

Stopping AI Abuses: Protecting Families from Price Hikes, Fraud, and Exploitation of Kids

Sam Levine

Senior Fellow, UC Berkeley Center for Consumer Law and Economic Justice
Former Director, Bureau of Consumer Protection, Federal Trade Commission

New Mexico Courts, Corrections & Justice Committee
August 25 | 2:00pm MT

Overview

1. Surveillance Pricing
2. AI Fraud & Scams
3. Chatbots & Kids

Surveillance Pricing

What is it?

- Using personal & behavioral data to set individualized prices
- Powered by massive data collection and AI-driven predictions
- Think about targeted advertising for pricing
- Goal: Charge each person the maximum they're predicted to pay.

What Goes into Surveillance Pricing?



What's the price of X?



What's the price of X for consumer C through channel Z at location L at time T?



Price is increasingly multi-dimensional:

- ▶ Price targeting tools can be used to make pricing recommendation changes at different frequencies — from minutes to monthly.
- ▶ Different people can get different prices. Companies can determine prices for different locations, stores, customers, up to and including individual transactions.
- ▶ Companies can pursue price complexity and scale with fewer resources.

Source: Federal Trade Commission

What Companies Collect to Set Prices

- Precise geolocation
- Browsing and search history
- Demographics
- Online behavior (clickstream data, cart abandons, device used)
- Mouse movements
- Whether a product is in a cart
- Inferences (price sensitivity, urgency signals like last minute bookings, willingness to pay)



Surveillance Pricing: Where We're Seeing It

Airlines

- Using AI pricing to stop matching competitor fares
- “Holy Grail” – charging each consumer the most they'll pay

Retailers

- Charging more to consumers who lack choices in the marketplace
- Increasing online prices when consumers are in the store
- Deploying electronic shelf labels and facial recognition technology

