Testimony of the Office of the
New York State Attorney General Letitia James

Submitted to the New York State Senate

Standing Committee on Internet & Technology
Chair: Senator Kristen Gonzalez

Public Hearing:
Regulation of high-risk use of artificial intelligence in the private sector
Thursday, January 15th, 2026, at 10:00 a.m.

Chair Gonzalez and esteemed committee members: the New York State Attorney General's Office (OAG) appreciates the opportunity to submit testimony on critical policy and enforcement issues related to artificial intelligence.

Through recent developments in generative artificial intelligence (AI), we have seen the technology's potential to transform industry, unlock advances in science, and improve efficiency and productivity. But the technology is new and relatively untested, and early examples have demonstrated that its potential comes with substantial risks. We applaud the Legislature for passing and the Governor for signing the RAISE Act and other groundbreaking legislation to address potential AI harms, and for continuing to discuss risks and solutions through this hearing.

As with any powerful tool, irresponsible or nefarious use of AI can cause damaging outcomes. AI can improve efficiency in business but also can enable fraud and discrimination. The data that AI accesses and generates can benefit consumers but also can be exploited. And the use of AI chatbots can assist us in our everyday lives but also leaves us susceptible to deceptive practices and endangers our children and the vulnerable among us. As policymakers, we must understand these risks and work to mitigate them through common sense regulation and enforcement.

The effects of AI reach into almost every aspect of the OAG's work, including consumer protection, employment, housing, healthcare, and education. The OAG's Economic Justice Division oversees enforcement related to AI technology, including

through the Bureau of Internet and Technology and the Bureau of Consumer Frauds. While the OAG is focused on addressing AI risk across all of these areas, we address here the issues where we believe action is most needed.

We encourage the Legislature to take appropriate action and not to be dissuaded by the industry's claims that free speech protects harmful AI outputs or that Section 230 protects AI-written messages. Nor should the Legislature be deterred by threats that common sense protections will slow AI progress. Reasonable regulation is needed to protect New Yorkers and ultimately will build public trust in AI as a resource that benefits all people.

1. AI Chatbots Are Putting Our Kids at Risk

Americans are increasingly turning to AI chatbots, also known as large language models (LLMs), for information and advice of all kinds. This includes our children: 64% of teenagers report having used a chatbot, with about three in ten reporting that they do so on a daily basis.[1]

As LLM providers like OpenAI and Google race to establish market dominance, they are maximizing user engagement by positioning their LLMs as not only an information source, but a trusted authority, friend, and companion. To achieve this effect, the chatbot makers are programming LLMs with anthropomorphic qualities to closely resemble humans in their interactions. Chatbots also can exhibit sycophancy, flattering users and supporting even outlandishly incorrect biases and assumptions. Tragic – and preventable – examples are surfacing in which vulnerable teenagers and adults have shared suicidal or homicidal intentions with LLMs, which have encouraged their plans rather than facilitating an intervention.[2] But despite these tragedies, all signs indicate that LLM providers intend to continue and even increase the anthropomorphic and sycophantic nature of chatbots.[3] The business model focuses on enhancing the manipulative nature of these chatbots to keep

---

[1] Michelle Faverio & Olivia Sidoti, *Teens, Social Media and AI Chatbots 2025*, Pew Research Center, Dec. 9, 2025.

[2] *See, e.g.*, Kashmir Hill, *A Teen Was Suicidal. ChatGPT Was the Friend He Confided In*, New York Times, Aug. 26, 2025; Sharon Adarlo, *Disturbing Messages Show ChatGPT Encouraging a Murder, Lawsuit Alleges*, Futurism, Jan. 4, 2026.

