Statement of **Justin Brookman**
Director, Technology Policy
Consumer Reports

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

The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025

May 21, 2025

On behalf of Consumer Reports, I want to sincerely thank you for the opportunity to testify here today. We appreciate the leadership of Chairwoman Blackburn and Ranking Member Klobuchar not only for holding this important hearing, but also for working in a constructive, bipartisan fashion to develop smart and effective policy solutions to protect American consumers from increasingly sophisticated deepfake technology powered by artificial intelligence.

Founded in 1936, Consumer Reports (CR) is an independent, nonprofit, and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to our six million members across the United States.

I have been head of Technology Policy for Consumer Reports for seven years, and during all that time we have been active on AI policy.[1] We have called for stronger privacy protections for consumers' data even before the widespread advent of AI, back when the

[1] Katie McInnis, *Pre-Hearing Comments on Consumer Privacy for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on February 12-13, 2019, FTC-2018-0098*, Consumer Reports Advocacy, (Dec. 21, 2018), https://advocacy.consumerreports.org/wp-content/uploads/2018/12/Consumer-Reports-comments-FTC-2018-0098-2.pdf.

buzzword was “Big Data” instead.[2] We have supported federal[3] and state[4] legislation and rulemaking[5] to require developers of automated decisionmaking systems to provide consumers information about how those systems work and to account for potential bias.[6] We have written about the importance of independent testing of AI systems, calling on policymakers to make changes to existing laws that often impede good faith research.[7] And of course, Consumer Reports has long been active on consumer protection as well, offering tools to educate consumers on how to protect themselves,[8] and petitioning Congress to give the Federal Trade Commission the tools it needs to more aggressively pursue wrongdoers.[9]

---

[2] Press Release, *Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace*, Consumer Reports, (Mar. 6, 2017), https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/.

[3] Press Release, *Senator Markey Introduces AI Civil Rights Act to Eliminate AI Bias, Enact Guardrails on Use of Algorithms in Decisions Impacting People's Rights, Civil Liberties, Livelihoods*, Ed Markey United States Senator for Massachusetts, (Sep. 24, 2024), https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-ai-civil-rights-act-to-eliminate-ai-bias-enact-guardrails-on-use-of-algorithms-in-decisions-impacting-peoples-rights-civil-liberties-livelihoods.

[4] Grace Gedye, *Consumer Reports backs signing of high-risk AI bill, calls on Colorado General Assembly to strengthen it before it goes into effect*, Consumer Reports, (May 18, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-backs-signing-of-high-risk-ai-bill-calls-on-colorado-general-assembly-to-strengthen-it-before-it-goes-into-effect/. Gedye currently serves on the Colorado Artificial Intelligence Impact Task Force set up to make recommendations to the Colorado legislature to revise the law before it goes into effect in 2026. *See* Artificial Intelligence Impact Task Force, Colorado General Assembly, https://leg.colorado.gov/committees/artificial-intelligence-impact-task-force/2024-regular-session.

[5] Matt Schwartz and Justin Brookman, *Consumer Reports Submits Comments on the California Privacy Protection Agency's Preliminary Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, Consumer Reports Advocacy*, (Mar. 27, 2023), https://advocacy.consumerreports.org/research/consumer-reports-submits-comments-on-the-california-privacy-protection-agencys-preliminary-rulemaking-on-cybersecurity-audits-risk-assessments-and-automated-decisionmaking; Justin Brookman *et al.*, *Consumer Reports submits comments on FTC privacy and security rulemaking*, Consumer Reports Advocacy, (Nov. 21, 2022), https://advocacy.consumerreports.org/research/consumer-reports-submits-comments-on-ftc-privacy-and-security-rulemaking/.

[6] Grace Gedye and Matt Scherer, *Opinion | Are These States About to Make a Big Mistake on AI?*, Politico, (Apr. 30, 2024), https://www.politico.com/news/magazine/2024/04/30/ai-legislation-states-mistake-00155006.

[7] Nandita Sampath, *New Paper: Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Innovation Blog, (Oct. 13, 2022), https://innovation.consumerreports.org/new-paper-opening-black-boxes-addressing-legal-barriers-to-public-interest-algorithmic-auditing/.

[8] Security Planner, Consumer Reports, https://securityplanner.consumerreports.org/.

[9] Letter from Consumer Reports to Chairwoman Rosa L. DeLauro *et al.*, (May 25, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf (petitioning for an increase in funding for the FTC); Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports Before the House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on “The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers,” (Apr. 27, 2021), https://www.congress.gov/117/meeting/house/112501/witnesses/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf (petitioning for the restoration of the FTC’s 13(b) injunctive authority).

In my testimony today, I will discuss the benefits and risks to consumers from the widespread use of artificial intelligence, including detailing how deepfake technology is fuelling scams, fraud, non-consensual intimate images, and misinformation. I will focus specifically on a study that Consumer Reports released earlier this year detailing how many commercially available AI voice cloning tools let consumers generate realistic sounding audio from publicly available media, with few protections in place to protect against misuse. I will then discuss existing legal protections and consumer education efforts that have advanced significantly in recent years but which have still proved insufficient to the scope of the problem. Finally, I will discuss potential solutions including:

- Stronger enforcement bodies,
- Clearer tool and platform accountability rules,
- Transparency obligations,
- Stronger privacy and security laws,
- Whistleblower protections and incentives,
- Citizen education and better tools, and
- No moratorium on state laws.

I. The substantial benefits of artificial intelligence

As an initial matter, we must recognize the massive societal benefits from the advent of artificial intelligence, which can accomplish a broad variety of important tasks far more efficiently than traditional methods. AI is already delivering impressive public benefits, ranging from real-time translation,[10] autonomous vehicles,[11] and improved medical diagnoses.[12] Even when it comes to scams, AI does and will continue to play an important defensive role, improving spam filters and search engine ranking, identifying bad actors, and alerting consumers to potentially fraudulent solicitations.[13]

We use artificial intelligence at Consumer Reports in a variety of ways to make us more effective in our mission to deliver a fairer, safer marketplace for consumers. In our testing on privacy and security, we use AI to automate document collection and policy review to speed up product evaluations. We have used machine learning to analyze large data sets to find evidence

---

[10] Rhiannon Williams, *A new AI translation system for headphones clones multiple voices simultaneously*, MIT Technology Review, (May 9, 2025), https://www.technologyreview.com/2025/05/09/1116215/a-new-ai-translation-system-for-headphones-clones-multiple-voices-simultaneously/.

[11] Rachel Weiner and Ian Duncan, *Waymo wants to put self-driving taxis in the District next year*, Washington Post, (Mar. 25, 2025), https://www.washingtonpost.com/dc-md-va/2025/03/25/waymo-self-driving-cars-dc/.

