The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org

March 11, 2024

Joel Christie
Acting Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, N.W.
Suite 5610 (Annex E)
Washington, D.C. 20580

Submitted electronically via www.regulations.gov

Re: COPPA Rule Review, Project No. P195404

Dear Secretary Christie,

On behalf of The Leadership Conference on Civil and Human Rights (The Leadership Conference) and its Center for Civil Rights and Technology, and the undersigned organizations, we write in response to the Federal Trade Commission's (FTC) Notice of Proposed Rulemaking (NPRM), 89 FR 2034, January 11, 2024. In the proposed rule, the FTC puts forth amendments to the Children's Online Privacy Protection Act (COPPA) intended to respond to emerging technologies and online practices.[1] We agree that such action is needed to strengthen protection of children by safeguarding the personal information collected and subsequently used to target them. The way data is being used today means that it is imperative that the commission apply COPPA where data drives new technologies. For COPPA to be effective and achieve its purpose, it must protect children in a world of data-driven artificial intelligence (AI), and the proposed update to COPPA must reflect the widespread adoption and use of emerging technologies.

The Leadership Conference is a coalition charged by its diverse membership of more than 240 national organizations to promote and protect the civil and human rights of all persons in the United States. Through its membership, its Center for Civil Rights and Technology, and its Media and Telecommunications Task Force, The Leadership Conference works to ensure that civil and human rights, equal opportunity, and democratic participation are at the center of communication, public education, and technology policy debates. We have been actively engaged in policy development to ensure civil rights are at the center of the development and use of new technologies, especially where those technologies are rights and safety impacting.

[1] The Children's Online Privacy Protection Act of 1998, 15 U.S.C. 91.

The Leadership Conference

The FTC should be commended for its continued commitment to protecting our children's privacy. Its update to the COPPA rule is right to be informed by its experience, new learnings, and changes in the marketplace. We appreciate the effort to improve aspects of the COPPA rule in this proceeding. However, the FTC must also take into account that we are now living in an era of data-driven AI. AI has become ubiquitous, and in order to protect children's privacy today, the FTC's update to COPPA must reflect that children's data may end up in AI systems — and it must move to implement needed safeguards.

Congress intended COPPA to protect children against harm caused by the collection and use of their data — and today that means that the FTC's update to COPPA must include consideration of AI.

When Congress passed COPPA in 1998, it directed the FTC to promulgate rules "to prohibit unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the Internet."[2] Among the enhanced privacy provisions the FTC is proposing in the rule is requiring verifiable parental opt-in consent for targeted advertising, data retention limits, COPPA Safe Harbor accountability, and codifying FTC education technology guidelines. These are important developments, and the FTC should be commended for its work to further privacy protections for children. However, to begin to more fully safeguard children's privacy, the FTC's proposal must be further refined to include safeguards related to the use of AI.

With the widespread use of artificial intelligence and its reliance on massive amounts of data,[3] the need to protect children from unfair and deceptive acts is greater than ever. AI technology collects massive amounts of data from people, including children, and stores it in databases that can be accessed and used for various purposes.[4] The FTC should look to further evolve its COPPA rule to ensure that data used in AI systems does not lead to children being harmed.

The commission must include safeguards where children's data are used in AI systems.

As a 2022 Time magazine article noted, "new technologies like digital assistants already fulfill functions traditionally served by the adults who take care of children. These functions include—but aren't limited to—teaching academic subjects, reading stories, helping with homework, singing lullabies, and answering all sorts of questions. Digital assistants are already morphing into a variety of lovable personal robots, marketed today as able to act 'like a friend,' develop 'young minds through education,' 'be a child's mentor,' or both 'nurture their emotional and interaction skills' and 'build healthy relationships.'"[5] Children's information, including sensitive biometric data, is being captured and processed by AI-driven

[2] Federal Trade Commission, Notice of Proposed Rulemaking, 64 Fed.Reg. 22750 (Apr. 27, 1999).
[3] Rohit Sehgal, "AI Needs Data More Than Data Need AI," Forbes (Oct 5, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/10/05/ai-needs-data-more-than-data-needs-ai/?sh=493486453ed0.
[4] Rachel Achieng, "AI & Children: Privacy, Trust, and Safety in the Digital Age," Center for Intellectual Property and Information Technology Law, Strathmore University, (Mar. 29 2023), https://cipit.strathmore.edu/ai-children-privacy-trust-and-safety-in-the-digital-age/.
[5] Susan Linn, "How AI-Powered Tech Can Harm Children," Time Magazine (Oct. 21, 2022), https://time.com/6216722/how-ai-tech-harms-children/.

devices like virtual assistants and smart toys.[6] Those applications could ultimately be harmful if the underlying AI systems, or the AI systems that are using the data collected, are biased. We cannot lose sight of the fact that the AI systems noted above are fueled by data collected from children.

