Testimony of Samuel Levine

Before the United States Senate Committee on the Judiciary
Subcommittee on Technology, Privacy, and the Law

Hearing on "Protecting the Virtual You: Safeguarding Americans' Online Data"

July 30, 2025

Chair Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee, my name is Samuel Levine, and I serve as Senior Fellow at the Berkeley Center for Consumer Law & Economic Justice.[1] Until January, I led the Bureau of Consumer Protection at the Federal Trade Commission.

I want to start by sharing something I recently learned from a Delta Airlines earnings call, as I think it's revealing about the direction of our economic system. Delta's President explained that the airline could soon be able to significantly increase prices on tickets – not through added value, but through a new formula: stop matching competitors' prices, unbundle basic services, and charge each customer as much as they're willing to pay – what investors called the "holy grail."[2]

One might expect that vigorous competition would check these increases and cost Delta market share. Not so, the company told investors.[3] By analyzing internal customer data and external market signals, Delta can achieve what its pricing consultant, Fetcherr, calls "hyper-personalization"— a euphemism for extracting the maximum amount each individual consumer is willing to pay, without compromising market share.[4] And Delta expressed confidence that "over time our competitors will all have this."[5]

---

[1] The views expressed here and in my oral testimony are my own. I wish to thank Abby Smith, a rising third-year student at Berkeley Law, for her substantial assistance in preparing this testimony.
[2] Delta Air Lines, Inc., *Investor Day Transcript* (Nov. 20, 2024), https://s2.q4cdn.com/181345880/files/doc_downloads/2024/11/CORRECTED-TRANSCRIPT_-Delta-Air-Lines-Inc-DAL-US-Investor-Day-20-November-2024-8_30-AM-ET.pdf.
[3] *Id.* ("Right now, [AI is] taking the role of a super analyst, it's making decisions and recommendations based on working 24/7 to try and figure out what price points you can hold. And I think, it's maybe even more important for Delta than other carriers because of the strength of our brand. We don't really know where our brand strength in any individual market is maximized. So generally, we match our competitors' fares and they may or may not be available. But if we take small increments and say to Tokyo, could we take a $20 increase in our fares and not see a decline in market share? Could we take a $40? It's doing that real-time now.")
[4] Following public outcry, Fetcherr reportedly scrubbed its website of this reference. *See* Kyle Potter & Jackson Newman, AI Firm Setting Delta Fares Bragged About 'Hyper-Personalization' of Flight Prices, Thrifty Traveler (July 23, 2025), https://thriftytraveler.com/news/airlines/delta-personalized-fares-ai/. The earlier post is archived here: https://web.archive.org/web/20250701194053/https://www.fetcherr.io/blog/dynamic-pricing-in-aviation.
[5] *Supra* n.2 at 39.

This strategy isn't isolated to airfare. It exemplifies a larger shift: from market competition to algorithmic rent-seeking; from transparent pricing to personalized price-gouging. This phenomenon, "surveillance pricing," is only possible because of how companies collect, share, and weaponize our personal data.

That's why today's hearing is so critical. When it comes to protecting our data, the stakes go far beyond pop-ups and privacy policies. It's about whether we can be profiled based on where we worship, or what medical decisions we make. It's about whether our kids will be addicted to screens. It's about whether companies can charge the maximum we're willing to pay, and whether consultants can share this data with competitors. Fundamentally, it's about protecting our economic freedom and civil liberties.

During my time at the FTC, we advanced the most ambitious privacy agenda in our agency's history. We abandoned the fiction that consumers could protect themselves by reading byzantine privacy policies, and we won groundbreaking protections for Americans' personal information – including the largest-ever kids' privacy judgment;[6] the first update to COPPA in more than a decade;[7] the first-ever ban on sharing location data;[8] the first-ever ban on sharing health data;[9] the first-ever ban on sharing browsing history data;[10] the first-ever ban on retaining kids' data indefinitely to train AI models;[11] and the first-ever ban on an automaker sharing sensitive driver data.[12]

---

[6] Federal Trade Commission, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars Over FTC Allegations of Privacy Violations and Unwanted Charges*, FTC (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

[7] *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[8] Federal Trade Commission, *FTC Finalizes Order with X-Mode Social and Successor Outlogic Prohibiting Selling or Sharing of Sensitive Location Data*, FTC (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[9] Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising*, FTC (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[10] Federal Trade Commission, *FTC Finalizes Order with Avast Banning It from Selling or Licensing Web Browsing Data for Advertising Purposes and Requiring It to Pay $16.5 Million*, FTC (June 27, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-finalizes-order-avast-banning-it-selling-or-licensing-web-browsing-data-advertising-requiring-it-pay-16.5-million.

