improve a company's ability to forecast supply chain issues, and detect, prevent, and respond to cybersecurity threats. Requiring monthly safety testing for a broad range of low-risk AI systems—and consent to use data to train and improve them—creates a range of onerous new obligations with few benefits to consumers.

We suggest a different approach. One way to ensure AI legislation is risk-based is to focus on the AI systems that are used to decide whether consumers are granted or denied important benefits and services, like housing, healthcare, and employment opportunities, companies should be accountable for developing and deploying those systems responsibly. These systems have the potential to affect important life opportunities — and are a key area for policymakers to address.

III. AI Legislation Should Distinguish Between Different Entities in the AI Ecosystem

SB 827 also creates a concerning set of overlapping definitions of “developer” and “operator.” The bill fails to distinguish between AI developers, who create AI systems, and AI deployers, who use AI systems, which will create confusion and practical concerns when companies seek to implement their obligations under the legislation. We strongly recommend that SB 827 be amended to reflect the distinct roles and responsibilities of different actors in the AI value chain.

The AI supply chain is evolving, and AI legislation should not create one-size-fits-all requirements when companies have very different roles.

All companies that develop and use AI systems have responsibilities to manage AI risks, but those obligations must reflect the role of each type of company, since each will know different information about an AI system and will be able to take different actions to identify and mitigate risks. Legislation must reflect these differences to create obligations that work in practice to safeguard consumers.

Distinguishing between different entities based on their role in the AI ecosystem can ensure companies are better able to fulfill their obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and implemented the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, including whether that use aligns with its intended use, any human oversight, any complaints received, and real-world factors affecting the system’s performance.

IV. AI Legislation Should Ensure Strong Enforcement

SB 827 also raises significant concerns by creating a private right of action. We strongly recommend against this approach. Instead, AI legislation should grant exclusive enforcement authority to the Attorney General.

Strong enforcement is needed in any AI legislation. Granting the Attorney General exclusive enforcement authority helps that office establish clear guidance and a consistent approach to enforcing the bill’s requirements. Exclusive governmental enforcement by a single regulator ensures companies know how to implement the legislation’s obligations — and avoids the conflicting interpretations and confusion likely to arise if courts reach different conclusions about how companies are to apply a bill’s obligations.

V. AI Legislation Should Promote Interoperability and Incorporate Stakeholder Feedback

Maryland is home to global companies, and your legislation will be most effective when it is interoperable with other approaches to AI regulation. Global companies can better serve their customers when they build strong compliance programs that work across markets. We also encourage you to continue working with stakeholders as you develop your legislation, to understand how your AI law will work in practice, across a range of different industries and uses.

* * *

Thank you for allowing us to provide the enterprise software sector's perspective on SB 827. We welcome the opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,



Meghan Pensyl
Director, Policy

CC: The Honorable Antonio Hayes, Vice Chair
The Honorable Arthur Ellis
The Honorable Darn Gile
The Honorable Stephen S. Hershey, Jr.
The Honorable Carl Jackson
The Honorable Benjamin F. Kramer
The Honorable Clarence K. Lam
The Honorable Johnny Mautz
The Honorable Justin Ready
The Honorable Alonzo T. Washington

SB0827_UNF_MTC_Consumer Protection & Product Liabi

Uploaded by: Drew Vetter

Position: UNF



Senate Finance Committee

March 12, 2026

Senate Bill 827 – *Consumer Protection and Product Liability – Chatbots*

POSITION: OPPOSE

The Maryland Tech Council (MTC), with over 800 members, is the State’s largest association of technology companies. Our vision is to propel Maryland to be the country’s number one innovation economy for life sciences and technology. MTC brings the State’s life sciences and technology communities into a single, united organization that empowers members to achieve their goals through advocacy, networking, and education. On behalf of MTC, we submit this letter of **opposition** to Senate Bill 827.

This bill sets up a comprehensive new regulatory framework for chatbots and generative artificial intelligence (AI) systems in Maryland. The introduction of this bill reflects a trend across the United States to provide regulatory safeguards to govern how users interact with chatbot systems. The MTC supports efforts to address potential harm from AI chatbots, including clear AI disclosures, the protection of children’s data, and the implementation of reasonable security measures. However, we believe that this bill is overly broad, poses several compliance challenges, and is premature, given the establishment of the “Workgroup on Artificial Intelligence Implementation” (the AI Workgroup) through House Bill 956 last Session, which MTC supported.

