Testimony before Subcommittee on Innovation, Data, and Commerce
United States House of Representatives

April 17, 2024

Kara Frederick
Director, Tech Policy Center
The Heritage Foundation

Chairman Bilirakis, Vice Chair Walberg, and Ranking Member Schakowsky, thank you for the opportunity to testify. My name is Kara Frederick and I am the Director of Tech Policy at The Heritage Foundation. My perspective today is informed by my current policy research, as well as my time as a practitioner in the U.S. Intelligence Community, my work at a Big Tech company in Menlo Park, California, and—most importantly—my role as a mother. The views I express in this testimony are my own and should not be construed as an official position of The Heritage Foundation.[1]

I'll begin with a few observations on both privacy and the impact of social media on young Americans. I hope to conclude with solutions that address the exploitation of the American user and contend with the noxious practices of social media companies, especially when it comes to children.

PRIVACY ABUSES

Americans should be in control of their own data. From Google reportedly tracking its users' "private" internet use to IBM grabbing millions of unwitting citizens' images from a photo hosting site to train its facial recognition algorithms, privacy abuses are legion. Risks of continued abuse include data security vulnerabilities to hacks and leaks, the outsourcing of government surveillance to unaccountable private companies, and the potential integration of disparate data sets with other personally identifiable information through the expansion of mass surveillance. Without a national data protection framework to guarantee baseline safeguards for everyday Americans, methods and avenues for data exploitation will only intensify.

Beyond the now-routine cases of Big Tech's ad tech models that exploit user data for profit, methods of surveillance and monitoring will be sharpened and sold to the highest bidder—both public and private.[2] Now, faster networks with lower latency like 5G provide quick transmission and higher throughput to handle increased data flows. More compute power and options to sort

[1] The concepts and recommendations throughout this testimony are drawn from the author's previous working papers, publications and congressional testimonies, including but not limited to: K. Frederick, "Combating Big Tech's Totalitarianism: A Roadmap," K. Frederick, "Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021," K. Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," K. Frederick, "Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity," K. Frederick, "Facial Recognition Technology: Examining Its Use by Law Enforcement;" and the author's media appearances from 2019–2024.

[2] Big Tech companies already evaluate the digital behavior of their customers and then use their specific digital fingerprints to microtarget their users or deliver tailored ads and information to the user based on this fingerprint. These companies quietly sell this information to advertisers, as well as use it to maximize user engagement and the addictive properties of their platforms.

and process data are advancing in concert along with developments in machine learning and sophisticated analytics that extract value from data. These improvements fit together in mutually reinforcing ways. Multiple data sources can be aggregated and synchronized to look for patterns in behavior, and even potentially identify individuals for further targeting and scrutiny. Private companies like Apple have teased a desire to scan images—and ultimately other files and content—*directly on an individual's private device*,[3] opening the door for the company (and any entity with leverage over this technology) to automatically process and monitor the content of an individual's phone.[4] Certain initiatives may eventually combine these developments into regional panopticons that monitor individuals at local levels using a combination of public and private power.

And yet we already have a real-world example of what happens absent a rigorous, enforceable privacy regime to impose genuine costs on bad commercial actors—the case of kids and social media.

DELETERIOUS IMPACT OF SOCIAL MEDIA ON KIDS

Recent scholarship is finally beginning to reify a causal link between social media and negative impacts on children and teenagers in the West. A January 2023 study conducted by neuroscientists at the University of North Carolina found that social media use, particularly "social media checking behaviors," could be associated with changes in sensitivity to social rewards and punishments in children's brains.[5] In other words, habitual social media use is *rewiring the brains of kids as young as 12 years old*.