In addition to posing a threat to their privacy, there are also concerns over the use of children's data and possible discrimination, bias, and unfair treatment.[7] A report from the World Economic Forum noted that "Younger generations are growing up interacting with artificial intelligence (AI) algorithms, yet little attention is paid to the impact of AI and related technologies on children" — further recognizing the risk to their privacy and safety and the need to prioritize their rights and well-being when it comes to AI.

By providing safeguards for the collection and use of children's data, the FTC can protect them from harm. But the FTC must consider the use of data in AI systems and ensure that parents are fully informed about the ways in which the data will be used — and, if in an AI system, what guardrails are put in place including assessments and testing for bias and discrimination. At a minimum, parents must have this information in order for their consent for data collection and use to be meaningful.

There are ways to protect data in the era of AI that should inform the FTC's rulemaking.

We have been clear on the elements that need to be put in place for data in today's AI environment, which are also relevant when it comes to protections related to the collection and use of children's data:

- *Civil rights protections:* With data-driven AI systems becoming more ubiquitous, those systems should not result in discriminatory outcomes or exacerbate existing biases.
- *Privacy protections:* The law should require companies to minimize the data they collect; define permissible and impermissible purposes for collecting, sharing, and using personal data; prohibit discriminatory uses of personal data; and provide for algorithmic transparency and fairness in decision-making.

Given the relationship between data and AI, we have called for strong protections in federal privacy legislation. Those protections are appropriate in considering what is needed to ensure that children do not face unfairness or deception in the collection and use of their data:

- *Applying protections to the digital age:* Prohibit the use of personal data to discriminate based on protected characteristics. This will address data practices and automated decision-making systems that have led to discrimination and which have negatively impacted communities of color.
- *Prohibiting algorithmic bias:* Prohibit algorithms from reproducing patterns of discrimination.
- *Requiring companies to perform impact assessments:* Require companies to identify biases and mitigate harms through impact assessments.
- *Requiring algorithms to be audited for bias*: Require companies to evaluate their algorithms at the design phase, which will help identify potential discriminatory impacts before they are deployed.

[6] Natasa Perucica, "Our Children are Growing Up with AI: Here's What You Need to Know," World Economic Forum (Jan. 28 2022), https://www.weforum.org/agenda/2022/01/artificial-intelligence-children-technology/.
[7] *Id.*

Given the amount of data needed to drive AI, broader privacy protections are warranted.

This rulemaking highlights the need for broader privacy protections. To that end, the commission should move forward with its Commercial Surveillance Rulemaking.[8] As we said in our comments, such protections are imperative given the ubiquitous use of AI and the massive collection of data that is occurring.

As we noted in our comments, in 2014, a coalition of civil rights and media justice groups released "Civil Rights Principles for the Era of Big Data" calling on the U.S. government and businesses to respect and promote equal opportunity and equal justice in the development and use of data-driven technologies. These principles, along with the Obama White House's subsequent reports on big data, highlighted the need for rules of the road for the private and public institutions whose decisions can protect or deny civil and human rights.

Today, while the terminology has shifted from "big data" to "AI" and "biometrics," the issues remain the same and the threats that technology can pose to civil rights have only grown. Recognizing this increased urgency, on October 21, 2020, The Leadership Conference joined dozens of leading civil rights and technology advocacy organizations in releasing updated Civil Rights Principles for the Era of Big Data. Of relevance to this inquiry, the principles propose a set of civil rights protections, including:

- *Ending High-Tech Profiling.* Surveillance technologies are empowering governments and companies to collect and analyze vast amounts of information about people. Too often, these tools are deployed without proper safeguards or are themselves biased. In some cases, surveillance technologies should simply never be deployed. In other cases, clear limitations and robust auditing mechanisms are needed to ensure that these tools are used in a responsible and equitable way. Law should hold both the government and private actors accountable for abuses.
- *Ensuring Justice in Automated Decisions.* Statistical technologies, including machine learning, are informing important decisions in areas such as employment, health, education, lending, housing, immigration, and the criminal-legal system. Decision-making technologies too often replicate and amplify patterns of discrimination in society. These tools must be judged not only by their design but also, even primarily, by their impact — especially on communities who have been historically marginalized. Transparency and oversight are imperative to ensuring that these systems promote just and equitable outcomes, and in many cases the best outcome is to not use automated tools in high-stakes decisions at all.
- *Preserving Constitutional Principles.* Enforcement of constitutional principles such as equal protection and due process must keep pace with government use of technology. Search warrant requirements and other limitations on surveillance and policing are critical to protecting fundamental civil rights and civil liberties, especially for communities who have been historically marginalized and subject to disproportionate government surveillance. Moreover, governments

[8] Trade Regulation Rule on Commercial Surveillance, Federal Trade Commission, Proposed Rule, 87 Fed.Reg. 51299 (Aug. 22 2022) (*available at* https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security).

should not compel companies to build technologies that undermine basic rights, including freedom of expression, privacy, and freedom of association.