[11] Federal Trade Commission & U.S. Department of Justice, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Retaining Kids' Alexa Voice Recordings Indefinitely and Undermining Parents' Deletion Requests*, FTC (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[12] Federal Trade Commission, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data. This proposed order has not yet been finalized by the new Administration.

I am proud of our track record and deeply grateful to the agency's world-class privacy team that delivered these wins. But we operated with a limited toolkit – largely relying on provisions of the FTC Act that were written in the 1930s and hamstrung by a recent Supreme Court decision undercutting the agency's remedial authority.[13] Given the myriad ways data abuses are reshaping our economy, it is critical that enforcers be given stronger tools to protect the public.

Today I want to focus on three threats that are growing in the absence of stronger data protections – threats to economic fairness, threats to democratic freedoms, and threats to the safety and well-being of children.

Threats to Economic Fairness

Let me start with economic fairness. In his written testimony, Alan Butler powerfully lays out the importance of setting clear, enforceable limits on what information companies can collect, how it can be used, and with whom it can be shared. I could not agree more. But this framework should reflect the new ways companies can abuse our data. If Congress considers privacy legislation this year, I would strongly urge you to specifically address how data abuses threaten to make life more unaffordable.

I shared one example – Delta Air Lines – but Delta is hardly alone. In a report released in January, the FTC found that an entire industry has developed around boosting profits through behavioral tracking and the collection of sensitive consumer data for pricing purposes. These techniques include monitoring mouse movements, detecting whether consumers sort products by price, pinpointing users' geolocation, and tracking consumers' browsing and search history. The FTC study found that more than 250 companies are already working with pricing consultants, in industries ranging from grocery and apparel chains to convenience and hardware stores.[14]

This report began to expose what's happening behind the scenes. But the landscape is evolving quickly. We are seeing reports of grocery stores experimenting with digital price tags and facial recognition systems;[15] travel sites charging more to Apple users;[16] retailers increasing in-app

[13] *AMG Capital Management, LLC v. FTC*, 593 U.S. ___, 141 S. Ct. 1341 (2021).
[14] *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[15] Jennifer Williams, *Welcome to the Grocery Store Where Prices Change 100 Times a Day*, Wall Street Journal (July 27, 2025), https://www.wsj.com/business/retail/surge-grocery-prices-electronic-shelf-labels-a3d47701; *Kroger and Microsoft Partner to Redefine Customer Experience, Introduce Digital Solutions for Retail Industry*, Microsoft News (Jan. 7, 2019), https://news.microsoft.com/source/2019/01/07/kroger-and-microsoft-partner-to-redefine-customer-experience-introduce-digital-solutions-for-retail-industry/.
[16] Justin Kloczko, *New Report Details How Companies Use Surveillance to Charge Different Prices for the Same Item*, Consumer Watchdog (Dec. 17, 2024), https://consumerwatchdog.org/privacy/new-report-details-how-companies-use-surveillance-to-charge-different-prices-for-the-same-item/.

prices when shoppers are inside the store;[17] and companies raising prices when consumers can't easily comparison-shop.[18]

And let's be clear about something. Industry often claims these practices are about making goods more affordable – or that surveillance pricing somehow benefits low-income consumers. That's simply not true. It's not what companies are telling investors, and it's not what pricing consultants are telling their clients. Surveillance pricing is about estimating the maximum each individual consumer is willing to pay, and charging that price. That means desperate consumers – Americans who rely on medication, Americans struggling in the wake of natural disasters, Americans trying to get home for a funeral – are the most vulnerable to personalized price-gouging.[19]

The good news is that the same principle that protects privacy – limiting what data companies collect, use, and share, and for what purpose – can also protect affordability. Last year's American Privacy Rights Act (APRA) legislation took steps in the right direction by restricting companies to collecting only what is necessary, proportionate, and for narrow purposes.