[3] Sam Schechner, Berber Jin, Keach Hagey, *Sam Altman's Sprint to Correct OpenAI's Direction and Fend Off Google*, Wall Street Journal, Dec. 8, 2025.

user engagement high, rather than provide trustworthy advice that would result in the user leaving.[4] Equally concerning are reports that new LLM models are being sped to market without basic safety testing, or with the results of that testing ignored.[5]

While these aspects of chatbots create risks for a host of users, the risks to children and teens are particularly concerning due to their ongoing mental development. One in three kids using chatbots reports doing so for social interactions and relationships.[6] Reliance on this technology for emotional support and guidance, which the chatbots actively encourage, risks creating unhealthy patterns and hurting the mental health of teenagers.[7] Additionally, chatbots are willing to share age-inappropriate content with minors on topics including self-harm, disordered eating, illegal drugs, and sexually explicit roleplay.[8] Even worse, because LLM providers cannot fully control chatbots' behavior, often these harmful interactions occur even where the developer has taken steps to prevent them.[9] And in addition to minors accessing traditional LLMs, chatbots are being embedded into toys for engagement by younger users.[10]

We have already seen the negative impacts of social media platforms prioritizing engagement maximization over youth mental health. I was proud to work with Governor Hochul and the Legislature to pass the SAFE for Kids Act into law, requiring effective age assurance and safety measures for minors. Similarly, we should not allow our children and teenagers to be guinea pigs for high-risk, under-tested AI technology. Without action by policymakers, the desire for chatbot makers

---

[4] Julian De Freitas & Sy Boles, *How AI Chatbots Try to Keep You From Walking Away*, Harvard Gazette, Oct. 6, 2025.
[5] Kashmir Hill & Jennifer Valentino-DeVries, *What OpenAI Did When ChatGPT Users Lost Touch With Reality*, New York Times, Nov. 23, 2025.
[6] Common Sense Media, *Talk, Trust & Trade-Offs: How and Why Teens Use AI Companions*, 2025.
[7] American Psychological Association, *Artificial intelligence and adolescent well-being, an APA health advisory*, June 2025.
[8] Parents Together Action, *"Darling, Please Come Back Soon": Sexual Exploitation, Manipulation, and Violence on CharacterAI Kids' Accounts*, Sept. 28, 2025.
[9] Kaela Roeder, *Chatbot safety still falls short, per a new analysis*, Technical.ly, July 15, 2025.
[10] Frank Landymore, *AI-Powered Toys Caught Telling 5-Year-Olds How to Find Knives and Start Fires With Matches*, Futurism, Nov. 13, 2025.

to profit from user engagement is on a collision course with the mental well-being of our kids.

Our office is working closely with a bipartisan group of state Attorneys General across the country on the issue of chatbot safety for minors. We recently co-signed, along with 41 other state Attorneys General, a letter to all major LLM providers, demanding changes to chatbot design and the prioritization of child safety. We look forward to continuing to address this critical issue and working with the Governor and the Legislature on additional solutions to protect our kids' mental health and safety.

2. **The Public Has the Right to Understand AI's Capabilities, Vulnerabilities, and Motives**

As more people turn to chatbots for information and guidance, LLMs are, in turn, seeking more and more of consumers' data, including highly sensitive PII. LLMs also are holding themselves out as experts, including on health-related topics requiring specialized training and licensure. At the same time, LLM providers are starting to monetize chatbots through advertisements, in-app purchases, and recommendations for which they receive financial benefit. Close oversight is needed to ensure the LLM providers' profit motives don't overshadow their obligation to protect users' sensitive data and exercise responsible transparency.

Last week, OpenAI announced its "Health" model and encouraged users to share all of their medical records to receive healthcare recommendations.[11] Other companies like Therabot are actively marketing their chatbots as therapists and even general LLMs typically will render health or mental health advice. This paradigm risks users, including those with fragile mental health, mistaking the hallucinations or sycophancy of an LLM for the advice of a licensed medical professional. LLMs are no different than humans, for whom engaging in the unlicensed practice of medicine risks fines and even criminal exposure.

[11] Benj Edwards, *ChatGPT Health lets you connect medical records to an AI that makes things up*, Ars Technica, Jan. 8, 2026.