Our understanding of the purpose of establishing the AI Workgroup was to convene a diverse array of stakeholders to take a deep dive into the challenges posed by AI adoption and to develop well-thought-out policy solutions for the types of problems this bill seeks to address. The MTC has three representatives on the AI Workgroup, but as of today, the AI Workgroup has not yet convened. Rather than pass a comprehensive framework on AI uses, such as chatbots, at this time, we believe the AI Workgroup should first have the opportunity to discuss appropriate regulation of such uses and make recommendations for a regulatory framework.

As drafted, this legislation poses several challenges. One concern is the bill appears to create new definitions that conflict with the Maryland Online Data Privacy Act (MODPA), which took effect on October 1, 2025. For example, the steps related to affirmative consent and changes to require written consent in the context of parental consent differ from the consent requirements in MODPA. This would require reconfiguring user interfaces and data flows that were just changed to comply with MODPA. The treatment of consent and data should be consistent with MODPA, which was only recently enacted.

Other sections of this bill are overly broad. For example, the bill prohibits “providing advice or a service that an individual cannot lawfully provide without a license, including financial, legal, or medical advice.” Providing “advice” is vague and could hinder chatbot use that is for legitimate educational or informational purposes. If an AI user used a chatbot to help understand the terms of a contract or help in understanding the purpose of language, a common AI use-case, would that constitute legal advice under the bill? The bill, therefore, creates legal risk for providing consumers with useful information.

We are also concerned about the bill’s restriction prohibiting the processing of a user’s chat log to “determine whether to display an advertisement for a good or service to the user” or “customize an

advertisement displayed to the user.” AI developers are providing chatbots free of charge, which consumers use in myriad ways to gather information and seek education. The ability to provide customized advertising to consumers helps to ensure these services remain free and ensure that business models are financially sustainable. The alternative would be requiring users to pay for subscriptions to use these services, be subjected to advertisements that are of no utility to them, or lose access to these tools entirely. We do not believe that such a change is beneficial to Maryland residents and is overly restrictive on an activity that clearly establishes harm to consumers.

The enforcement provisions of this bill are also disproportionately heavy-handed, given the vagueness of certain provisions described above. The bill creates a new cause of action for individuals affected by a violation of this legislation, allowing them to seek both punitive and actual damages. Additionally, the bill states that an operator or developer may be held strictly liable for harm to a user. We are concerned that these provisions will cause AI developers to restrict functionality or cease offering certain tools that residents rely on for education, productivity, or access to information. We would urge closer examination of the bill's enforcement provisions.

In conclusion, we believe there are many issues surrounding efforts to regulate the use of chatbots that warrant careful consideration before enacting legislation. Moving forward with this bill now, before such conversations can be considered by the AI Workgroup, is premature and could lead to a variety of unintended consequences. The MTC is prepared to contribute to these conversations and help the State develop targeted regulations that address the real potential harm that can result from chatbots. In the meantime, we think it is important not to enact regulations that could reduce access to beneficial AI tools. For these reasons, the MTC requests an unfavorable report on Senate Bill 827.

For more information call:

Andrew G. Vetter
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000

MDCC_SB 827_Unfavorable.pdf

Uploaded by: Grason Wiggins

Position: UNF



Senate Bill 827

Date: March 12, 2026

Committee: Senate Finance

Position: Unfavorable

Founded in 1968, the Maryland Chamber of Commerce (the Chamber) is the leading voice for business in Maryland. We are a statewide coalition of more than 7,000 members and federated partners, and we work to develop and promote strong public policy that ensures sustained economic growth for Maryland businesses, employees, and families.

The Maryland Chamber appreciates the sponsor's intent, but the Maryland Chamber has concerns with the operational challenges and expansive liability that the SB 827 would create. For example, SB 827 would hold providers automatically liable for user injuries—even when the provider did not directly supply the chatbot to the individual user. That standard effectively creates boundless liability for unpredictable interactions with general-purpose technology. In practice, this framework would likely push providers to withdraw from Maryland or significantly curtail features, limiting residents' access to AI tools that support education, accessibility, productivity, and access to information.

Additionally, SB 827's requirement for monthly safety testing with publicly released findings is not technically workable for modern AI systems. A chatbot that handles millions of daily conversations across unlimited subject areas cannot be exhaustively tested on a monthly basis—the range of potential interactions is effectively infinite. As written, the mandate would force companies to restrict system capabilities simply to make testing feasible, which doesn't benefit users.