- *Ensuring that Technology Serves People Historically Subject to Discrimination.* Technology should not merely avoid harm, but actively make people's lives better. Governments, companies, and individuals who design and deploy technology should strive to mitigate societal inequities. This includes improving access to the internet and addressing biases in data and decision-making. Technologies should be deployed in close consultation with the most affected communities, especially those who have historically suffered the harms of discrimination.
- *Defining Responsible Use of Personal Information and Enhancing Individual Rights.* Corporations have pervasive access to people's personal data, which can lead to discriminatory, predatory, and unsafe practices. Personal data collected by companies also often end up in the hands of the government, either through the direct sale of personal data or through data-driven systems purpose-built for the government. Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help prevent these harms.
- *Making Systems Transparent and Accountable.* Governments and corporations must provide people with clear, concise, and easily accessible information on what data they collect and how it is used. This information can help equip advocates and individuals with the information to ensure that technologies are used in equitable and just ways. Any technology that has a consequential impact on people's lives should be deployed with a comprehensive, accessible, and fair appeals process with robust mechanisms for enforcement, and governments and corporations must be accountable for any misuse of technology or data. When careful examination reveals that a new, invasive technology poses threats to civil rights and civil liberties, such technology should not be used under any circumstance.

As we said in our comments on commercial surveillance, which are also applicable here, by establishing rules of the road for privacy and civil rights, the commission can empower communities of color, open doors for underserved populations, and hold companies accountable for the data they collect and use. Privacy rights are civil rights, even for our children who are often among the most vulnerable. The commission, in this rulemaking, has the opportunity to ensure that those rights are upheld.

The FTC should hold entities using AI accountable for their collection and use of data from children, and existing actions should provide a roadmap for reasonable requirements.

As we have advocated, it is critical to center equity and civil rights in technology policy to address the impact of artificial intelligence technology on people's rights and opportunities. That is equally important for technology that impacts our children. The commission has the opportunity to take action as it considers this rulemaking.

The civil rights impact of AI systems — systems that rely on data, including data from children — represent an urgent set of issues that require sustained attention, investigation, and action. We appreciate the commission's work on these issues and urge it to bring that same level of scrutiny to the collection and use of children's data.

The FTC's recent order requiring Rite Aid to implement comprehensive safeguards to prevent harm when deploying automated systems serves as a model for ways to address potential harms to children caused by collection and use of their data by an AI system.[9] Like the requirements in the order, entities collecting and using data from children — even in AI systems — should be required to implement comprehensive safeguards to prevent harm, and they should be required to discontinue using any such technology if it cannot control potential risks.

The FTC's complaint includes specific actions that Rite Aid should have taken. Those actions serve as a roadmap for what entities using AI systems should do:

- Consider and mitigate potential risks.
- Test, assess, measure, document, or inquire about the accuracy of the AI system — *before deploying it.*
- Ensure the veracity of the data being used.
- Monitor or test the accuracy of the technology after deployment.
- Train employees tasked with operating the AI system.

Those measures will help ensure that children are protected from unfairness when their data are used in AI systems.

Conclusion

We appreciate the opportunity to comment on the proposed rule. To fully protect children where their data are being collected, the rule must consider where the data are then used in an AI system. In those instances, it is imperative that parents be fully informed and that there are assurances that the AI system will not result in unfairness or deception. It is only then that they can make meaningful consent choices about their children's data.

Please direct any questions about these comments to Koutstubh "K.J." Bagchi, vice president of the Center for Civil Rights and Technology at The Leadership Conference on Civil and Human Rights, at bagchi@civilrights.org, or Frank Torres, civil rights and technology fellow of the Center for Civil Rights and Technology at The Leadership Conference on Civil and Human Rights, at torres@civilrights.org.

[9] "Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards," Federal Trade Commission, (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

Sincerely,

The Leadership Conference on Civil and Human Rights
Access Now
Center for American Progress
Japanese American Citizens League
National Council of Asian Pacific Americans (NCAPA)
National Hispanic Media Coalition