Another study published by Cambridge University researchers in March 2022 found a direct relationship between social media use and life satisfaction in younger adolescence. The researchers discovered "…higher estimated social media use predicts a decrease in life satisfaction ratings" and "lower estimated social media use predicts an increase in life satisfaction ratings…" during these critical developmental stages.[6] And the playing field is hardly level. As Surgeon General Vivek Murphy told CNN in January 2023:

> You have some of the best designers and product developers in the world who have designed these products to make sure people are maximizing the amount of time they

[3] Frank Bajak and Barbara Ortutay, "Apple to Scan U.S. iPhones for Images of Child Sexual Abuse," Associated Press, August 6, 2021, https://apnews.com/article/technology-business-child-abuse-apple-inc-7fe2a09427d663cda8addfeeffc40196 (accessed February 5, 2022), and Apple, "Expanded Protections for Children," September 3, 2021, https://www.apple.com/child-safety/ (accessed February 5, 2022).
[4] Matthew D. Greene and Alex Stamos, "Apple Wants to Protect Children. But It's Creating Serious Privacy Risks," The New York Times, August 11, 2021, https://www nytimes.com/2021/08/11/opinion/apple-iphones-privacy html (accessed February 5, 2022).
[5] Maria T. Maza, Kara A. Fox, and Seh-Joo Kwon, "Association of Habitual Checking Behaviors on Social Media With Longitudinal Functional Brain Development," *Psychometric Properties of Screening Instruments for Social Network Use Disorder in Children and Adolescents*, January 3, 2023, https://jamanetwork.com/journals/jamapediatrics/article-abstract/2799812 (accessed March 10, 2023).
[6] Amy Orben, Andrew K. Przybylski, Sarah-Jayne Blakemore, and Rogier A. Kievit, "Windows of developmental sensitivity to social media," Nature, March 28, 2022, https://www.nature.com/articles/s41467-022-29296-3 (accessed March 10, 2023).

> spend on these platforms. And if we tell a child, use the force of your willpower to control how much time you're spending, you're pitting a child against the world's greatest product designers. And that's just not a fair fight.[7]

The sheer breadth and reach of these digital applications and the targeted nature of their algorithms renders these platforms transformative.

TikTok provides but one example. According to an August 2022 Pew poll, sixty seven percent of American teenagers use TikTok and 16 percent do so "almost constantly."[8] But it is not just teenagers. In July 2020, Pew found that 30 percent of *preteens*—children from nine to 11 years old—use TikTok.[9]

And these platforms are ushering in a new phase of teen despair characterized by suicidal ideation and self-harm. One 2022 study found that the platform pushed suicidal content to the 13 year olds in under three minutes of registering.[10] Other studies by Western media outlets created fake profiles to test the algorithm and found that TikTok served registered 14 year old users self-harm and suicidal content within five minutes, as well as depression and mental illness posts within similar timeframes.[11] Young users themselves describe the torrent of self-harm and suicide content from TikTok as "endless."[12] Facebook's own internal research from 2020 determined six percent of American teen Instagram users traced their desire to kill themselves directly to the platform.[13]

Another feature of these platforms, social media challenges, involve engaging in risky—sometimes life-threatening—behaviors meant to go viral. *Bloomberg Businessweek* assessed that TikTok's "blackout challenge," where players attempt to choke themselves with various items until they faint, was linked to the deaths of approximately 15 children aged 12 or younger in the

---

[7] Allison Gordon and Pamela Brown, "Surgeon General says 13 is "too early" to join social media," CNN, January 29, 2023, https://www.cnn.com/2023/01/29/health/surgeon-general-social-media/index html (accessed March 11, 2023).
[8] Emily A. Vogels, Risa Gelles-Watnick, and Navid Massarat, "Teens, Social Media and Technology 2022," Pew Research Center, August 10, 2022, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/ (accessed March 10, 2023).
[9] "Children's Engagement with Digital Devices, Screen Time: Parents of an older child are more likely to say child uses social media sites," in Brooke Auxier, Monica Anderson, Andrew Perrin, and Erica Turner, Parenting Children in the Age of Screens, Pew Research Center, July 28, 2020, https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/pi_2020-07-28_kids-and-screens_01-09/ (accessed March 11, 2023).
[10] Elizabeth Germino, "TikTok pushes potentially harmful content to users as often as every 39 seconds, study says," CBS News, December 14, 2022, https://www.cbsnews.com/news/TikTok-pushes-potentially-harmful-content-to-users-as-often-as-every-39-seconds-study/ (accessed March 10, 2023).
[11] Jim Norton and Jacob Dirnhuber, "We posed as a TikTok teen... and suicide posts appeared within minutes," *The Daily Mail*, September 30, 2022, https://www.dailymail.co.uk/news/article-11268609/We-posed-TikTok-teen-suicide-posts-appeared-minutes html (accessed March 15, 2023); and Asia Grace, I pretended to be a 14-year-old girl on TikTok — and what I saw was so upsetting," *The New York Post*, March 8, 2023 (accessed March 8, 2023).
[12] "The Wall Street Journal Tech News Briefing: The TikTok Spiral, Part 1: Descent," *The Wall Street Journal*, December 27, 2021, https://www.wsj.com/podcasts/tech-news-briefing/the-tiktok-spiral-part-1-descent/90b0fef4-d48d-426d-854f-cab1b1f7afd0 (accessed March 15, 2023).
[13] Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *The Wall Street Journal*, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show -11631620739?mod=hp_lead_pos7 (accessed February 4, 2022).