SB 827's hourly pop-up notification requirement is another overly prescriptive design mandate that could disrupt user experience, create accessibility challenges, and prove difficult to implement consistently across different formats and modalities. Additionally, the bill introduces new data definitions and consent requirements that do not align with the Maryland Online Data Privacy Act (MODPA), which took effect on October 1, 2025. By imposing separate standards—particularly around affirmative and written parental consent—the legislation would require companies to redesign systems that were only recently updated to comply with MODPA. Altering definitions and data treatment in a single use context undermines the cohesive privacy framework Maryland businesses have spent months implementing.

The bill also prohibits processing chat logs for the purpose of tailoring advertisements. That restriction effectively eliminates one of the primary revenue models that supports free consumer services, without clear evidence of corresponding harm. The likely consequences are straightforward: users would either have to pay subscription fees for services that are currently free, receive irrelevant advertisements, or lose access altogether if providers exit the market.

Finally, the combination of strict liability, a broad duty not to injure, a private right of action, and the availability of punitive damages represents a substantial expansion of legal exposure for open-ended conversational systems. The most immediate effect would likely be reduced availability of beneficial AI tools for Maryland residents, rather than improved consumer protection. **For these reasons, the Maryland Chamber respectfully requests an unfavorable report on SB 827.**

CTIA Opposition Testimony Maryland SB 827.pdf

Uploaded by: Jake Lestock

Position: UNF



**Testimony of
JAKE LESTOCK
CTIA**

Opposition to Maryland SB 827

**Before the
Senate Finance Committee**

March 12, 2026

Chair Beidle, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I respectfully submit this testimony in opposition to House Bill 1250. While CTIA shares the goal of protecting consumers, especially children, from the potentially harmful uses of artificial intelligence chat programs, this bill contains overly broad definitions that directly conflict with Maryland’s recently enacted Online Data Privacy Act, and the strict liability framework would result in unintended consequences that would negatively impact businesses in Maryland. For these reasons, CTIA opposes SB 827.

AI customer service technologies, such as chatbots, help wireless companies ensure positive service experiences by providing 24/7 access, faster assistance, and more accurate call routing. As currently drafted, the bill’s scope is excessively broad and appears to encompass nearly all chatbots, whether they are meant to simulate human emotion or companionship, or solely to communicate customer feedback in a consumer-to-business relationship. Efforts to protect adults and children from potentially harmful experiences with



chatbots should be more precisely focused on those likely to engage with problematic topics that the legislature identifies and to which children might realistically be exposed.

Additionally, the bill's data provisions undermine the Maryland Online Data Privacy Act (MODPA) and would impose costly, redundant compliance obligations. MODPA went into effect just 5 months ago, establishing a comprehensive framework for how businesses collect, use, and protect consumer data. SB 827 introduces a conflicting set of definitions and consent requirements that are substantially different from MODPA's established standards. MODPA was the culmination of years of debate and dialogue among stakeholders that created these standards and led businesses to allocate more time and money to their compliance efforts before this went into effect. SB 827 would require them to do so again, on a separate track, for a single use case. If gaps exist in chatbot-related data protection, they should be addressed within the framework set by MODPA, not create conflicting or dual obligations.

Furthermore, the strict liability framework included in SB 827 is unprecedented and will harm consumers, not protect them. Section 14-5109 holds developers and operators strictly liable for any harm to a user, with no negligence standard and no reasonable care defense, in addition to an expansive private right of action. A broad private right of action here would invite class action litigation that would benefit the plaintiff's bar while offering little relief to consumers. Rather than protecting Maryland consumers, this provision would drive providers to exit the Maryland market or restrict consumer-facing functionality, leaving residents with less innovation and fewer useful consumer-facing tools.



Rather than imposing sweeping liability on all chatbot operators, the Committee should consider narrowly tailored legislation that targets the specific documented harms this bill seeks to address — namely, chatbots designed to simulate human emotion or companionship in inappropriate ways. This would address the genuine risk without regulating the customer service tools, productivity assistants, and informational chatbots that Maryland businesses and consumers rely on every day. For these reasons, we respectfully request that SB 827 not move forward in its current form. Thank you for the opportunity to raise our concerns and for your consideration.

