FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Technology Blog

# AI and the Risk of Consumer Harm

**By:** Staff in the Office of Technology and the Division of Advertising Practices

January 3, 2025

People often talk about “safety” when discussing the risks of AI causing harm. AI safety means different things to different people, and those looking for a definition here will be disappointed. These discussions can sometimes focus on the possibility of existential risk stemming from some sort of AI agent or cyborg of the future. But speculation about human extinction is well beyond the FTC’s immediate concerns. Instead, the FTC focuses on AI through the lens of our consumer protection and competition mission.

**The FTC is increasingly taking note of AI’s potential for real-world instances of harm—from incentivizing commercial surveillance to enabling fraud and impersonation to perpetuating illegal discrimination.**

Consumers are encountering AI systems and tools, whether they know it or not, from customer service chatbots, to educational tools, to recommendation systems powering their social media feeds, to facial recognition technology that could flag them as a security risk, and to tools that determine whether or on what terms they’ll get medical help, a place to live, a job, or a loan. Because there is no AI exemption from the laws on the books, firms deploying these AI systems and tools have an obligation to abide by existing laws, including the competition and consumer protection statutes that the FTC enforces. FTC staff can analyze whether these tools violate people’s privacy or are prone to adversarial inputs or attacks that put personal data at risk. We can also scrutinize generative AI tools that are used for fraud, manipulation, or non-consensual imagery, or that endanger children and others. We can consider the impacts of algorithmic products that make decisions in high-risk contexts such as health, housing, employment, or finance. Those are just a few examples, but the canvas is large.

The following examples from real-world, recent casework and other initiatives highlight the need for companies to consider these factors when developing, maintaining, using, and deploying an AI-based product:

1. **Taking necessary steps to prevent harm before and after deploying a product.** Last year the FTC alleged that retail pharmacy Rite Aid failed to take reasonable measures to prevent harm to consumers in its use of facial recognition technology (FRT) that falsely tagged consumers in its stores, particularly women and people of color, as shoplifters. For instance, the complaint alleged that the company failed to take reasonable steps to test, assess, measure, document, or inquire about the accuracy of its FRT before deploying the technology. The complaint further alleged that the company failed to take "reasonable steps" after deploying "to regularly monitor or test the accuracy of the technology." This included failing to "implement any procedure for tracking the rate of false positive facial recognition matches or actions taken on the basis of false positive facial recognition matches." The agency has highlighted that companies offering AI models need to assess and mitigate potential downstream harm before and during deployment of their tools, which includes addressing the use and impact of the technologies that are used to make decisions about consumers.

2. **Taking preventative measures to detect, deter, and halt AI-related impersonation, fraud, child sexual abuse material, and non-consensual intimate imagery.** Earlier this year, the FTC finalized a rule to combat impersonation of governments and businesses, which can be turbocharged with AI-generated deepfakes. Relatedly, the FTC launched a Voice Cloning Challenge to promote the development of ideas to protect consumers by detecting and halting the misuse of voice cloning software by unauthorized users. In announcing the challenge, FTC staff discussed considerations including applying effective real-time detection or monitoring measures, using solutions to evaluate existing content, preventing and deterring AI-enabled scams and fraud, and leveraging solutions to build robust guardrails that provide authentication or prevent upstream harm.

   While generative AI technology may be relatively recent, these harms are not new for the FTC. The agency has discussed deepfakes at PrivacyCon and in its Combatting Online Harms Report to Congress. The agency also took action against MyEx.com, a revenge porn site, that resulted in a court order permanently shutting down the website and requiring the operators pay harmed consumers for illegally posting their intimate images and personal information without their consent and extorting them by charging takedown fees.

3. **Avoiding deceptive claims about AI tools that result in people losing money or put users at risk of harm.** The FTC has brought a number of cases involving deceptive claims that an AI product would help people start a business or make money, including the cases recently announced as part of Operation AI Comply. Even more recent are actions against Evolv Technologies for deceptive claims about an AI-enabled security screening product, Intellivision Technologies for deceptive claims

about its facial recognition software, and accessiBe for misrepresentations about its AI-powered web accessibility tool. Earlier in the year, the FTC banned NGL Labs and its founders from offering anonymous messaging apps to kids and teens under 18 and halted claims around AI-related content moderation that the Commission alleged were deceptive. In its complaint against Everalbum, a photo app developer, the FTC alleged that the company deceived users who deactivated their accounts about the use and retention of their photos and videos and enabled face recognition by default, failing to give consumers the ability to disable it. In terms of biometric and health data, the agency has also challenged companies for allegedly baseless claims around algorithmic solutions and accuracy of their genetic DNA testing reports (CRI Genetics, LLC), and claims that mobile apps could detect symptoms of melanoma, even in its early stages (MelApp and Mole Detective).

4. **Ensuring privacy and security by default.** Generative AI tools require a massive amount of data inputs as part of the training process for large language models, among other types of AI models. Some of this data may be highly sensitive. The Commission has a long record of providing guidance to businesses about ensuring data security and protecting privacy, including via its Policy Statement on Biometric Information. The FTC has also sued companies that failed to abide by their legal obligations. For example, the FTC issued a complaint against Amazon's voice assistant service, Alexa, over the company's default settings to retain users' (including children's) voice recordings indefinitely. The agency alleged that Amazon "misled Alexa users about their ability to delete voice recordings collected by Alexa" and used the data it unlawfully retained to help improve its Alexa algorithm. FTC staff have also advised that companies shouldn't quietly or surreptitiously change their terms of service.

The actions above are not a comprehensive overview of what companies should be considering when they design, build, test, and deploy their own products and services to millions of customers. Each case illustrates how the FTC's enforcement efforts encompass both the claims that companies make about their own products and services and the actions they take to ensure that they do not cause harm to consumers and violate laws enforced by the Commission.

In this blog post, we're not covering the agency's other important work relating to AI, including concerns relating to competition. Chair Khan previously outlined several relevant principles that agency staff is keeping in mind: highlighting how business models drive incentives; aligning liability with capability and control; and crafting effective remedies that establish bright-line rules on the development, use, and management of AI inputs. AI will continue to evolve in ways that will reveal both the benefits and the risks of technology, and effectively mitigating those risks can help spur those benefits. Companies can use AI tools in ways that have serious impacts on consumers, so they need to address associated risks before, during, and after consumers come in contact with them. As firms think about their own approach to developing, deploying, and maintaining AI-based systems, they should be considering the risks to consumers that each of them carry in the here-and-now, and take steps to proactively protect the public before their tools become a future FTC case study.

*Thank you to those who contributed to this post: Michael Atleson, Shoshana Wodinsky, Stephanie Nguyen, Dan Salsburg, Leah Frazier, Mark Suter, Sam Levine.*

**Tags:** Technology | Artificial Intelligence | Office of Technology

More from the Technology Blog

Technology Blog

Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans

Staff in the Office of Technology & the Division of Privacy and Identity Protection | December 13, 2024

Technology Blog

Solving the Traveling Salesman Problem? Not quite, but here are more research questions from the Office of Technology

Staff at the Office of Technology | December 4, 2024

Technology Blog

Unpacking Real Time Bidding through FTC's case on Mobilewalla

Staff in the Office of Technology & Division of Privacy and Identity Protection | December 3, 2024

Technology Blog

Data Clean Rooms: Separating Fact from Fiction

Staff in the Office of Technology and the Division of Privacy and Identity Protection | November 13, 2024