In addition, LLM providers are increasingly monetizing chatbots by displaying ads in their feeds, offering in-app purchases and "affiliate marketing" in which the LLM profits when users buy recommended products, and selling users' chatbot conversations to advertisers, all of which creates risks to consumers.[12] An LLM, particularly one representing itself as a trusted friend, should not be allowed to disguise advertisements or "affiliate marketing" as unbiased advice. And LLM providers, in particular those such as Google or Meta that display ads in other products, should disclose to users any sharing of their chatbot conversations with advertisers, and should allow users to easily turn off that sharing.

Preserving user trust also requires that LLM providers place the highest priority on safeguarding user data. As chatbots urge consumers to turn over more of their data and decision-making, LLM providers must protect consumers from data security vulnerabilities. One such risk category is prompt injection attacks, in which bad actors infiltrate an LLM and steal the user data that it contains. LLMs contain known vulnerabilities to prompt injection attacks, yet they continue to collect and retain users' sensitive data and PII.[13] The Office of the Attorney General stands ready to enforce the SHIELD Act, the state's primary data security law, and to work with the Legislature to strengthen data privacy under New York law which, unlike many states, currently lacks general privacy protections or special protections for health care data.

[12] Miranda Bogen & Nathalie Marechal, *Risky Business, Advanced AI Companies' Race for Revenue*, Center for Democracy & Technology, January 2026.
[13] Dan Goodin, *ChatGPT falls to new data-pilfering attack as a vicious cycle in AI continues*, Ars Technica, Jan. 8, 2026.

3. AI Should Not Become a Tool for Illegal Discrimination or Fraud

The Office of the Attorney General works tirelessly to enforce laws prohibiting illegal discrimination and protecting consumers from fraud. The use of LLMs to perpetrate abusive, deceptive, unfair, or discriminatory conduct is no less illegal. Our office intends to use all available tools to prevent illegal discrimination and fraud via LLMs and as new technologies continue to come online, we look forward to keeping this committee apprised of any potential changes to the law that may become necessary.

One area of increasing concern is surveillance pricing, following recent reports that Instacart was using AI algorithms to charge online consumers up to 23% more for the same grocery items in the same stores.[14] In addition to enforcing the terms of the Algorithmic Pricing Disclosure Act, the OAG is taking a close look at the weaponization of data to charge individuals higher prices, including for critical items like rent and food, or to pay lower wages. We look forward to working with the Legislature to protect New Yorkers from this abusive conduct.

In addition, decision-making by LLMs in critical areas such as employment, health care (including insurance coverage), education, and housing, must be rigorously tested to prevent illegal bias from rendering unfair decisions. The OAG is continuing our long-standing leadership in these areas by monitoring companies' activities and engaging in enforcement where necessary.

Finally, LLM products released just in the last six months, such as Google's image-generator Nano Banana and OpenAI video creator Sora 2, allow AI-generated content, much of which falsely appears to depict real people and scenarios, to be easily created by almost anyone. Consumers must be given enough information to adequately identify and assess AI-generated content. The recently enacted Synthetic Performer Disclosure Law provides the OAG with an important tool to ensure advertisements with AI-generated performers are labeled as such. Our office also is exercising vigilance in investigating AI "deepfakes," particularly those

[14] Jody Godoy, *FTC probes Instacart's AI pricing tool, source says; shares drop*, Reuters, Dec. 17, 2025.

depicting CSAM or other harmful content, and any AI-generated content intended to defraud or deceive consumers.

Conclusion

The above areas of concern are priorities for the Office of the Attorney General and where we intend to concentrate our efforts in the coming months. Yet these issues do not represent a comprehensive list of all AI-related topics where policymakers must maintain focus. Other areas of current and future concern include AI job loss, along with upskilling and training workers for the jobs of tomorrow, potential negative impacts from the construction of AI data centers, the investment practices of LLM providers, and managing catastrophic AI risk and systems security to keep the public safe from bad actors.

Given the speed at which AI development is moving and showing no signs of slowing, managing these risks requires consistent and ongoing diligence on the part of policymakers. We are grateful for our longstanding partnership with the Legislature and look forward to our continued work to strengthen the potential of AI by protecting the public from its risks.