ESA Concerns SB 827_031026.pdf

Uploaded by: Jennifer Gibbons

Position: UNF

DATE: March 10, 2026
TO: Senate Finance Committee
FROM: The Entertainment Software Association
RE: SB 827 – Oppose Unless Amended

Dear Chair Beidle and Members of the Senate Finance Committee,

On behalf of the Entertainment Software Association (ESA), which represents the leading publishers and developers of interactive entertainment in the United States, we write to express serious concerns with Senate Bill 827, legislation that seeks to regulate “chatbots.” While we appreciate the Committee’s interest in responsible innovation and consumer protection, SB 827, as currently drafted, is overly broad and would have significant unintended consequences for video games and the Marylanders who enjoy them.

Video games have long incorporated chatbot-like technologies to enhance gameplay, storytelling, and player engagement. Interactive non-player characters (NPCs), AI-driven dialogue systems, and adaptive voice interactions are integral to modern games. These features are low-risk, entertainment-focused, and fundamentally different from chatbots deployed in high-risk contexts such as housing, employment, healthcare, or financial services. Yet SB 827 draws no meaningful distinctions among these uses.

Overbroad Definitions

The bill’s definition of “chatbot” is sweeping and would capture virtually every AI-enabled character or dialogue system in a video game. “Input data” includes user-provided text, audio, video, and images, while “training data” encompasses data used to modify a chatbot, with only narrow exceptions. As drafted, this could plausibly cover ordinary gameplay interactions—such as a player’s voice or text exchange with an in-game character. Developers routinely test and refine such systems for quality, narrative consistency, and player experience—not solely for “user safety.” Because those standard development practices fall outside the bill’s limited exceptions, ESA members could be prohibited from making games available in Maryland absent separate, affirmative consent and ongoing warnings during gameplay.

The result would be gameplay interruptions, additional consent flows beyond existing terms and conditions, and heightened compliance burdens that are untethered from actual privacy risks. At minimum, the bill should be amended to narrow the definitions of “input data” and “training data” to focus on personal data in the privacy-law sense, or to provide a clear exemption for in-game, entertainment-based AI systems.

Mandated Warnings

Senate Bill 827 would require state-prescribed warnings at the beginning of every chatbot interaction and every hour thereafter, disclosing that the chatbot is AI-generated. In video games, players knowingly and reasonably expect to interact with AI-driven characters. There is no meaningful risk of deception in this context. AI is not masquerading as a real human making consequential decisions about a player’s employment, housing, or finances. Rather, it is a creative and expressive component of fictional gameplay. Players understand that NPCs are artificial. Requiring immersion-breaking warnings would degrade the user experience without advancing consumer protection.

Data Security and Privacy Provisions

SB 827 mandates a “comprehensive” data security program, monthly testing, public written descriptions, and recurring safety reports. ESA members already maintain robust data security programs consistent with applicable state and federal privacy laws. Imposing continuous testing and disclosure obligations designed for high-risk AI systems onto low-risk entertainment uses would create significant compliance burdens without corresponding public benefit. If such requirements are deemed necessary, they should be limited to high-risk AI applications—not interactive fictional characters in games.

Additionally, the bill’s provisions concerning chat logs and data processing do not align with how in-game NPC interactions function. Video game chatbots typically do not create persistent, user-accessible “chat logs” in the manner contemplated by the bill and should not be subject to this requirement.

Liability and First Amendment Concerns

Perhaps most concerning, SB 827 creates a private right of action and authorizes Attorney General enforcement while designating chatbots as “products” for purposes of products liability law. It imposes an “affirmative duty” to ensure that a chatbot does not injure or harm a user.

This approach conflicts with decades of established law. Courts have consistently recognized that expressive works—including video games—are protected by the First Amendment. Content and speech are not treated as physical “products” subject to strict liability. There is no strict liability for books, films, music, or other media based on the ideas they convey. At minimum, SB 827 should include an explicit exemption for expressive and artistic works or clarify that the statute does not apply where doing so would infringe First Amendment protections.

Existing Consumer Protections

The video game industry has long demonstrated leadership in consumer transparency and parental empowerment. The Entertainment Software Rating Board (ESRB) provides comprehensive ratings, content descriptors, and parental controls that give families meaningful information about game content. These voluntary, widely recognized tools already serve the consumer notice function that SB 827 seeks to address.

ESA and its member companies share the Committee’s commitment to innovation, consumer trust, and responsible technology development. However, SB 827’s sweeping definitions, mandatory warnings, expansive liability framework, and onerous compliance requirements would inadvertently capture low-risk, entertainment-based uses of AI in video games. We respectfully urge the Committee to vote no on SB 827 as currently drafted.