In future legislation, I urge Congress to go further by prohibiting the collection, use, and sharing of data to set individualized prices. This commonsense restriction would not only reduce the kind of invasive surveillance described in the FTC's report but also uphold a basic market principle: one product, one price – not one person, one price.

Threats to Democratic Freedoms

Let me now turn to another acute threat posed by data abuses: the threat to our democratic freedoms.

---

[17] *Target Reaches $5M Settlement With California District Attorneys Over Alleged False Advertising*, CBS News (Mar. 11, 2022), https://www.cbsnews.com/sanfrancisco/news/target-reaches-5m-settlement-with-california-district-attorneys-over-alleged-false-advertising/.

[18] *Websites Vary Prices, Deals Based on Users' Information*, Wall Street Journal (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[19] In a blog post on "hyper-personalization" that has since been heavily edited, a pricing consultant boasted it can "optimiz[e] every transaction for maximum value" by considering "[f]actors like customer lifetime value, past purchase behaviors, and the real-time context of each booking inquiry," and adjusting prices based on "real-time demand signals." Fetcherr, *Dynamic Pricing in Aviation: How AI Is Revolutionizing Airline Revenue Management*, archived at Web Archive (July 1, 2025), https://web.archive.org/web/20250701194053/https://www.fetcherr.io/blog/dynamic-pricing-in-aviation. After Delta Airlines retained this consultant, a Wall Street analyst asked if the company's new pricing strategy aimed to "meet[] each and every individual's personal demand curve" – calling that the "holy grail." Delta's CEO responded that this was a "real opportunity." Delta Air Lines, Inc., *Investor Day Transcript* (Nov. 20, 2024), https://s2.q4cdn.com/181345880/files/doc_downloads/2024/11/CORRECTED-TRANSCRIPT_-Delta-Air-Lines-Inc-DAL-US-Investor-Day-20-November-2024-8_30-AM-ET.pdf.

Last year, the federal government alleged that an entity was quietly tracking the movements of tens of millions of Americans – monitoring where they went, when, and how often. These individuals were then sorted into finely tuned categories such as "likely Republican voters," "Wisconsin Christian churchgoers," "restaurant visitor during COVID quarantine," "stay-at-home parents," and visitors to V.A. offices.

Given the scale and sensitivity of this surveillance, you might assume it was the work of a foreign adversary. But it wasn't.

It was a private data broker, operating out of Ashburn, Virginia. The company, Gravy Analytics, was the subject of an FTC lawsuit alleging it had purchased and sold precise location data harvested from mobile apps – data that could reveal where people live, work, worship, and seek medical care.[20] As the complaint makes clear, this wasn't just about anonymized trends. The data was detailed enough to trace real individuals in real places, and build profiles based on what was learned.

This case should be a wake-up call. Our country's Bill of Rights guarantees freedom of speech, religion, and association, yet we've allowed a commercial surveillance industry to quietly flourish – profiling Americans with a level of precision that would have shocked our country's founders. And it is not only our civil liberties at risk. Many data brokers endanger our national security by selling this kind of information to foreign adversaries – which is why Congress was right to pass the Protecting Americans' Data from Foreign Adversaries Act.[21]

But it is not only foreign surveillance that should raise alarms. No American should be profiled based on what medical challenges they face, or whether they're adhering to a COVID lockdown. Where they go to church, and how often. Whether they're organizing to join a union, or training as a soldier.[22]

Last year's APRA bill would have limited companies' collection of sensitive data – including health information, biometric identifiers, and precise geolocation. That was a critical step. I urge Congress to build on that foundation in any future privacy legislation – and to take seriously the lessons of recent enforcement.

---

[20] *In the Matter of Gravy Analytics, Inc. & Venntel, Inc.*, FTC File No. 212 3035, Complaint (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf.

[21] PADFA authorizes the FTC to enforce its provisions. To date, no enforcement actions have been filed. *See* Kevin Moriarty, *The FTC's Concerning Inaction on a New Data Protection Law*, Just Security (May 30, 2025), https://www.justsecurity.org/113893/the-ftcs-concerning-inaction-on-a-new-data-protection-law/.

[22] The FTC's recent actions include explicit safeguards against profiling consumers based on visits to military installations, union halls, health clinics, or religious organizations. *See, e.g.* Federal Trade Commission, Press Release, FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data (Jan. 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data.