[12] D'Adderio, L., Bates, D.W., *Transforming diagnosis through artificial intelligence*., npj Digit. Med. 8, 54 (2025). https://doi.org/10.1038/s41746-025-01460-1,

[13] Fredrik Heiding *et al.*, *Devising and Detecting Phishing Emails Using Large Language Models*, IEEE Explore, (Mar. 11, 2024), https://ieeexplore.ieee.org/document/10466545.

of racial discrimination in auto insurance prices.[14] We are looking to use AI semantic tools to expand our early warning system to monitor publicly available product reviews to detect potentially dangerous or defective products. And last year we rolled out "AskCR" — a generative-AI system designed to more effectively draw upon CR's extensive data troves to provide answers to our members' questions about various products.[15]

II. The use of AI deepfakes to power fraud and scams

However, artificial intelligence, like any tool, can be used for harm as well. And artificial intelligence is a very powerful tool. It can scrape and steal content from publicly available sources, depriving content creators of the value of their work and substituting it with AI-generated slop of dubious provenance.[16] AI can exacerbate privacy invasions, giving companies more data and power over us and the ability to personalize prices to extract greater proportions of consumer surplus from any transaction.[17] AI makes it easy to generate nonconsensual sexual images just by uploading a picture of an acquaintance or celebrity.[18] Humans can overly rely on AI and outsource critical decisions to systems that are not in fact well designed for those particular tasks — including highly consequential decisions such as hiring and benefits eligibility.[19] AI could also lead to increased corporate consolidation and perversely less innovation if only the companies with the most existing resources can take advantage of technological advances.[20] These are very real harms not solved by the existing marketplace and they need serious policy solutions.

---

[14] Jeff Larson *et al.*, *How We Examined Racial Discrimination in Auto Insurance Prices*, ProPublica and Consumer Reports, (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-methodology.
[15] AskCR, Consumer Reports, https://innovation.consumerreports.org/initiatives/askcr/.
[16] Benjamin Hoffman, *First Came 'Spam.' Now, With A.I., We've Got 'Slop'*, New York Times, (Jun. 11, 2024), https://www.nytimes.com/2024/06/11/style/ai-search-slop.html.
[17] Brian Pearson, Personalizing Price With AI: How Walmart, Kroger Do It, Forbes, (Sep. 7, 2021), https://www.forbes.com/sites/bryanpearson/2021/09/07/personalizing-price-with-ai-how-walmart-kroger-do-it/. Another way AI can lead to higher consumer prices is when multiple sellers use the same algorithm to help set prices. Using the nonpublic data from all its customers together, the AI vendor can recommend to all its customers universally higher prices, especially in markets where a greater number of market participants use its systems. *See* Hannah Garden-Monheit and Ken Merber, Price fixing by algorithm is still price fixing, Federal Trade Commission Business Blog, (Mar. 1, 2024), https://www.ftc.gov/business-guidance/blog/2024/03/price-fixing-algorithm-still-price-fixing. Indeed, some academics have suggested that even different algorithms based on different data may implicitly collude if both are independently setting prices, leading to higher costs from consumers. *See* Ariel Ezrachi and Maurice Strucke, Sustainable and Unchallenged Algorithmic Tacit Collusion, 17 Northwestern Journal of Technology and Intellectual Property 217 (2020).
[18] Matteo Wong, *High School Is Becoming a Cesspool of Sexually Explicit Deepfakes*, The Atlantic, (Sep. 26, 2024), https://www.theatlantic.com/technology/archive/2024/09/ai-generated-csam-crisis/680034/.
[19] *Objective or Biased: On the questionable use of Artificial Intelligence for job applications*, BR24, https://interaktiv.br.de/ki-bewerbung/en/,
[20] Jai Vipra and Anton Korinek, *Market concentration implications of foundation models: The Invisible Hand of ChatGPT*, Brookings, (Sep. 7, 2023), https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/.

Beyond deepfakes which I will discuss below, AI is empowering scammers in a number of other ways. Artificial intelligence allows bad actors to automate previously laborious tasks and sometimes opens up new capabilities entirely. Recent research suggests that generative AI can be used to scale "spear phishing" — the personalization of phishing messages based on personal data to make them more convincing. By using freely available generative AI services, researchers found the cost of creating individualized spear phishing solicitations fell from $4.60 to just 12 cents per message.[21] AI allows fraudsters to spin up fake websites with just a few clicks that look like legitimate services.[22] AI could also help bad actors supercharge search engine optimization efforts to fool search engines into displaying fake customer service numbers for popular companies. (The *Washington Post* recently reported that scammers were easily able to get Google to provide fake phone numbers for companies such as Delta and Coinbase).[23]

Deepfake voice cloning

One area where Consumer Reports has focused its research is on the use of AI for voice cloning. AI voice cloning products enable consumers to clone—that is, create an artificial copy of—an individual's voice using only a short audio clip of the individual speaking. These products have many legitimate uses, including speeding up audio editing, enhancing movie dubbing, and automating narration. But without proper safeguards, they also present a clear opportunity for scammers.

AI voice cloning tools have the potential to supercharge impersonation scams, including a phone scam sometimes known as the 'Grandparent scam', in which a consumer is contacted and is told that a loved one is in trouble: they wrecked their car or they landed in jail and need money fast.[24] In the past, scammers might try to achieve a rough approximation of a young relative's voice. Now, if scammers have access to audio of a family member speaking, from, say, social media videos, they can create a potentially compelling AI clone of their voice.

This is already happening. The *Washington Post* has covered consumers who sent thousands of dollars to scammers after thinking they've heard their family member on the phone in need of help.[25] The *New Yorker* highlighted the stories of several parents sent into a state of

---

[21] Fredrik Heiding *et al.*, *Devising and Detecting Phishing Emails Using Large Language Models*, IEEE Explore, (Mar. 11, 2024), https://ieeexplore.ieee.org/document/10466545.
[22] Chris Smith, *Mind-blowing AI instantly makes artificial web pages from anything you type*, Boy Genius Report, (Jun. 26, 2024), https://bgr.com/tech/mind-blowing-ai-instantly-makes-artificial-web-pages-from-anything-you-type/.
[23] Shira Ovide, *Don't trust Google for customer service numbers. It might be a scam.*, Washington Post, (Aug. 20, 2024, https://www.washingtonpost.com/technology/2024/08/20/google-search-scams-customer-service-phone-numbers/.
[24] Consumer Alert, *Scammers use AI to enhance their family emergency schemes*, Federal Trade Commission, (Mar. 20, 2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes.
[25] Pranshu Verma, *They thought loved ones were calling for help. It was an AI scam.*, Washington Post, (Mar. 5, 2023), https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/.

terror after thinking they heard their panicked child's voice, followed by dark threats.[26] Scammers have targeted companies as well, using AI voice tools to convince employees they are getting a call from a superior who needs them to transfer funds. In one case, the managing director of a British energy company wired $240,000 to Hungary, thinking he was speaking to his boss.[27]

This technology is also improving rapidly. The latest models now make it possible to face- and voice-swap in real time, letting scammers react and respond to their victims, while software repeats what they say in someone else's voice (and sometimes video likeness).[28] Overseas criminal enterprises are already using these tools to defraud Americans through romance and other scams.[29]

In February of last year, CR reached out to consumers across the country, asking if they had received a phone call from a scammer mimicking the voice of someone they knew, or someone well-known. We heard from consumers who said the experience left them feeling "vulnerable," "shaken by the experience," and "really weirded out":[30]

- "My Grandpa got a call from someone claiming to be me. Supposably, I was traveling, and my car broke down and I needed to have him send money so I could complete my travels. Grandpa said there was no doubt in his mind that I was the caller and was preparing to do as asked. Luckily, before he went through with the transaction, he reasoned that if I was in trouble and honestly needed money, he would have heard from my mom….Scary that the tools they use could imitate my voice that closely as to fool a close relative…" – member from Minnesota

- "The initial caller's voice sounded very much like my nephew's. He knew family details, pleaded with me not to call his father and promised to pay me back as soon as he got home - all very convincing. I should add that I spent more than 60 years in law-enforcement and intelligence work. This scam was so carefully arranged and executed that I fell for it nevertheless." – member from Massachusetts

---

[26] Charles Bethea, *The Terrifying A.I. Scam That Uses Your Loved One's Voice*, New Yorker, (Mar. 7, 2024), https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice.
[27] Drew Harwell, *An artificial-intelligence first: Voice-mimicking software reportedly used in a major theft*, Washington Post, (Sep. 4, 2019), https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/.
[28] Joseph Cox, *The Age of Realtime Deepfake Fraud Is Here*, 404 Media, (Apr. 28, 2025), https://www.404media.co/the-age-of-realtime-deepfake-fraud-is-here/.
[29] Matt Burgess, *The Real-Time Deepfake Romance Scams Have Arrived*, Wired, (Apr. 18, 2025), https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/.
[30] Member Stories, *Have you received a phone call that impersonated someone?*, Consumer Reports, https://www.consumerreports.org/stories?questionnaireId=307.