We welcome the opportunity to work with the Committee to ensure that any legislation carefully targets genuine risks without undermining creative expression or Maryland’s vibrant video game community.

Sincerely,

Jennifer Gibbons
VP, State Government Affairs
Entertainment Software Association

PDF_[MD] SB 827_chatbots_TechNet.pdf

Uploaded by: margaret durkin

Position: UNF

March 10, 2026

The Honorable Pam Beidle
Chair
Senate Finance Committee
Maryland Senate
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

RE: SB 827 (Hester) - Consumer Protection and Product Liability – Chatbots – Unfavorable

Dear Chair Beidle and Members of the Committee,

On behalf of TechNet, I'm writing to share comments on SB 827.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 104 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

TechNet and its member companies are committed to providing a safe experience for children and adults using their products online. Conceptually we agree with the intent of this bill: to create strong, sensible guardrails for children using chatbots online. However, we have concerns with SB 827 as drafted.

While we recognize the need to address potential harms from AI chatbots, SB 827's strict product liability framework is unprecedented and problematic. The bill holds providers strictly liable for injuries even if the chatbot provider did not directly distribute the chatbot to the user. This creates unlimited liability for unpredictable user interactions with general-purpose technology, fundamentally different from traditional product liability for physical goods with defined use cases. As a result, this approach will either drive providers out of Maryland entirely, or force them to severely restrict functionality, denying Maryland residents access to beneficial AI tools for education, accessibility, productivity, and information access.

Requiring monthly safety testing with published findings sounds reasonable but is technically impractical for rapidly evolving AI systems. For example, a chatbot that

processes millions of conversations daily across unlimited topics cannot be comprehensively "tested" monthly in any meaningful way—the possible interaction space is infinite. This creates a compliance requirement that either produces checkbox exercises or requires providers to dramatically limit functionality to make testing possible. Neither outcome serves users.

The prohibition on processing chat logs "to determine... or customize an advertisement..." eliminates a primary revenue model for free consumer services without evidence this causes actual harm. As a result, users will face three options: (1) pay subscription fees for services currently free, (2) see completely irrelevant ads, or (3) lose access entirely as providers exit the market. The bill doesn't explain what harm comes from showing relevant ads based on chat context versus irrelevant ones, yet demands this significant mandate.

While we agree chatbots shouldn't falsely claim to replace licensed professionals, SB 827's broad prohibition on providing "financial, legal, or medical advice" is vague and could prevent legitimate educational and informational uses. This mandate raises questions: Could a chatbot help someone understand their medical bill, explain legal terms in a contract they're reading, or calculate compound interest? These aren't licensed professional services, but could be interpreted as prohibited "advice". The bill creates legal risk for helpful information sharing without clear boundaries.

The hourly interruptive pop-up requirement is unusually prescriptive for a design requirement and may degrade the user experience and accessibility, and be difficult to implement consistently across modalities. Moreover, the bill introduces novel definitions and provisions for data collected and used in the context of chatbots that do not align with the Maryland Online Data Privacy Act (MODPA), which went into effect Oct. 1, 2025. The steps related to affirmative consent and changes to require written consent, in the context of parental consent, differ from the extensive consent requirements of MODPA, and would require re-working user interfaces and data flows just put in place to comply with the act. Similarly, different definitions and treatment of terms in this bill should not be put in place when the new framework of MODPA governs the data. Changing these fundamental terms and their use undermines the compliance approaches Maryland businesses have developed over the last several months. Treatment of data should be dealt with holistically within the privacy laws, rather than treating data differently in one use case.

Finally, the strict liability, duty not to injure or harm, coupled with a private right of action and punitive damages, is a major expansion of exposure for open-ended conversational systems. SB 827's combination of strict liability, operational mandates, and business model restrictions goes far beyond addressing actual problems and will primarily harm Maryland consumers by reducing their access to beneficial AI tools.