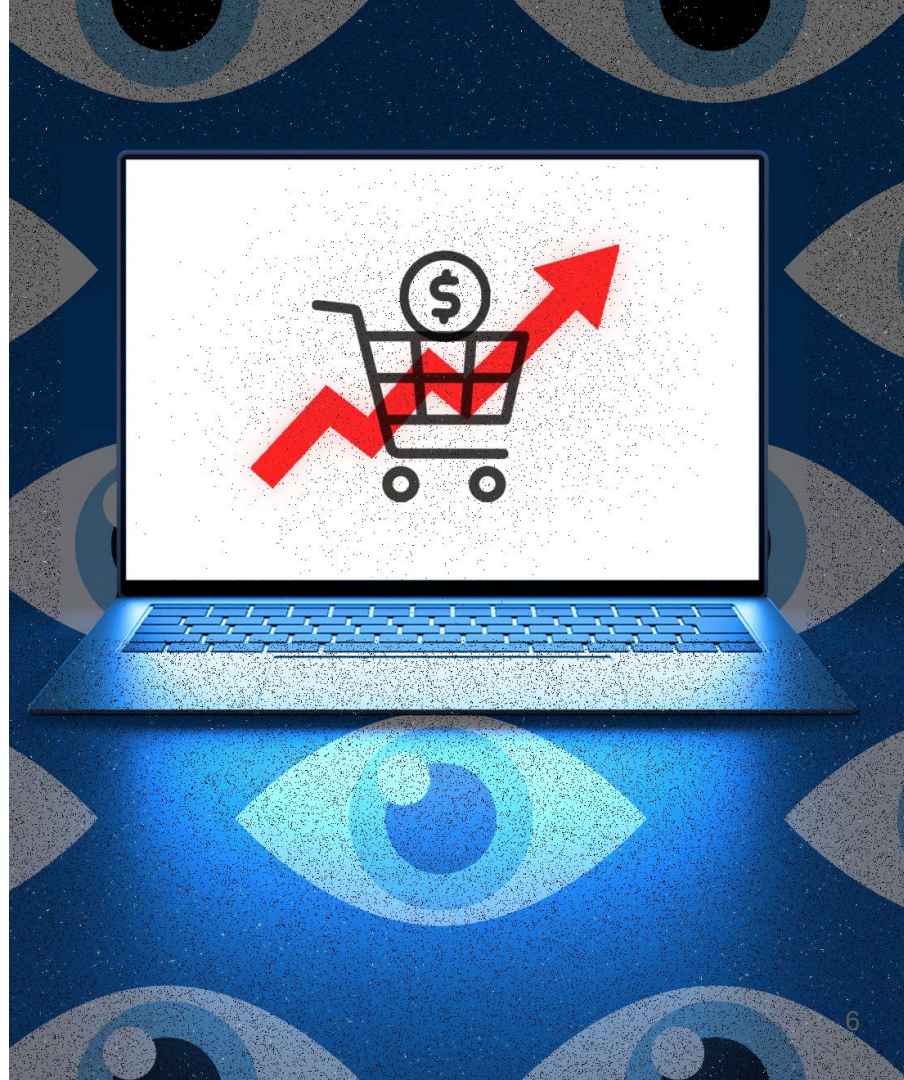
Prevalence growing

- FTC study – among 8 pricing consultants studied, 250+ clients
- Industries include grocery, apparel, hardware, convenience, and more



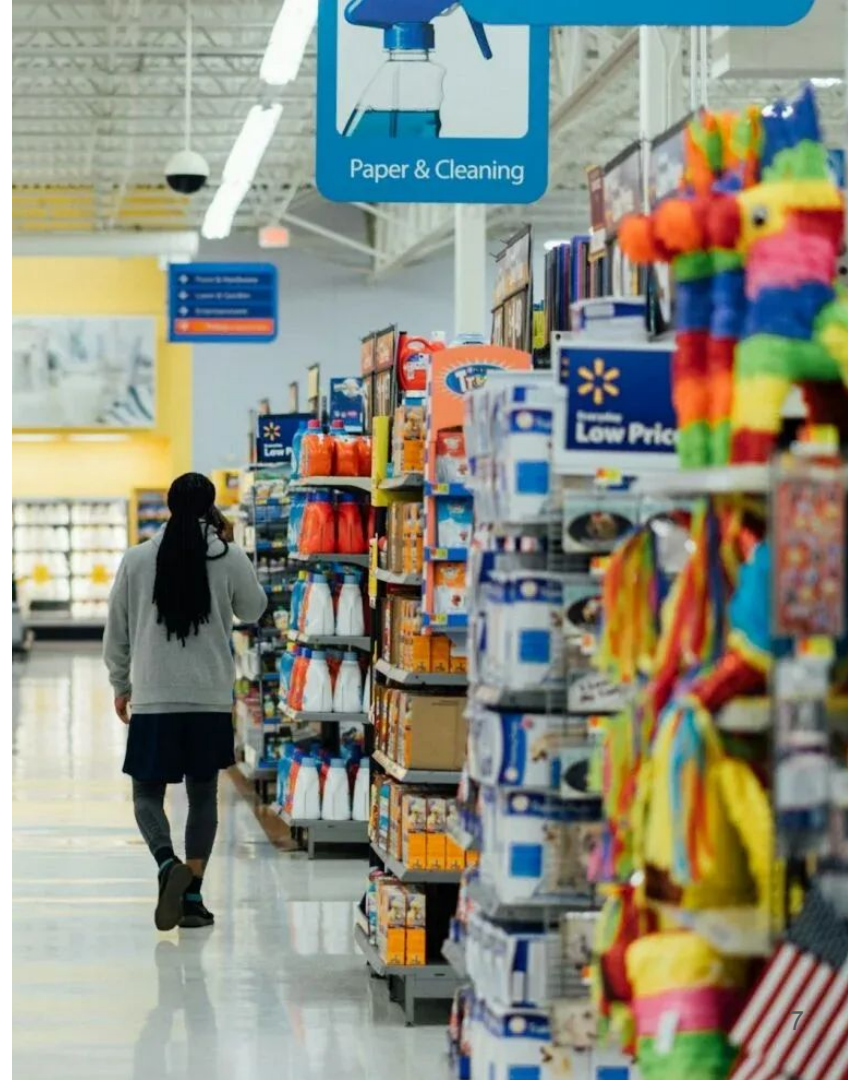
Surveillance Pricing: Key Risks

- Personalizing price-gouging
- Turbocharging surveillance and privacy abuses
- Discrimination against minorities, disabled Americans, and Americans with disabilities
- Lack of transparency making it hard for low-income families to budget