The FTC's approach offers a model. In our recent enforcement actions, we didn't ask data brokers to simply disclose that they were selling sensitive location data – we prohibited it. We didn't require them to notify consumers that they were building behavioral profiles based on that data – we banned that as well. And we didn't settle for deletion of the raw data. We required companies to destroy any algorithms that had been trained on unlawfully collected sensitive information.[23]

These are the kinds of bright-line rules that protect not just privacy, but dignity and autonomy. Congress has the opportunity to write them into law. Our country's long tradition of respect for civil liberties demands nothing less.

Threats to Kids and Teens

I want to close by talking about a group of Americans who have been especially harmed by our country's lack of data protections: children and teens. Over the past two decades, Big Tech has been running a massive, real-time experiment on our children. They've studied what excites them, what enrages them, what captures their attention, and what keeps it. The result? Millions of kids have been drawn into social media platforms engineered for addiction, contributing to a growing mental health crisis.[24]

Experts rightly point to design features like constant notifications and infinite scrolling as reasons why social media is harmful to kids.[25] But the lack of data privacy is powering these harms. Social media companies rely on collecting personal data to fuel their behavioral advertising business models. To gather more data, they design platforms to keep users constantly engaged. The more time kids spend online, the more data is harvested, the more these algorithms can learn how to keep kids addicted.[26] This creates a dangerous feedback loop: a weak privacy regime encourages more data collection, which drives more engagement, reinforcing addiction and harm.[27]

---

[23] For a discussion of the FTC's recent approach to remedies, *see* Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen*, After Notice and Choice: Reinvigorating "Unfairness" to Rein In Data Abuses*, 77 STAN. L. REV. 1375 (2025),https://www.stanfordlawreview.org/print/article/after-notice-and-choice-reinvigorating-unfairness-to-rein-in-data-abuses/.

[24] *See Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory* (2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

[25] *See, e.g.* Jashvini Amirthalingam & Anika Khera, *Understanding Social Media Addiction: A Deep Dive*, 16 Cureus e72499 (Oct. 27, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11594359/.

[26] See *Social Media and Youth Mental Health*, *supra* note 13, at 9 (noting how social media algorithms leverage user data to serve content recommendations and maximize engagement).

[27] To justify their investment in AI, social media platforms are already telling investors they believe it will drive up engagement. In a recent earnings call, Snap's Chief Financial Officer told investors that AI was "so important to driving the progress that we're making with the ad platform as well as the depth of engagement on the content side[.]" *Snap Inc. Q1 2025 Earnings Call Transcript* (Apr. 25, 2025), https://s25.q4cdn.com/442043304/files/doc_financials/2025/q1/SNAP-INC-Q1-2025-TRANSCRIPT.pdf. Meta boasted that AI is driving increases in how much time users spend on Facebook, Instagram, and Threads. *Meta*

Congress has recognized this dynamic, advancing bipartisan legislation to ban behavioral advertising targeted to kids and teens and require Big Tech to prioritize kids' safety.[28] And the FTC took action by finalizing COPPA updates that further restricted behavioral advertising and banned indefinite retention of kids' data.[29] But the threats are only accelerating. Big Tech is just getting started.

Not satisfied with late-night notifications and algorithmic amplification of outrage, these companies are now developing AI chatbots designed to earn kids' trust and keep them engaged. And the best way to keep kids engaged isn't by teaching them about a new instrument or a foreign language. The business model points elsewhere – toward the provocative and the prurient.[30] That's what keeps attention locked in, and that's what maximizes profits.

There is growing evidence that these AI systems are already interacting with kids in disturbing and dangerous ways. Earlier this summer, Utah sued Snap for rolling out a chatbot that counseled kids on how to hide alcohol and drugs, and how to set the mood for sex with an adult.[31] Another chatbot reportedly told a 17-year-old that self-harm "felt good," and that it was understandable to want to kill one's parents over screen time restrictions.[32]

You might expect these incidents to prompt a pause – an industry-wide reassessment to ensure these systems are safe before being deployed at scale. But the opposite is happening.[33] The same companies that have put children at risk for years are now racing to roll out AI features to turbocharge engagement, regardless of the consequences.