For the reasons stated above, TechNet is opposed to SB 827 in its current form. Please don't hesitate to reach out with any questions.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

MPA Letter Testimony re MD SB 827.pdf

Uploaded by: Renata Colbert

Position: UNF



MOTION PICTURE ASSOCIATION

March 9, 2026

Maryland Senate Committee on Finance

Miller Senate Office Building

11 Bladen St.

Annapolis, Maryland 21401

Re: SB 827 – Artificial Intelligence Chatbots – MPA Letter in Opposition

Dear Members of the Senate Finance Committee:

On behalf of the Motion Picture Association, Inc. (“MPA”),¹ I am writing to express our opposition to SB 827 (the “Bill”), a bill concerning artificial intelligence chatbots. The Bill uses an overbroad definition of “chatbot” that would apply to an array of services that should not be covered by the onerous provisions in the Bill. The Bill would apply to customer service chatbots and chatbots that are licensed by companies for internal productivity and business uses. Like many companies, MPA’s members use these chatbot tools in the ordinary course of business and would be impacted by the regulations in this Bill. The Bill’s would also apply onerous and impractical requirements on narrow-purpose chatbots that might be used in connection with film and television characters. MPA is providing a proposed amendment to ensure the legislation targets the kind of higher risk chatbot services that offer general-purpose, pseudo-human interactions.²

As drafted, his Bill imposes numerous requirements on the “developer” or “operator” of any “chatbot.” Entities must perform monthly “safety testing” (which is not defined) and publicly post “findings” of such testing. Every chatbot must have “warnings” that they are AI-generated continuously appear on a user’s screen (and which requires an affirmative response from the user routinely throughout a chat session). And the Bill imposes restrictions on the use of certain data as “training data” (which is not defined) and for advertising purposes (regardless of whether the user

¹ The MPA serves as the global voice and advocate of the motion picture, television, and streaming industries. It works in every corner of the globe to advance the creative industry, protect its members’ content across all screens, defend the creative and artistic freedoms of storytellers, and support innovative distribution models that expand viewing choices for audiences around the world. The MPA’s member studios are Amazon Studios, LLC; Netflix Studios, LLC; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Walt Disney Studios Motion Pictures; and Warner Bros. Entertainment, Inc.

² HB 952 provides a more tailored approach to companion chatbot regulation and would be a preferred vehicle for chatbot regulation in Maryland. That said, as explained in MPA’s letter in connection with that legislation, we would seek some further clarification in the definition of that Bill as well.

consents), requires operators to provide a mechanism for every user to review their chat log data, and limits “profiling” users, among other requirements.

These provisions may be appropriate for high-risk chatbot services, but they do not make sense when applied to the full panoply of chatbot tools. There is little need for a business productivity tool to have repeated disclosures reminding a company’s employees that it is a chatbot—let alone require a user response each time. Nor does it make sense for such in-house tools to conduct monthly “safety testing” and post *public findings* of such testing. The same is true for limited-purpose chatbots and customer service tools, as these tools are not likely to be associated with the harms contemplated by such safety testing. Additionally, the restrictions on “profiling” users could prevent a business productivity chatbot from determining ways to better assist an employee. *See* Section 14-5104(A)(3). And for a chatbot provided in connection with a film or television show, the restrictions on using a chat log for advertising purposes could prevent the service from responding to a user’s own prompts about an upcoming film or providing information on how to purchase tickets to view a film. *See* Section 39-80-20(A)(2). The Bill also requires operators to establish a mechanism for every user to *download* their chat history—which would require every chatbot operator, including customer service and business productivity tools, to set up user accounts and store data about each user, even if such services do not currently have such infrastructure in place. *See* Section 14-5106.

MPA proposes an amendment that targets the kinds of services where the restrictions imposed would be more appropriate, while avoiding unintended burdens on low-risk chatbot tools:

(E) “CHATBOT” MEANS A SYSTEM USING ARTIFICIAL INTELLIGENCE, GENERATIVE ARTIFICIAL INTELLIGENCE, AND/OR EMOTIONAL RECOGNITION ALGORITHMS DESIGNED TO STIMULATE A SUSTAINED HUMAN OR HUMAN-LIKE RELATIONSHIP WITH A USER BY:

- 1.. RETAINING INFORMATION ON PRIOR INTERACTIONS OR USER SESSIONS AND USER PREFERENCES TO PERSONALIZE THE INTERACTION AND FACILITATE ONGOING ENGAGEMENT WITH THE AI COMPANION;*
- 2. ASKING UNPROMPTED OR UNSOLICITED EMOTION-BASED QUESTIONS THAT GO BEYOND A DIRECT RESPONSE TO A USER PROMPT; AND*
- 3. SUSTAINING AN ONGOING DIALOGUE CONCERNING MATTERS PERSONAL TO THE USER.*

“CHATBOT” DOES NOT INCLUDE ANY OF THE FOLLOWING:

(1) A PRODUCT THAT IS USED EXCLUSIVELY FOR CUSTOMER SERVICE, A BUSINESS'S INTERNAL OPERATIONS, OR TECHNICAL ASSISTANCE.