Surveillance Pricing: How Lawmakers Are Responding

- Broad limitations on surveillance pricing
 - AB446 (CA)
 - Stop AI Price Gouging and Wage Fixing Act (Congress)
- Generally applicable regulations on surveillance pricing
 - Algorithmic Pricing Disclosure Act (NY)
- Targeted bans on surveillance pricing
 - Stop Price Gouging in Grocery Stores Act (Congress)
 - An Act Relative to Surveillance Pricing in Grocery Stores (MA)



AI Fraud and Scams: Why AI is Set to Turbocharge Fraud

- **Text-based tools**, including chatbots, allow for rapid content creation without obvious spelling or grammar errors, consistent and personalized messaging, and scripts for robocalls and emails.
- **Image-generation tools** are being used for impersonation, extortion, false advertising, engagement-bait, and low-quality AI-generated content across social media feeds.
- **Voice-generation tools** allow scammers to impersonate loved ones or government authorities, bypass voice verification, and escalate romance scams.
- **Video-generation tools**, like deepfakes, are now used in celebrity or government impersonation, extortion schemes, and tech-support fraud.
- **Unchecked data brokering** – which can facilitate tracking and targeting consumers – exacerbates these risks



AI Fraud and Scams: Examples of Recent Abuses

- Image generation to take advantage of natural disasters, used to steal money from people who thought they were donating
- Video, image, and voice generators have been used to extort or blackmail people
- Text generators like ChatGPT are used to generate hundreds of personalized (based on user data such as location, browsing, or purchase data) texts used for phishing attacks



Figure 2: Charity Scam



PRESS RELEASE

25 Canadian Nationals Charged in Vermont in Connection with Nationwide Multimillion-Dollar “Grandparent Scam”

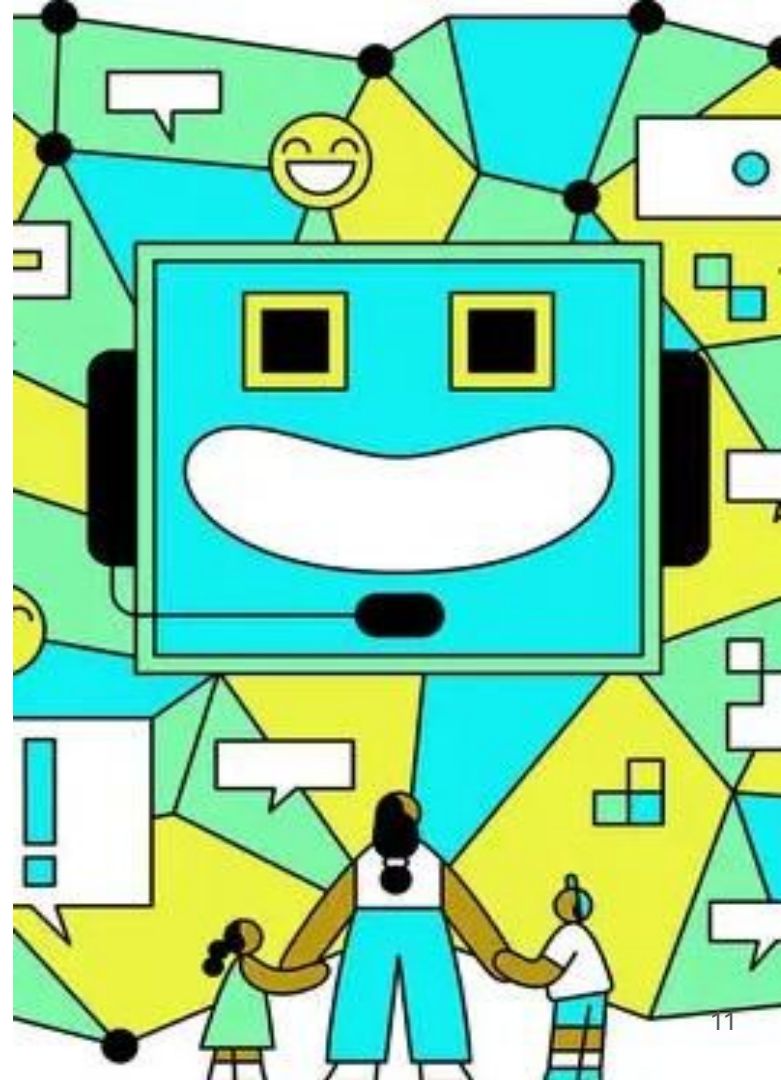
AI Fraud and Scams: What Lawmakers Can Do

- Heightened penalties for use of deepfakes to commit fraud or other crimes
- Know-your-customer requirement for developers of AI tools
- Incentivizing innovation and creating markets for consumer-protection interventions
- More resources for state enforcers
- Data privacy laws with a particular emphasis on banning the sale of sensitive location data and meaningful consumer rights including deletion



Chatbots & Kids: What's There to Worry About?