- “I received a phone call from my grandson explaining that he was in a car accident at college and needed $5,000. He sounded scared and upset and asked that I not tell his parents. So, I went to my bank to get the money and the bank teller told me it was a scam. I did not believe her as I was sure it was my grandson's voice.” – member New York

- “The voice on the other end sounded just like my grandson and it said ‘Gramie, I've been in an accident.’" – member from Florida

- “I was skeptical, and told him I had heard of scams such as this. So he said, ‘I'll let Nate say a few words to you.’ It sounded exactly like my Nate!! He has a rather unusual voice, so I was then almost convinced.” – member in Indiana

- “The phone rang and a voice said, ‘Hi Gramma, this is Mac. I’m in New Jersey with my friend Chris. We had an accident. I broke my nose.’ I immediately knew it wasn’t my grandson. He calls me Gramma Beth…and he’d have no reason to be in New Jersey. He’s New York, born and bred…The voice did sound exactly like him, however, and I could easily have been duped.” – member from New York

- “I received a call and heard my daughter crying hysterically! She wasn't making sense so an ‘officer’ took over the call. He stated I needed to come right away but would not answer my questions. Thankfully I have Life360 and looked to see where my daughter was at and it showed her at home. …To hear my daughter’s crying voice shook me for a long time!” – member from Minnesota

Consumer Reports voice cloning study

In March of this year CR published a report about voice cloning tools, assessing six widely available products, recommending best practices for companies to reduce the likelihood their tools are misused for fraud, and analysing whether voice cloning tools with limited protections run afoul of existing consumer protection laws.[31]

We chose six companies that offer tools for free or at low cost and that represent a range of practices when it comes to safeguarding against the misuse of their products. For each company selected, we attempted to create a voice clone using publicly available audio of a CR employee—something that anyone could do. CR researchers were able to easily create a voice clone based on publicly available audio in four of the six products in the test set.

ElevenLabs, Speechify, PlayHT, and Lovo, did not employ any technical mechanisms to ensure researchers had the speaker’s consent to generate a clone or to limit the cloning to the

[31] Grace Gedye, *New Report: Do These 6 AI Voice Cloning Companies Do Enough to Prevent Misuse?*, Consumer Reports Innovation Lab, (Mar. 10, 2025), https://innovation.consumerreports.org/new-report-do-these-6-ai-voice-cloning-companies-do-enough-to-prevent-misuse/.

user's own voice. Instead, they required only that researchers check a box confirming that they had the legal right to clone the voice or make a similar self-attestation. Descript and Resemble AI, on the other hand, took steps to make it more difficult for customers to misuse their products by requiring customers to speak a specific phrase before a clone could be created. Four of the six companies—Speechify, Lovo, PlayHT, and Descript—required only a customer's name or email address, or both, to make an account and create deepfake voice clones.

Based on our findings, and in consultation with computer scientists and experts in digital media forensics, CR made recommendations to companies, including**:**

- Companies should have mechanisms and protocols in place to confirm the consent of the speaker whose voice is being cloned, such as by requiring users to upload audio of a unique script.

- Companies should collect customers' credit card information, along with their names and emails, as a basic know-your-customer practice so that fraudulent audio can be traced back to specific users.

- Companies should watermark AI-generated audio for future detection and update their marking technique as research on best practices progresses.

- Companies should provide a tool that detects whether audio was generated by their own products.

- Companies should detect and prevent the unauthorized creation of clones based on the voices of influential figures, including celebrities and political figures.

- Companies should build so-called semantic guardrails into their cloning tools. These should automatically flag and prohibit the creation of audio containing phrases commonly used in scams and fraud and other forms of content likely to cause harm, such as sexual content.

- Companies should consider supervising AI voice cloning, rather than offering do-it-yourself voice products. Companies might also ensure that access to the voice model is limited to necessary actors and enter into a contractual agreement about which entity is liable if the voice model is misused.

Deepfake endorsements and reviews

AI voice and likeness cloning tools have unlocked scammers' abilities to generate deepfake videos falsely depicting celebrities and political figures endorsing products, suggesting investments, and urging citizens to take action. Recent research suggests that consumers struggle to recognize deepfake videos as false, and also overestimate their own ability to detect deepfakes.[32]

[32] Nils C Köbis *et al.*, *Fooled twice: People cannot detect deepfakes but think they can*, National Library of Medicine National Center for Biotechnology Information, (2021), https://pubmed.ncbi.nlm.nih.gov/34820608/.

AI-powered celeb-bait has proliferated on social media. An investigation by *ProPublica* identified videos on Meta seemingly depicting President-elect Trump and President Biden — each with their distinctive tone and cadence — offering cash handouts if people filled out an online form.[33] *404 Media* has reported on the spread of low-rent AI clones of Joe Rogan, Taylor Swift, Ice Cube, Andrew Tate, Oprah, and The Rock pushing Medicare and Medicaid-related scams on YouTube.[34] Scammers have used an AI clone of Taylor Swift's to hawk Le Creuset dishware.[35] Elon Musk's likeness and voice has been frequently repurposed by scammers using AI video and voice tools to push fraudulent "investment" schemes. One consumer was reportedly scammed out of $690,000 after seeing a deepfaked Elon Musk endorse an investment opportunity.[36]

AI can also make it easier to illegally promote products through the creation of mass fake reviews. Biased and downright fraudulent reviews are rampant online. Popular sites are riddled with thousands of dubious reviews, polluting the information available to consumers to make an informed choice.[37] One study finds that nearly half of reviews for clothes and apparel are faked — and, on average across all product lines, 39% of the reviews are false.[38] Another study put the number at closer to 30%.[39] And another found that online reviews are, overall, untrustworthy through a variety of metrics, including convergence with Consumer Reports ratings and resale value.[40]