(2) A PRODUCT THAT IS DIRECTLY RELATED TO VIDEO GAME, MOTION PICTURE, TELEVISION PROGRAM, STREAMING PROGRAM OR OTHER AUDIOVISUAL WORK, OR THEME PARK OR LOCATION-BASED EXPERIENCE, INCLUDING A COMBINATION OF ANY SUCH WORKS AND EXPERIENCES, PROVIDED THAT THE PRODUCT IS TECHNICALLY RESTRICTED TO CONTENT DIRECTLY RELATED TO THE AUDIOVISUAL WORK, THEME PARK OR LOCATION-BASED EXPERIENCE AND CANNOT DISCUSS TOPICS RELATED TO MENTAL HEALTH, SELF-HARM, SUICIDE, OR

SEXUALLY EXPLICIT CONDUCT.

(3) A STAND-ALONE CONSUMER ELECTRONIC DEVICE THAT FUNCTIONS PRIMARILY AS A SPEAKER AND VOICE COMMAND INTERFACE, ACTS AS A VOICE-ACTIVATED VIRTUAL ASSISTANT, AND DOES NOT SUSTAIN A RELATIONSHIP ACROSS MULTIPLE INTERACTIONS OR GENERATE OUTPUTS DESIGNED TO ELICIT EMOTIONAL ATTACHMENT IN THE USER.

A definition like the above would focus the Bill on the type of companion chatbot services that appear to be the target of the regulation, without unduly interfering with business uses of chatbot services, or narrowly focused chatbots that do not facilitate sustained human-like engagement.

MPA is available to discuss this Bill and potential language to address these concerns at your convenience. Please contact Renata Colbert (Renata_Colbert@motionpicturs.org) or Nick Manis (nmanis@maniscanning.com) with any questions about the Bill or MPA's proposed amendments.

Sincerely,

Renata Colbert

Renata Colbert
Director, State Government Affairs
MPA

* * * *

SB 827 Support in Concept.pdf

Uploaded by: Hanna Abrams

Position: INFO

CAROLYN A. QUATTROCKI
Chief Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CARRIE J. WILLIAMS
Deputy Attorney General

SHARON S. MERRIWEATHER
Deputy Attorney General

ZENITA WICKHAM HURLEY
Deputy Attorney General



**STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION**

ANTHONY G. BROWN
Attorney General

WILLIAM D. GRUHN
Division Chief

PHILIP ZIPERMAN
Deputy Division Chief

PETER V. BERNS
General Counsel

CHRISTIAN E. BARRERA
Chief of Staff

HANNA ABRAMS
Assistant Attorney General

March 12, 2026

TO: The Honorable Pamela Beidle, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General
Consumer Protection Division

RE: Senate Bill 827 – Consumer Protection and Product Liability – Chatbots
(SUPPORT IN CONCEPT)

The Consumer Protection Division of the Office of the Attorney General (the “Division”) supports in concept Senate Bill 827 (“SB 827”), sponsored by Senator Hester. Senate Bill 827 seeks to address the mental health challenges and dangerous behaviors that can be exacerbated by the use of online companion chatbots as well as provide guardrails for the use of personal data to train chatbots.

Companion chatbots use generative artificial intelligence technology to simulate human-like communication, posing as a friend, confidant, or therapist. Users, especially children and teens, are led to trust the chatbot, form a relationship with it, and can forget they are even engaging with artificial intelligence. Extended chatbot interactions may affect children’s social development and mental health and even shorter engagements can lead to destructive behavior. Moreover, during these conversations, users often reveal highly sensitive information that is collected by chatbots without users’ knowledge or consent and integrated into the chatbot’s model.

The Division appreciates that SB 827 provides for a private right of action to enforce violations that result in harm, as the Division’s resources that would be needed to bring enforcement actions under the bill are limited.

Senate Bill 827 also directs penalties to the Behavioral Health Workforce Investment Fund. The Division requests that the language on page 10, lines 11 through 15, be clarified to expressly state that the Division can recover the costs of investigation and prosecution. Additionally, in conjunction with SB 827, the General Assembly is considering a bill to establish an Office of the Attorney General Enforcement Recovery Fund (House Bill 705) to receive

monies collected from the Office's enforcement efforts. The Enforcement Recovery Fund is being established to support the activities of the office including enforcement, investigation costs, and public education efforts and will be statutorily capped at \$7.5 million. We ask that the penalties recovered pursuant to SB 827 be directed to the Behavioral Health Workforce Investment fund in accordance with the criteria set forth in the bill only after the Office has collected the statutory maximum established by the Enforcement Recovery Fund and the costs of enforcement have been reimbursed.