course of 18 months between 2021 and 2022.[14] In one example, a Pennsylvania mother alleged her daughter accidentally killed herself attempting the blackout challenge after viewing a video suggested by the app.[15] Her daughter was ten years old. As researcher Chris Griswold notes, social media platforms now have "a body count."[16]

Companies like Facebook are aware of these impacts yet continue to double down and expand efforts targeted at children.[17] Facebook set a multi-year goal to create products specifically for *pre*teens, considering them a "valuable but untapped audience."[18] In March 2021, Facebook revealed that it intended to create an Instagram for children younger than 13 years old. (It already has a Messenger app focused on children from six years old to 12 years old). Even after research on Instagram's toxic effects on young girls was made public in October 2021, the head of Instagram declared publicly that "building 'Instagram Kids' is the right thing to do."[19] YouTube Kids invoked children as young as three years old in its rollout in 2015 after easily absorbing a $170 million fine by the Federal Trade Commission (FTC) and the state of New York in 2019 for collecting data on children younger than 13 without parental permission.[20]

At the heart of all of this is the privacy question. I submit that the incentives of private companies to blow past fines, forgo privacy enhancing technologies and age verification, and recruit younger and younger users would be dampened but for a national data protection framework. Such a privacy regime would insulate all Americans—old and young—from the worst to come.

THE WAY FORWARD

As I wrote in 2022, proposals to hold Big Tech companies accountable should empower citizens to redress the imbalance between the companies and their users, focus on how Big Tech

---

[14] Olivia Carville, "TikTok's Viral Challenges Keep Luring Young Kids to Their Deaths," Bloomberg, November 30, 2022, https://www.bloomberg.com/news/features/2022-11-30/is-TikTok-responsible-if-kids-die-doing-dangerous-viral-challenges (accessed March 10, 2023).

[15] Cecilia Kang, "Indiana Sues TikTok for Security and Child Safety Violations," *The New York Times*, December 7, 2022, https://www nytimes.com/2022/12/07/technology/TikTok-lawsuit html (accessed March 10, 2023); and Brendan Pierson, "TikTok immune from lawsuit over girl's death from 'blackout challenge' -judge," Reuters, October 27, 2022, https://www reuters.com/legal/TikTok-immune-lawsuit-over-girls-death-blackout-challenge-judge-2022-10-26/ (accessed March 10, 2023).

[16] Sen. Marco Rubio and Sen. Marsha Blackburn, "Pro-Family Priorities for the 118th Congress," Ethics and Public Policy Center, February 16, 2023, https://eppc.org/events/pro-family-priorities-for-the-118th-congress/ (accessed March 10, 2023).

[17] This section is almost exclusively drawn from my 2021 House Testimony: "Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity," https://www heritage.org/testimony/holding-big-tech-accountable-targeted-reforms-techs-legal-immunity.

[18] Georgia Wells and Jeff Horwitz, "Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show," The Wall Street Journal, September 28, 2021, https://www.wsj.com/articles/facebook-instagram-kids-tweens-attract-11632849667 (accessed November 30, 2021).

[19] Adam Mosseri, "Pausing 'Instagram Kids' and Building Parental Supervision Tools," Instagram Blog, September 27, 2021, https://about.instagram.com/blog/announcements/pausing-instagram-kids (accessed November 30, 2021).