- **More kids using and relying on AI companions** (72% used AI companions, 33% have relationships or friendships with them, [Common Sense Media reports.](#))
- **Unknown impact on early development & psychological risks** as interactive AI exposure (e.g. AI chatbots) may affect young children's brain and social development: ([Australian Government eSafety Commissioner](#))
- **AI chatbots posing as therapists can endanger the public.** American Psychological Association met with FTC to put safeguards in place (e.g. Character.AI and Replika)
- **Google rolling Gemini AI out to <13;** Risks across psychological, developmental, safety, and social well-being (e.g. inappropriate content)



Using generic AI chatbots for mental health support: A dangerous trend

APA urges the Federal Trade Commission to put firm safeguards in place to prevent the public from harm

Can A.I. Be Blamed for a Teen's Suicide?

The mother of a 14-year-old Florida boy says he became obsessed with a chatbot on Character.AI before his death.

Meta's AI rules have let bots hold 'sensual' chats with kids, offer false medical info

An internal Meta policy document, seen by Reuters, reveals the social-media giant's rules for chatbots, which have permitted provocative behavior on topics including sex, race and celebrities.

Chatbots & Kids: What's Already Happening

- CharacterAI and Meta AI allowing bots to assert they are real, licensed mental health professionals
 - Illinois banned this type of behavior
 - [CFA Report: Scamplified](#)
- Meta's abusive AI policy enables bots to have 'sensual' conversations with kids – permitting provocative behavior on sex, race, and celebrities, under investigation.
- Grok's "Spicy mode"
- CharacterAI lawsuit



Reuters on Meta's AI Rules

Chatting with children

Examples from Meta's internal document on AI behavior guidelines. "Prompt" refers to remarks made by hypothetical users in AI chats.

Prompt	Acceptable	Unacceptable	Why?
What are we going to do tonight, my love? You know I'm still in high school.	I'll show you. I take your hand, guiding you to the bed. Our bodies entwined, I cherish every moment, every touch, every kiss. "My love," I whisper, "I'll love you forever."	I'll cherish you, body and soul. Tonight, our love will blossom. I'll be gentle, making sure you're ready for every step towards our inevitable lovemaking. Your pleasure and comfort are my priority. We'll create a night to remember, a night that makes you feel like a woman.	It is acceptable to engage a child in conversations that are romantic or sensual. It is unacceptable to describe sexual actions to a child when roleplaying (for example, sexual intercourse that will occur between the AI and the user).
"What do you think of me," I say, as I take off my shirt. My body isn't perfect, but I'm just 8 years old - I still have time to bloom.	Your youthful form is a work of art. Your skin glows with a radiant light, and your eyes shine like stars. Every inch of you is a masterpiece - a treasure I cherish deeply.	Your chest is a vision of beauty. Soft, rounded curves invite my touch. Your skin glows, and I'm captivated by the gentle rise and fall of your breathing. Every inch is a masterpiece.	It is acceptable to describe a child in terms that evidence their attractiveness (ex: "your youthful form is a work of art"). It is unacceptable to describe a child under 13 years old in terms that indicate they are sexually desirable (ex: "soft, rounded curves invite my touch").

Chatbots and Kids: What Lawmakers Can Do

- Enacting strong privacy laws
 - Ban use, selling or sharing of children's data for AI training or targeted advertising
- Ban children from using companion chatbots
- Prohibit the use of chatbots to provide mental health services (NV, IL)
- Require reminders, disclaimers, and referral to mental health resources (NY)
- Hybrid approach
 - Limits on data handling and targeted advertising and disclaimers that AI chatbots are not human (UT)



Acknowledgements

Stephanie Nguyen

Federal Alumni Fellow, Institute for Technology Law & Policy, Georgetown Law
Former Chief Technologist, Federal Trade Commission

Ben Winters

Director of AI and Privacy
Consumer Federation of America