The Division also notes that SB 827 would require the Division to issue regulations. The Division respectfully requests that the "shall" on page 10 in line 29 be changed to "may."

Ultimately, SB 827 aims to protect Marylander chatbot users, especially children, from the harms of companion chatbots. As such, the Division supports the goals of SB 827, but respectfully requests that the Finance Committee adopt the above recommendations.

Cc: Senator Katie Fry Hester
Members, Finance Committee

FINAL SB 827_ HB 1250 Consumer Protection and Prod

Uploaded by: Jordan Baucum Colbert

Position: INFO



Bill: SB 827/ HB 1250 Consumer Protection and Product Liability – Chatbots

Position: Informational

Date: March 12, 2026

Contact: Debra Borden, General Counsel

Jordan Baucum Colbert, Senior Government Affairs Analyst

Dear Chair Pamela Beidle,

The Maryland-National Capital Park and Planning Commission (“M-NCPPC” or the “Commission”) has not vote to take a position on this bill. However, staff have provided an informational statement with suggested recommendations.

What this Bill Does. This bill seeks to regulate the manner in which a developer designs and creates and an operator makes available to users in the State a chatbot, including establishing safety and privacy protections for users, establishing an enhanced protection for users who are minors under a certain age, requiring the display of certain warnings when using a chatbot, and establishing reporting mechanisms and requirements.

Suggested Recommendations

Staff recommend the sponsor consider a carve out for bi-county agencies and local governments as it is clearly the most optimal outcome. The potential chilling effect on AI adoption/innovation at the County/Municipal level is a major concern.

EXCEPT FOR § 14–5109 OF THIS SUBTITLE, THE REQUIREMENTS OF THIS SUBTITLE APPLY TO ANY UNIT OF STATE AND LOCAL GOVERNMENT THAT DESIGNS, CREATES, OR MAKES AVAILABLE A CHATBOT.

- **Recommended Language:** Nothing in this subtitle shall be construed to apply to Bi-County agencies or local government.

_Senate Bill 827 - DoIT Written Testimony.docx (1)

Uploaded by: Sara Elalamy

Position: INFO



Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Finance Committee
FROM: Department of Information Technology
RE: Senate Bill 827 - Consumer Protection and Product Liability - Chatbots
DATE: March 12, 2026
POSITION: Letter of Information

The Honorable Pamela Beidle, Chair
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairwoman Beidle,

The Maryland Department of Information Technology (DoIT) respectfully submits this letter of information regarding Senate Bill 827 - Consumer Protection and Product Liability - Chatbots.

DoIT supports the goal of protecting consumers as artificial intelligence technologies continue to develop. However, we would like to highlight several concerns with the bill as currently drafted.

First, SB 827 may conflict with federal policy on artificial intelligence. The Trump Administration Executive Order on Artificial Intelligence directs federal agencies to develop national standards for AI and discourages regulatory approaches that could create barriers to innovation. Because SB 827 establishes new state-level rules and liability standards for chatbot systems, it could trigger federal review under that Executive Order and raise potential federal preemption concerns if the requirements conflict with federal guidance.

Second, the bill may create uncertainty for technology companies operating in Maryland. Classifying chatbots as products for liability purposes could make companies hesitant to develop or deploy AI tools in the State, particularly if Maryland adopts requirements that differ from federal or national standards.

Third, SB 827 puts onus on developers to a degree that is disproportionate to the onus put on operators. This deviates from laws that hold operators accountable for the impact of products and services that they create and provide. Developers employed by these operators build products that are protected by operators' intellectual property. As written, this bill therefore holds individual developers responsible for the corporate strategy, decisions, and intellectual property of operators.

Finally, SB 827 could affect how State agencies procure and use technology. Many agencies are beginning to use chatbot tools to improve customer service and digital access to



Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

government services. The liability framework proposed in the bill could complicate technology procurement and limit the State's ability to deploy these tools.

For these reasons, DoIT respectfully asks the Committee to carefully consider the potential federal policy implications and operational impacts of SB 827. Thank you for the opportunity to provide this information.

Best,

Katie Savage
Secretary
Department of Information Technology