[20] Federal Trade Commission, "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," September 4, 2019, https://www ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (accessed November 29, 2021).

companies leverage their scale and reach to exploit users' data, and implement much more rigorous oversight of these entities.[21]

In terms of company-to-user imbalance, Big Tech companies are restricting choice, demonstrating anti-competitive behavior, and exploiting the consumer. Big Tech companies often preference their own products over those of competitors, quietly sell this information to advertisers, and use it to maximize user engagement and the addictive properties of their platforms. The proposed solutions contend with these practices and address the exploitation of the American consumer. Remedies like circumscribing the collection, storage, and sharing of customer data can also help the consumer by increasing protection of individual privacy and reducing the likelihood of data exploitation. There are a few things we can do right now, with many of these solutions encompassed in the legislative proposals before the subcommittee today:

Pass data privacy legislation.

- Establish a federal data protection framework with appropriate standards and oversight for how the federal government and commercial entities collect, store, and share U.S. user data.
    - Consumers must affirmatively opt in to any system that allows their data to be shared with any third party (with possible exceptions for law enforcement and national security authorities).
    - This should be enforceable by a private right of action with a minimum amount of statutory damages (in the absence of evidence of a greater amount of actual damages) and an attorney's fee provision for any federal private right of action.

Require transparency.

- Require transparency on algorithmic impacts through quarterly transparency reports to the FTC with a public availability component.**[116]**
    - Programmers and other personnel dictate the design and implementation of those algorithms. Users have a right to information on this main ingredient of the product they use.
    - Transparency reports should include detailed impact assessments of how these companies' algorithms operate and affect users, including details on the impact of any ad hoc changes within reporting periods.
    - If companies choose to incur fines rather than comply with FTC enforcement, more aggressive transparency measures such as insight into algorithmic design might be warranted.
        - Carve-outs for smaller competitors and new entrants would be necessary in this instance.
- Require data transparency through quarterly transparency reports to the FTC with a public availability component.

[21] This section is drawn directly from my 2022 Heritage report: "Combating Big Tech Totalitarianism: A Roadmap" with an additional proposal drawn from my 2023 Heritage report: "TikTok Generation: A CCP Official in Every Pocket."

    - Companies should be required to implement Fair Information Practice Principles when handling U.S. user data.
    - Like truth in lending, Congress should require truth in data use through FTC enforcement.
        - Companies should use plain language to tell consumers what happens with their data.

If the above proposed solutions prove ineffective, Big Tech companies should be required to provide researchers with third-party access to data to conduct external impact assessments for algorithmic and data-transparency efforts instead of doing so on a voluntary basis.

Scrutinize Big Tech companies' ad tech model.

- Prompt the FTC to investigate unfair and exploitive data collection, storing, and sharing; excessive online surveillance; and anti-competitive digital advertising practices such as those mentioned above.
- Severely curtail current microtargeting practices that exploit user privacy. For instance, companies can collect generic consumer information under a certain threshold of identifiable information, but biometric data should be classified as "sensitive data" and be given additional privacy protections and strictures including strict time limits on data retention, third-party data sharing, and the prohibition of indefinite data storage.
- Privacy-preserving technologies should be encouraged at all times.

Ensure a national data protection framework addresses third party data collection mechanisms on U.S. users.

- Congress can take measures to curtail the use of these third-party tools—which can be employed by American apps to track and send U.S. user data to foreign controlled companies like TikTok—through comprehensive privacy legislation.
    - Third-party apps can track and send data to completely different companies, even if a user does not sign up for that company's product. Companies can circumvent attempts to protect U.S. user data from certain foreign adversary controlled entities like TikTok because they can still collect this data from the third-party apps.[22] Governing such partnerships between tech companies and the third-parties they share data with would prevent such an end-run around partial bans of companies like TikTok, including those on government devices. For example, blocking such apps from sending data to TikTok is critical to the integrity of a TikTok ban.

Create provisions for platform accountability and transparency when it comes to users under 18 years old, with robust enforcement mechanisms.

[22] Thomas Germain, "How TikTok Tracks You Across the Web, Even If You Don't Use the App," Consumer Reports, September 29, 2022, https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/ (accessed April 15, 2024).

Provide recourse for kids and parents against companies that have become more aggressive in targeting children.

Require public reports on breaches of parental tools and technical safeguards that include privacy by design, opt-in features, and stringent default settings.

The law is a teacher. When it comes to privacy and our children, the time to govern is yesterday. Big Tech—or any commercial or government actor endeavoring to abuse and exploit the American citizen—should be on notice.