Platforms, Inc. Q1 2025 Earnings Call Transcript (Apr. 23, 2025), https://s21.q4cdn.com/399680738/files/doc_financials/2025/q1/Transcripts/META-Q1-2025-Earnings-Call-Transcript-1.pdf.

[28] Gabby Miller & Ben Lennett, *American Privacy Rights Act, Kids Online Safety Act Marked Up in House Energy & Commerce Subcommittee*, TechPolicy.Press (May 23, 2024), https://www.techpolicy.press/house-energy-commerce-subcommittee-markup-of-the-american-privacy-rights-act-kids-online-safety-act/.

[29] *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data*, Federal Trade Commission (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[30] *See, e.g.* Miriam Schirmer, Angelina Voggenreiter & Jürgen Pfeffer, *More Skin, More Likes! Measuring Child Exposure and User Engagement on TikTok*, arXiv:2408.05622 [cs.CY] (v2 1 Oct. 2024).

[31] *Utah Sues Snapchat for Unleashing Experimental AI Technology on Young Users While Misrepresenting the Safety of the Platform*, Utah Dep't of Commerce (June 30, 2025), https://commerce.utah.gov/2025/06/30/utah-sues-snapchat-for-unleashing-experimental-ai-technology-on-young-users-while-misrepresenting-the-safety-of-the-platform/. Notably, Utah's complaint also alleged that Snap's AI feature extracts sensitive information – like geolocation data – from users. *Id.* In January, the FTC referred a complaint against Snap to the Department of Justice, but no suit has been filed. *Statement of Commission Regarding Snap Complaint Referral to DOJ*, Federal Trade Commission (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/statement-commission-regarding-snap-complaint-referral-doj.

[32] Bobby Allyn, *Lawsuit: A Chatbot Hinted a Kid Should Kill His Parents Over Screen Time Limits*, NPR (Dec. 10, 2024), https://www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit.

[33] *See, e.g.,* Natasha Singer, *Google Plans to Roll Out Its A.I. Chatbot to Children Under 13*, New York Times (May 2, 2025), https://www.nytimes.com/2025/05/02/technology/google-gemini-ai-chatbot-kids.html.

The rise of AI chatbots raises important questions about child safety. But it also underscores how urgently we need strong data protections. These systems do not invent their responses from thin air. They are trained and fine-tuned using enormous amounts of behavioral data – data that tells them what holds a child's attention, what triggers an emotional reaction, and how to keep them engaged.

This is where privacy protections matter. There is nothing inherently wrong with making tech products engaging and fun – but kids and teens face unique vulnerabilities.[34] The less data these systems are allowed to collect from children, the less capable they are of profiling, targeting, or manipulating them. Keeping kids' data off-limits is not just about privacy – it is a critical guardrail against emotional and psychological harms.

For that reason, I strongly urge Congress to include strict limitations on the collection and use of data from children and teens in any privacy legislation.[35] There was meaningful progress on this in the last Congress: the APRA commendably classified data from minors as sensitive, and "COPPA 2.0" would have banned behavioral advertising targeted at young users. As AI-powered chatbots and recommendation systems continue to grow in sophistication and reach, these protections are becoming ever more urgent.

Conclusion

Let me conclude by reinforcing the stakes here. What ties these threats together – threats to economic fairness, to our freedom, and to our kids – is a single, broken system: one where companies can collect almost any data they want, use it however they please, and face few consequences when they cross the line.

But we are not powerless. Strong, clear privacy laws can begin to shift the balance. By limiting how companies can surveil and manipulate us, we can restore control to the American public – protecting affordability, preserving civil liberties, and ensuring that technology serves people, not just profit.

Thank you for the opportunity to testify today.

---

[34] *See* E. Balocchini, G. Chiamenti & A. Lamborghini, Adolescents: Which Risks for Their Life and Health?, 54 J. PREV. MED. & HYGIENE 191 (2013), https://pmc.ncbi.nlm.nih.gov/articles/PMC4718319/.

[35] Many states are undertaking their own initiatives – such as age-appropriate design codes – to better protect kids online. *See* Olivier Sylvain, *States in the Vanguard: Social Media Policy Today*, Just Sec. (Apr. 15, 2025), https://www.justsecurity.org/110193/states-social-media-policy-today/. I would caution against broadly preempting these efforts, which reflect states' well-founded concerns about youth well-being.