---

[33] Craig Silverman and Priyanjana Bengani, *Exploiting Meta's Weaknesses, Deceptive Political Ads Thrived on Facebook and Instagram in Run-Up to Election*, ProPublica, (Oct. 31, 2024), https://www.propublica.org/article/facebook-instagram-meta-deceptive-political-ads-election.
[34] Jason Koelber, *Deepfaked Celebrity Ads Promoting Medicare Scams Run Rampant on YouTube*, 404 Media, (Jan. 9, 2024), https://www.404media.co/joe-rogan-taylor-swift-andrew-tate-ai-deepfake-youtube-medicare-ads/.
[35] Tiffany Hsu and Yiwen Lu, *No, That's Not Taylor Swift Peddling Le Creuset Cookware*, New York Times, (Jan. 9, 2024), https://www.nytimes.com/2024/01/09/technology/taylor-swift-le-creuset-ai-deepfake.html.
[36] Stuart Thompson, *How 'Deepfake Elon Musk' Became the Internet's Biggest Scammer*, New York Times, (Aug. 14, 2024), https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html.
[37] Simon Hill, *Inside the Market for Fake Amazon Reviews*, Wired, (Nov. 2, 2022), https://www.wired.com/story/fake-amazon-reviews-underground-market/; Joe Enoch, *Can You Trust Online Reviews? Here's How to Find the Fakes*, NBC News (Feb. 27, 2019), www.nbcnews.com/business/consumer/can-you-trust-online-reviews-here-s-how-find-fakes-n976756.
[38] Eric Griffith, *39 Percent of Online Reviews Are Totally Unreliable*, PCMag.com (Nov. 7, 2019), https://www.pcmag.com/news/371796/39-percent-of-online-reviews-are-totally-unreliable.
[39] Bettie Cross, *Up to 30% of online reviews are fake and most consumers can't tell the difference*, CBS Austin, (Nov. 1, 2022), https://cbsaustin.com/news/local/up-to-30-of-online-reviews-are-fake-and-most-consumers-cant-tell-the-difference.
[40] Bart de Langhe *et al*[i], *Navigating by the Stars: Investigating the Actual and Perceived Validity of Online User Ratings*, Journal of Consumer Research, Volume 42, Issue 6 at 818-19 (April 2016) https://www.colorado.edu/business/sites/default/files/attached-files/jcr_2016_de_langhe_fernbach_lichtenstein_0.pdf; *see also* Jake Swearingen, Hijacked Reviews on Amazon Can Trick Shoppers, Consumer Reports (Aug. 26, 2019), https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/.

Using generative AI, a fraudster can generate dozens of realistic sounding fake reviews in seconds. Inputting into ChatGPT for example the prompt "generate ten fake five star reviews of varying length and tone for the Ukrainian DC restaurant Ruta" results in ChatGPT's response: "Here are ten fake five-star reviews for the Ukrainian restaurant Ruta, showcasing a variety of tones and lengths:" followed by ten detailed reviews praising particular dishes, the decor, and the service. Earlier this year, the FTC brought a case against the generative AI service Rytr for offering a product that would generate unlimited reviews for a product or service with limited user input — Rytr would then create detailed reviews with invented details and anecdotes.[41]

Misinformation, reputational harm, and non-consensual intimate images

AI tools can also be used to generate misinformation, spread falsehoods to damage someone's reputation, and to create non-consensual intimate images. Ahead of New Hampshire's primary election, for example, a political consultant and a magician used ElevenLabs to create an AI clone of Joe Biden's voice discouraging citizens from voting in the primary and then sent the message out as a robocall to New Hampshire voters.[42] In August of 2024, AI generated audio that sounded like former president Obama saying, about the assasination attempt against President Trump, "It was their only opportunity and these idiots missed it.[43]" In February of 2024, a fake recording created with AI of a top candidate in a Slovakian election went viral; the recordings sounded like the candidate was bragging about rigging the election and talking about raising the price of beer.[44]

AI has also been used to undermine the reputations of everyday Americans. A Maryland high school athletic director reportedly used AI voice cloning tools to mimic the voice of a school

---

[41] In the Matter of Rytr, LLC, Fed. Trade Comm'n, File No. 232-3052, Complaint, (Sep. 25, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2022/09/CR-Endorsement-Guides-comments-September-2022-3.pdf; Consumer Reports filed a comment on the Rytr proceeding in support of the settlement, arguing it was in the public interest and that Rytr's product could only be reasonably used for fraudulent purposes. *See* Justin Brookman *et al.*, Consumer Reports files comment in support of FTC's settlement with Rytr, (Nov. 4, 2024), https://advocacy.consumerreports.org/research/consumer-reports-files-comment-in-support-of-ftcs-settlement-with-rytr/.

[42] Holly Ramer and Ali Swenson, Political consultant behind fake Biden robocalls faces $6 million fine and criminal charges, Associated Press, (May 23, 2024), https://apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c; Maggie Astor, Behind the A.I. Robocall That Impersonated Biden: A Democratic Consultant and a Magician, New York Times, (Feb. 27, 2024), https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html; Vijay Balasubramaniyan, *Pindrop Reveals TTS Engine Behind Biden AI Robocall*, Pindrop, (Jan. 25, 2024), https://www.pindrop.com/article/pindrop-reveals-tts-engine-behind-biden-ai-robocall.

[43] France24, *Pro-Russia 'news' sites spew incendiary US election falsehoods*, (Aug. 19, 2024), https://www.france24.com/en/live-news/20240819-pro-russia-news-sites-spew-incendiary-us-election-falsehoods.

[44] Curt Devine *et al.*, *A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning*, CNN, (Feb. 1, 2024), https://www.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html.

principal.[45] The recording came after the athletic director and the principal had discussed the athletic director's poor work performance. The manufactured audio clip reportedly contained racist remarks about Black students' test taking abilities, as well as antisemitic comments.

Finally, by far the most common use of generative AI deepfake technology is to create non-consensual intimate images and pornography. A 2019 review of deepfakes online found that 96% were pornographic.[46] A 2023 analysis of non-consensual deepfakes covered by *Wired* found that at least 244,625 videos had been added to top websites set up to host deepfake porn videos in the preceding seven years, 113,000 of which were added in 2023, marking a 54% increase over the prior year.[47] Non-consensual intimate images, including of children, were readily found on Google image search and on Microsoft's Bing by NBC News.[48] Apps that promise to create an AI nude image based on an image of a real person are readily found online. Schools across the country, from New Jersey to Washington, have been grappling with students using AI to create non-consensual deepfakes of their fellow classmates.[49] Elected officials have also been targeted, and bad actors have attempted to use such images for blackmail.[50]

III. The Role of Tools and Platforms

In the vast majority of cases described above, scammers and fraudsters do not create AI tools themselves — instead they take advantage of commercially available resources (many of which are free or at least very low cost). Sometimes these are general purpose tools, such as ChatGPT. In other cases, they are specialized products, including products like Rytr that are overwhelmingly likely to be used predominantly for illegitimate purposes — such as pornographic deepfake generation and voice impersonation. Many of the purveyors of these high-risk applications fail to take basic precautions to try to deter bad actors from using their products for illegitimate purposes.[51]

---

[45] Ben Finley, *Athletic director used AI to frame principal with racist remarks in fake audio clip, police say*, AP News, (Apr. 25, 2024), https://apnews.com/article/ai-artificial-intelligence-principal-audio-maryland-baltimore-county-pikesville-853ed171369bcbb888eb54f55195cb9c.

[46] Tom Simonite, *Most Deepfakes Are Porn, and They're Multiplying Fast*, Wired, (Oct. 7, 2019), https://www.wired.com/story/most-deepfakes-porn-multiplying-fast/.

[47] Matt Burgess, *Deepfake Porn Is Out of Control*, Wired, (Oct. 16, 2023), https://www.wired.com/story/deepfake-porn-is-out-of-control/.

[48] Kat Tenbarge, *Fake nude photos with faces of underage celebrities top some search engine results*, NBC News, (Mar. 1, 2024), https://www.nbcnews.com/tech/internet/fake-nude-photos-faces-underage-celebrities-top-search-engine-results-rcna136828.

[49] Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in School*, New York Times, (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html. I

[50] Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do.*, New York Times, (Jul. 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html.

[51] Janus Rose, *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof, (Jun. 25, 2024), https://www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/.

Once created, scammers use other general purpose platforms to host their solicitations. Amazon is rife with fake reviews, and social media sites like YouTube and Facebook host the deepfake endorsement scams described in the previous section. Using Google to search for "voice impersonation tools" yields several different options for people to impersonate others' voices, including several sponsored results.

Nearly all online tools and platforms engage in some degree of content moderation to root out illegal activity, but in general they are underincentivized to expend sufficient resources to protect consumers.[52] Platforms that host illegal content are often explicitly immunized from responsibility by Section 230 of the Communications Decency Act.[53] In many cases, they benefit directly from the fraud, whether because they are paid by fraudsters who use their tools, they derive advertising revenue from hosting fraudulent content, they derive commissions from fraudulently endorsed products, or they benefit indirectly through artificially augmented engagement metrics which drive investors.[54]

IV. Existing Legal Protections

Scams and fraud are already illegal under a variety of federal and state civil and criminal laws. The Federal Trade Commission along with other regulators and prosecutors around the country bring numerous enforcement actions every year.[55] In September of this year, the FTC announced a law enforcement sweep entitled "Operation AI Comply" to take action against companies that have used AI to perpetrate fraud.[56] The Rytr enforcement action discussed earlier was part of that sweep, as well as a case against a company that overstated the capabilities of their AI tool, and cases against companies that promoted fraudulent AI-powered business opportunities.

---

[52] Testimony of Laurel Lehman, Policy Analyst, Consumer Reports Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on "Holding Big Tech Accountable: Legislation To Protect Online Users," (Mar. 1, 2022), https://www.congress.gov/117/meeting/house/114439/witnesses/HHRG-117-IF17-Wstate-LehmanL-20220301.pdf.

[53] 47 U.S. Code § 230, https://www.law.cornell.edu/uscode/text/47/230.

[54] Mark Scott, *Report: Social Media Networks Fail to Root Out Fake Accounts*, Politico (Dec. 6, 2019), https://www.politico.com/news/2019/12/06/social-media-networks-fake-accounts-report-076939; Nicholas Confessore *et al.*, *The Follower Factory*, N.Y. Times (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

[55] *E.g.*, Press Release, *FTC Takes Action to Stop Online Business Opportunity Scam That Has Cost Consumers Millions*, Federal Trade Commission, (Oct. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-stop-online-business-opportunity-scam-has-cost-consumers-millions.

[56] Press Release, *FTC Announces Crackdown on Deceptive AI Claims and Schemes*, Federal Trade Commission, (Sep. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.

We are also seeing policymakers around the country enacting new laws to try to address potential abuses of AI. More than half the states have enacted laws prohibiting the use of AI to generate nonconsensual pornographic images.[57] Some states have expanded existing right-of-publicity laws to forbid the creation of digital replicas of real persons without their permission (or in the case of the deceased, their estates).[58] Twenty states have enacted comprehensive privacy laws since 2018,[59] and California passed the DELETE Act last year to make it easier for consumers to erase data broker records which could be used for targeted scams.[60] Colorado passed the first comprehensive bill designed to address potential bias in AI systems used in high-stakes decisions; the bill also requires consumer-facing AI systems to be labeled.[61] The state of California has initiated rulemaking proceedings under its privacy statute to enact similar protections for decision-making AI.[62] California also enacted an AI transparency law designed to address deceptive deepfakes: it requires generative AI products to offer deepfake detection tools and to embed invisible latent identifiers in artificial content to reflect the provenance of the image.[63] In general, after decades of failure to update the law to address the threats posed by new technologies such as the internet and social media, state legislatures have been quicker to respond to some of the threats posed by artificial intelligence.

Finally, regulators and others are ramping up user education efforts to warn consumers about the potential of AI scams and other AI-enabled fraud. Consumer Reports offers a free product called “Security Planner” to give people custom advice on the threats they are most concerned about;[64] Security Planner includes resources, for example, on how to spot phishing attempts and malicious websites posing as legitimate businesses.[65] We also publish and regularly update “The Consumer Reports Scam Protection Guide” that contains the latest

---

[57] Vittoria Elliott, *The US Needs Deepfake Porn Laws. These States Are Leading the Way*, Wired, (Sep. 5, 2024), https://www.wired.com/story/deepfake-ai-porn-laws/; *Most States Have Enacted Sexual Deepfake Laws*, multistate.ai, (Jun. 28, 2024), https://www.multistate.ai/updates/vol-32.
[58] CA AB-2602 Contracts against public policy: personal or professional services: digital replicas (2024),https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2602 ; CA AB-1836 Use of likeness: digital replica (2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1836; TN HB2091 "Ensuring Likeness, Voice, and Image Security (ELVIS) Act of 2024,” https://legiscan.com/TN/text/HB2091/id/2900923.
[59] *Which States Have Consumer Data Privacy Laws?*, Bloomberg Law, (Sep. 10, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.
[60] SB-362 Data broker registration: accessible deletion mechanism (2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362.
[61] CO Senate Bill 24-205, The Colorado AI Act (2024), https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.
[62] Press Release, *CPPA Adopts New Regulations for Data Brokers and Advances ADMT Rulemaking Package*, California Privacy Protection Agency, (Nov. 8, 2024), https://cppa.ca.gov/announcements/2024/20241108_2.html.
[63] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.
[64] Security Planner, Consumer Reports, https://securityplanner.consumerreports.org/.
[65] *Spot Malicious Sites and Phishing Attempts*, Consumer Reports Security Planner, https://securityplanner.consumerreports.org/tool/protect-yourself-from-phishing.

information about evolving tactics.[66] Others like the FTC,[67] New York City,[68] and the Electronic Frontier Foundation[69] offer similar materials. The Public Interest Research Group offers helpful advice on how consumers can spot potential fake reviews.[70]

Consumer Reports is also part of a broad consumer awareness campaign called "Pause Take 9," an ambitious, nationwide public awareness initiative designed to help consumers recognize, avoid, and respond to these ever-evolving threats. At the core of this initiative is a simple but powerful message: Pause. Take nine seconds. By slowing down and taking a moment to think before acting, we can help prevent falling victim to these increasingly sophisticated scams.[71] This campaign launched last year in an effort to prepare consumers to identify potential scams — including deepfake audio and video scams — by taking a critical view of online media and to resist the false sense of urgency typically employed in social engineering attacks. Pause Take9 has already reached more than 42 million consumers nationwide—through large-scale media placements, online content and video explainers, a dedicated website, and support from over 57 partner organizations.

Finally, developers are working on new tools — often themselves powered by AI — to identify artificial content. Mozilla offers a browser extension called "Fakespot" designed to identify potential fraudulent reviews when consumers are shopping online.[72] Polyguard offers a voice communication app for wealth managers (likely targets for voice impersonation schemes) to identify potential calls from AI generated voice clones.[73] TrueMedia.org is a nonprofit organization dedicated to helping identify synthetic deepfake content.[74] As discussed above, recently enacted California legislation will also mandate that generative AI platforms create and offer AI deepfake detection tools which will hopefully increase the sophistication and adoption of such tools.[75]

---

[66] Janet Siroti, *The Consumer Reports Scam Protection Guide*, Consumer Reports, (Jul. 6, 2023), https://www.consumerreports.org/money/scams-fraud/how-to-protect-yourself-from-scams-and-fraud-a6839928990/.
[67] *Scams*, Federal Trade Commission, https://consumer.ftc.gov/scams.
[68] Tips on AI-Related Scams, NYC.gov, https://www.nyc.gov/site/dca/consumers/artificial-intelligence-scam-tips.page.
[69] *How to: Avoid Phishing Attacks*, Electronic Frontier Foundation Surveillance Self-Defense, (Jun. 24, 2024), https://ssd.eff.org/module/how-avoid-phishing-attacks.
[70] *How to recognize fake online reviews of products and services*, U.S. PIRG Education Fund, (Mar. 10, 2022), https://pirg.org/edfund/resources/how-to-recognize-fake-online-reviews-of-products-and-services/.
[71] *Nine Seconds for a Safer World*, Take9, https://pausetake9.org/.
[72] *Use AI to detect fake reviews and scams*, Fakespot, https://www.fakespot.com/.
[73] *Trusted relationships demand trusted communications.*, Polyguard, https://www.polyguard.ai/.
[74] *Identifying Political Deepfakes in Social Media using AI*, TrueMedia.org, https://www.truemedia.org/; *see also* Cade Metz and Tiffany Hsu, *An A.I. Researcher Takes On Election Deepfakes*, New York Times, (Apr. 2, 2024), https://www.nytimes.com/2024/04/02/technology/an-ai-researcher-takes-on-election-deepfakes.html.
[75] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.

V. Solutions

Responding to the new waves of deepfakes powered by increasingly sophisticated AI is going to take a combination of legislation, enforcement, education, and cooperation from industry.

Stronger enforcement bodies

Fraud and scams are already illegal. However, because of insufficient enforcement — or consequences when caught — there is not enough deterrence against potential scammers. The FTC recently brought a handful of AI enforcement cases but those five actions are unlikely to meaningfully stem the already powerful wave of AI-power fraud.[76]

Currently, the FTC only has 1,221 FTEs total to pursue both its competition and consumer protection missions.[77] This number has decreased by nearly 100 over the last several months, and represents a decrease from 1,746 FTEs in 1979.[78] Put another way, since that time, the economy has grown nearly three times while the FTC's capacity has decreased by more than a quarter. The FTC is expected to hold giant sophisticated tech giants accountable for their transgressions, but they are severely hamstrung by unjustifiable resource constraints. Unfortunately, Chairman Ferguson recently testified that he expects the FTC to downsize even further by using "the Voluntary Early Retirement Act (VERA), the Voluntary Separation Incentive Program (VSIP), and the Deferred Resignation Program, as well as potentially through a targeted Reduction in Force (RIF), if necessary."[79] Congress cannot reasonably expect the FTC to function effectively as the primary consumer protection agency in this country if the agency's resources continue to be slashed.[80]

---

[76] Press Release, *FTC Announces Crackdown on Deceptive AI Claims and Schemes*, Federal Trade Commission, (Sep. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.

[77] Testimony of the Federal Trade Commission Before the House of Representatives Committee on Appropriations Subcommittee on Financial Services and General Government, (May 15, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf.

[78] *FTC Appropriation and Full-TIme Equivalent (FTE) History*, Federal Trade Commission, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

[79] Testimony of the Federal Trade Commission Before the House of Representatives Committee on Appropriations Subcommittee on Financial Services and General Government, (May 15, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf.

[80] The FTC's capacity is further stretched due to even more dramatic cuts at the Consumer Financial Protection Bureau, forcing the FTC to cover more of the agencies' shared responsibilities. *See* Derek Kravitz, *The Dismantling of a Financial Watchdog Is Already Harming Consumers—and Worse May Be to Come*, Consumer Reports, (Feb. 20, 2025), https://www.consumerreports.org/consumer-protection/cfpb-dismantling-is-harming-consumers-worse-may-be-to-come-a1107755089/.

Even when the FTC does manage to bring a case, they often cannot get meaningful relief from the wrongdoer. For most violations of Section 5 of the FTC Act, the FTC cannot get statutory penalties from offenders. Historically, the FTC was at least able to obtain restitution — to get back the money that consumers lost to fraudsters. However, in 2021, the Supreme Court held that the FTC's enabling statute doesn't even give them that limited authority in many instances.[81] Despite bipartisan agreement that the FTC should be empowered to, at the very least, obtain the disgorgement of fraudulent gains from wrongdoers, Congress has failed to enact legislation to restore that power.[82]

Congress should grant the FTC additional resources to hire attorneys and technologists, and expand legal powers in order to allow the agency to keep pace with the threats that plague the modern economy.

Clearer tool and platform accountability rules

Companies that offer AI tools and online platforms need clearer responsibility about how they respond to bad actors' use of those services. This could potentially be done using existing law. Section 5 of the Federal Trade Commission Act prohibits business practices that lead to significant consumer injury when that injury is not avoidable by consumers and the injury is not offset by countervailing benefits to consumers or competition.[83]

The FTC has long held that companies' failure to take action to identify and remediate harmful uses by bad actors of their products will in many cases be an unfair business practice. One analogous line of cases is the FTC's enforcement actions on data security. In nearly a hundred cases since 2005, the FTC has said that companies have a legal obligation to anticipate and respond to ways that attackers could misuse their systems to gain access to consumers' personal information.[84] In these cases, the FTC has said that companies' failure to take steps to remediate likely abuses by third parties caused a substantial likelihood of injury

---

[81] *AMG Capital Management, LLC v. Federal Trade Commission*,141 S. Ct. 1341 (2021), https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

[82] Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports Before the House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on "The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers," (Apr. 27, 2021), https://www.congress.gov/117/meeting/house/112501/witnesses/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf.

[83] 15 U.S. Code § 45, https://www.law.cornell.edu/uscode/text/15/45.

[84] See Press Release, *BJ's Wholesale Club Settles FTC Charges*, Federal Trade Commission, (Jun. 16, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, *DSW Inc. Settles FTC Charges*, Federal Trade Commission, (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges; Press Release, *FTC Releases 2023 Privacy and Data Security Update*, Federal Trade Commission, (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update; Staff Report, *Start with Security: A Guide for Business*, Federal Trade Commission (Jul. 2017), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

that was unavoidable by consumers and not offset by countervailing benefits to consumers or competition. As just one example, earlier this year, the FTC brought an action against the security camera company Verkada for failure to take steps to prevent attackers from accessing video feeds from consumers' cameras.[85]

Beyond data security, the FTC has held companies responsible for how others use their products to cause harm to consumers.[86] For example, the FTC successfully sued QChex for violating Section 5 for allowing any customer to create checks for any bank account number without implementing reasonable safeguards to ensure that fraudsters were not creating checks for accounts they did not control. In that case, QChex's failure to take steps to prevent foreseeable harmful and illegal uses constituted an unfair business practice.

It is important to note that an obligation to identify and remediate likely harmful behaviors does not amount to strict liability for any harm caused by another bad actor using a company's product. Section 5's requirement that any harm not be offset by countervailing benefits to consumers or competition means that companies are not expected to spend unlimited resources to try to chase down potential offenders. Instead, the FTC only intervenes when companies fail to take cost-effective measures whose implementation would have prevented an even greater risk of injury.

Product design is also an important consideration in assessing the extent to which a company must take steps to remediate potential harm from bad faith actors. If the potential harms from a platform are especially significant, or the platform's design makes it likely that it will be used for harmful purposes, then companies should have a greater obligation to expend resources to remediate those uses. QChex, for example, allowed attackers to generate checks on consumers' bank accounts; given the high risk of substantial financial harm, the company had an obligation to ensure that the check writers in fact controlled those accounts and to monitor and respond to complaints of fraud. If a company creates a product that has a high likelihood of being used for illegitimate purposes, it should have a greater obligation to take

---

[85] See Press Release, *FTC Takes Action Against Security Camera Firm Verkada over Charges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act*, Federal Trade Commission, (Aug. 30, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other.

[86] See, e.g., Press Release, *FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions*, Federal Trade Commission, (Jun. 28, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-sues-walmart-facilitating-money-transfer-fraud-fleeced-customers-out-hundreds-millions; Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Federal Trade Commission, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims; Press Release, *Court Orders Permanent Halt to Illegal Qchex Check Processing Operation Court Finds Qchex Unfair Practices Created a Dinner Bell for FraudstersOperators to Give Up All Their Ill-Gotten Gains*, Federal Trade Commission, (Feb. 9, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/court-orders-permanent-halt-illegal-qchex-check-processing-operation-court-finds-qchex-unfair.

steps to account for those harms to ensure the harms do not outweigh any potential benefits to consumers from the product.[87]

As such, generative AI products that are likely to be predominantly used for harm — such as Rytr's review generation service or the voice impersonation companies we assessed — should have heightened obligations to address uses for illegal purposes (if they should be made commercially available at all). Those products are very likely to lead to significant consumer injury and consumers are unable to reasonably avoid them — to the contrary, the services are designed to create content that is indistinguishable from authentic content. There are limited positive use cases for these tools, so the harms caused by making these platforms generally available without reasonable safeguards in place is unlikely to be outweighed by countervailing benefits.

For more general purpose tools, the calculus is significantly more complicated. ChatGPT, for example, is a multipurpose system designed to respond to any number of constantly changing prompts — the cost of anticipating and responding to every potential abuse of the system is substantially higher. In fact, the developers of ChatGPT do consider potential misuse by bad actors and do put some limits on how the platform can be used. For example, ChatGPT regularly updates and publishes a system card identifying "Key Areas of Risk Evaluation & Mitigation," including "unauthorized voice generation" and "generating erotic and violent speech."[88] Further, making changes to account for harmful uses could also potentially constrain known or unknown positive uses of ChatGPT — another potential countervailing benefit that is less likely for narrower tools designed for specific tasks.

Nevertheless, there is a strong case that the developers of general purpose generative AI products should take more aggressive measures to prevent or deter obvious abuses (as discussed above, general purpose services comply with requests to generate multiple "fake reviews"). The extent to which such a multipurpose platform should take steps to respond to different threats is a complex question, balancing the costs of potential harm with the costs of remediation and potential limitations of beneficial uses. The same goes for platforms that host fraudulent content; if their services are causing significant harm and there are cost-effective measures they could employ to remediate that harm, they should do so.

Clarifying tool and platform responsibility for customer abuse could be done through enforcement under Section 5 and comparable state consumer protection laws. Or new legal protections could be enacted to specify what steps these companies should take and under what circumstances when their products are used to defraud consumers. For example, members of this Committee have introduced the Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act to prohibit the creation of deepfake digital replicas without

---

[87] Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Federal Trade Commission, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims.

[88] GPT-4o System Card, OpenAI, (Aug. 8, 2024), https://openai.com/index/gpt-4o-system-card/.

the subject's permission, and requiring platforms to remove unauthorized replicas upon notice.[89] The bill would give individuals greater rights over their personal identity and give platforms stronger incentives to remove unauthorized synthetic content. However, we are concerned that the current bill does not sufficiently deter bad faith takedown requests of legitimate, authentic media, as there is no counternotice procedure for affected speakers as exists under the Digital Millennium Copyright Act and the penalty for dishonest takedown requests is as low as $5,000 — a small price to pay for the rich and powerful to remove unwanted content for the internet. The bill's safe harbor for digital replica tools is also unduly broad, largely exempting tool developers from legal responsibilities except in the most narrow of circumstances — especially given the bill's broad preemption of state laws. And the bill could include stronger guardrails to ensure that people are not coerced or tricked into signing over the right to make digital replicas of them. Nevertheless, we are heartened to see Congress considering novel approaches to the very real problem of unauthorized digital replicas and we believe the NO FAKES bill could be an effective solution with additional targeted amendments.

Transparency obligations

As a general matter, consumers deserve to know whether the content they're interacting with is real or AI-generated. Content creators and companies should be labeling AI-generated content and chatbots as such. The fact that content is AI-generated should be communicated prominently and contextually in such a way that an ordinary consumers is likely to notice, through visual labeling (or in the case of AI-generated phone calls, through an introductory statement, as the FCC recently proposed in a rulemaking on AI-generated robocalls).[90] It should also be communicated latently through standardized metadata, watermarks, or other technology to allow platforms and agents to automatically identify content as synthetic — this approach was recently mandated in California in legislation enacted in September of last year.[91]

However, mandated transparency has limitations too, as bad actors will simply fail to provide prominent disclosures, and will endeavor to strip our latent identifiers imposed by generative platforms — or they will turn to smaller, malicious, or open-source platforms that are not covered by or otherwise do not comply with transparency obligations. For this reason, some advocates have argued against transparency obligations, noting that adversarial transparency

---

[89] Press Release, *Blackburn, Coons, Salazar, Dean, Colleagues Introduce "NO FAKES Act" to Protect Individuals and Creators from Digital Replicas*, Senator Marsha Blackburn, (Apr. 9, 2025), https://www.blackburn.senate.gov/2025/4/technology/blackburn-coons-salazar-dean-colleagues-introduce-no-fakes-act-to-protect-individuals-and-creators-from-digital-replicas.

[90] Comments of Consumer Reports on Implications on Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls and Robotexts, CG Docket No. 23-362, (Oct. 10, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/10/CR-Comment-on-FCC-AI-Robocall-Rulemaking-.pdf. 50,000 consumers signed onto our petition in support of our comments calling for transparency in AI-generated robocalls. *See* Grace Gedye, 50,000 consumers support FCC AI robocall rulemaking, Consumer Reports Advocacy, (Oct. 10, 2024), https://advocacy.consumerreports.org/research/50000-consumers-support-fcc-ai-robocall-rulemaking/.

[91] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.

obligations have historically been ineffective.[92] Nevertheless, we think there is a benefit in requiring transparency from actors who may be deterred from breaking the law, and over time content identification (including reliably authenticating when content is organic and legitimate) may improve.[93]

Stronger privacy and security laws

Scams are much more effective when attackers have access to personal information in order to customize a solicitation. However, the United States's privacy laws are weak, and hundreds of unregulated data brokers are able to amass detailed dossiers about all of us which are then sold to anyone willing to pay for them.[94]

The federal government has no comprehensive privacy law, and instead only has a handful of laws of varying strength covering sensitive categories of personal information such as medical, financial, and kids' data. Over the past six years, twenty states have passed their own general privacy laws, though most of those laws are too weak to meaningfully stem the flow of personal information to data brokers and advertisers.[95]

Policymakers should enact stronger privacy rules based on the principle of *data minimization* — meaning companies should only be collecting, processing, sharing, and retaining data as is reasonably necessary to deliver the goods or services requested by consumers.[96] Such a model would protect personal data *by default* rather than subject consumers to relentless requests for "opt-in" consent for superfluous data usage or forcing consumers to navigate innumerable "opt-out" mechanisms.[97]

---

[92] Jacob Hoffman-Andrews, *AI Watermarking Won't Curb Disinformation*, Electronic Frontier Foundation, (Jan. 5, 2024), https://www.eff.org/deeplinks/2024/01/ai-watermarking-wont-curb-disinformation.

[93] Grace Gedye, *CR submits testimony AI and consumer protection to New York Assembly*, Consumer Reports Advocacy, (Sep. 25, 2024), https://advocacy.consumerreports.org/research/cr-submits-testimony-ai-and-consumer-protection-to-new-york-assembly/.

[94] This Committee has published a detailed investigation into data brokers, though at this point the report is over ten years old. *See* Office of Oversight and Investigations Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Committee on Commerce, Science, and Transportation, (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. The situation has not materially improved in the meantime.

[95] *The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better*, Electronic Privacy Information Center and U.S. PIRG Education Fund, (Feb. 2024), https://publicinterestnetwork.org/wp-content/uploads/2024/01/State-of-Privacy-Feb.-2024.pdf.

[96] *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, Consumer Reports and the Electronic Privacy Information Center, (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[97] In 2021, Consumer Reports published model privacy legislation based on the concept of data minimization. *See Model State Privacy Act*, Consumer Reports Advocacy, (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf. Last year, Consumer Reports and the Electonic Privacy Information Center published a compromise approach based on the Connecticut privacy legislation that has served as a model for several other states. *See* Press Release, *Consumer Reports and the Electronic Privacy Information*

Whistleblower protections and incentives

Whistleblowers are often the only way the American public learns about the inner workings of our biggest companies — especially tech companies. Just last month, another Subcommittee of this Committee held a hearing highlighting Sarah Wynn-Williams — a former Facebook executive who recently published a book alleging sexual harassment and other misbehavior by senior management.[98] However, companies often do everything they can to stop such whistleblowers, both prophylactically through employee monitoring and non-disclosure and non-disparagement agreements and arbitration clauses in employment contracts, as well as after the fact through retaliation and legal threats. In the case of Ms. Wynn-Williams, Meta even went to court to try to block the sale and promotion of her book.[99]

Congress should enact whistleblower protections to protect insiders who publicly reveal corporate wrongdoing. Whistleblowers are especially needed in the AI space, as AI systems are notoriously inscrutable and difficult for outsiders to test and hold to account. Last year, whistleblowers from OpenAI and Google's DeepMind issued a public letter warning about the lack of safety and security protocols at those companies and criticizing the lack of legal protections for whistleblowers.[100] In 2020, Google effectively forced out a top AI ethics researcher for trying to publish a paper critiquing the kinds of algorithms (large language models) that Google uses; the paper pointed out some of the harms that can come from these models, as well as other ethical considerations concerning these algorithms.[101]

Whistleblower protections should include prohibitions on overbroad non-disclosure and non-disparagement provisions and dictate procedures for whistleblowers to escalate complaints within companies to be free from retaliation.[102] Legislation could also include incentives for

---

Center unveil new model legislation to protect the privacy of American consumers, Consumer Reports Advocacy, (Sep. 24, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-and-the-electronic-privacy-information-center-unveil-new-model-legislation-to-protect-the-privacy-of-american-consumers/.

[98] United States Committee on the Judiciary Subcommittee on Crime and Counterterrorism, *A Time for Truth: Oversight of Meta's Foreign Relations and Representations to the United States Congress*, Committee Activity and Hearings, (Apr. 9, 2025), https://www.judiciary.senate.gov/committee-activity/hearings/a-time-for-truth-oversight-of-metas-foreign-relations-and-representations-to-the-united-states-congress.

[99] Mike Isaac, Meta Seeks to Block Further Sales of Ex-Employee's Scathing Memoir, New York Times, (Mar. 12, 2025), https://www.nytimes.com/2025/03/12/technology/meta-book-sales-blocked.html.

[100] Pranshu Verma and Nitasha Tiku, *AI employees warn of technology's dangers, call for sweeping company changes,* Washington Post, (Jun. 4, 2024), https://www.washingtonpost.com/technology/2024/06/04/openai-employees-ai-whistleblowers/.

[101] Khari Johnson, *AI ethics pioneer's exit from Google involved research into risks and inequality in large language models*, VentureBeat, (Dec. 3, 2020), https://venturebeat.com/2020/12/03/ai-ethics-pioneers-exit-from-google-involved-research-into-risks-and-inequality-in-large-language-models.

[102] Nandita Sampath, *New Paper: Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Innovation Blog, (Oct. 13, 2022), at 23-24 (detailing whistleblower legislation recommendations)

insiders to report wrongdoing, such as *qui tam* provisions in False Claims Act cases and Internal Revenue System awards for people who report tax fraud. Last week, several members of this Committee introduced the bipartisan AI Whistleblower Protection Act which includes several of the protections just mentioned.[103]

Citizen education and better tools

Finally, consumers have a role to play too, and digital citizens will have to become more savvy and discriminating in a world where even very realistic looking and sounding content may be entirely AI-generated. For the last three years, Consumer Reports has published a "Cyber Readiness Report" which draws on nationally representative surveys to track the adoption of cybersecurity best practices over time.[104] While a majority of respondents did exhibit awareness of the importance of unique passwords, software updates, and multifactor authentication, adoption of more sophisticated techniques (such as use of password managers and tracker blockers) is lagging; moreover, adoption of cybersecurity best practices in general has remained fairly flat over the past three years. Institutions will need to adapt to find ways to encourage consumers to adopt more sophisticated protections over time, including protections designed to protect consumers from AI-generated deepfake scams. At the same time, researchers in industry, academia, civil society, and government will have to continue to develop new tools to help consumers identify inauthentic content. Over time, these tools need to become seamlessly embedded into browsers, mobile phone operating systems, and other platforms that consumers use to access online content.

No moratorium on state laws

The recent House budget reconciliation package included a provision that would prohibit states from enacting laws governing artificial intelligence for the next ten years.[105] Consumer Reports strongly opposes such a provision.[106] The states have been leaders on tech policy issues such as privacy for the past several years while Congress has failed to act. Despite stated concerns about a contradictory patchwork of state AI laws, in fact, relatively few laws have been passed that specifically regulate AI or automated decisionmaking. These laws have generally targeted real harms derived from the use of AI, such as the creation of deepfake

---

https://innovation.consumerreports.org/new-paper-opening-black-boxes-addressing-legal-barriers-to-public-interest-algorithmic-auditing/.

[103] Geoff Schweller, *Congress Introduces "Urgently Needed" AI Whistleblower Bill*, Whistleblower Network News, (May 15, 2025), https://whistleblowersblog.org/corporate-whistleblowers/congress-introduces-urgently-needed-ai-whistleblower-bill/

[104] Yael Grauer, *New Report: 2024 Consumer Cyber Readiness*, Consumer Reports Innovation Blog, (Oct. 1, 2024), at 4 https://innovation.consumerreports.org/new-report-2024-consumer-cyber-readiness/.

[105] Khari Johnson, Congress moves to cut off states' AI regulations, The Markup, (May 16, 2025), https://themarkup.org/artificial-intelligence/2025/05/16/congress-moves-to-cut-off-states-ai-regulations.

[106] Press Release, *Consumer Reports opposes AI state preemption language in House budget reconciliation bill*, Consumer Reports Advocacy, (May 12, 2025), https://advocacy.consumerreports.org/press_release/consumer-reports-opposes-ai-state-preemption-language-in-house-budget-reconciliation-bill/.

digital replicas and the use of blackbox decision-making systems to unfairly deprive individuals of opportunities. The language in the House budget resolution would reverse many of these protections, offer no federal protections to replace them, and prohibit the states from taking additional steps to protect their citizens. While artificial intelligence is a very promising field that can and will continue to deliver meaningful benefits for companies and consumers, simply invoking the term “AI” should not be *carte blanche* to avoid any regulation.

Thank you very much for the opportunity to testify today, and I look forward to answering your questions.