Center for AI and Digital Policy

ChatGPT and the Federal Trade Commission: Still No Guardrails

Center for AI and Digital Policy
Washington, DC

July 2024

TABLE OF CONTENTS

I. Executive Summary

More than a year ago, the Center for AI and Digital Policy (CAIDP) filed a detailed, formal complaint with the Federal Trade Commission (FTC) about OpenAI, alleging that OpenAI had violated U.S. consumer protection law by releasing a consumer product without sufficient safeguards. CAIDP urged the FTC to act to protect consumers and ensure independent oversight of OpenAI and other AI companies.[1] In July 2023, both the New York Times and the Wall Street Journal reported that the FTC had launched the investigation sought by CAIDP. However, a year later, there is still no legal outcome, no judgment, and no settlement. There are Still No Guardrails for AI products sold to consumers in the United States.

The CAIDP OpenAI case is likely the most consequential AI investigation currently pending before the FTC. It could establish safeguards for AI services and bring transparency and accountability to the AI industry. Regulators in several other jurisdictions recognize these concerns and have acted. The urgency of the OpenAI case is underscored also by the absence of new federal laws in the United States to address new challenges resulting from the deployment of AI services. Unlike many other countries in the world,[2] the United States has still not enacted legislation to address public concerns even though polling data shows widespread concern in the U.S.

The purpose of this report *Still No Guardrails* is to review developments since the filing of CAIDP's original OpenAI complaint. Relevant is the range of enforcement actions initiated in other jurisdictions for the same concerns highlighted in our complaint. Alarming is the repeated warnings from AI experts. Obvious is the growing concern about the lack of governance and oversight of AI companies, particularly OpenAI.

In this document we set out an overview of our efforts to get the FTC to establish guardrails for AI. We highlight the accelerated deployment of OpenAI's large language model (LLM) GPT-4, the growing consumer concerns over AI, the views of AI experts, the FTC's mandate and prior statements on AI, and the need for the Federal Trade Commission to act.

---

[1] Merve Hickok, Christabel Randolph, Marc Rotenberg, *It's time for the FTC to act on ChatGPT*, Opinion, (Jun. 14, 2024), https://thehill.com/opinion/technology/4722343-its-time-for-the-ftc-to-act-on-chatgpt/

[2] See, e.g., European Parliament, *The First Regulation on Artificial Intelligence,* (Jun. 18, 2024), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

II. Overview of the CAIDP Complaint to FTC re OpenAI and ChatGPT

In March 2023, CAIDP filed a detailed consumer complaint with the Federal Trade Commission (FTC) regarding ChatGPT and OpenAI. In the Complaint, the Supplements that followed, and appearances before the Commissioners at open Commission meetings, CAIDP set out the many problems with OpenAI's business practices and pointed to the FTC's previously issued guidance on AI products. CAIDP asked the Commission to halt the commercial release of new GPT models until necessary safeguards were established. CAIDP also said that such safeguards should be based on the FTC's previously issued guidance on AI products.

Summary of the CAIDP Complaint[3]

In the original Complaint, CAIDP explained that OpenAI released a product GPT-4 for the consumer market that is biased, deceptive, and a risk to privacy and public safety. OpenAI released AI-based products, DALL-E, GPT-4, OpenAI Five, ChatGPT, and OpenAI Codex for commercial use. OpenAI described these AI models as "products." OpenAI provided "pricing information" corresponding to the subscription levels. There was also downstream integration offered by OpenAI – plugins for GPT-4 was made available for routine consumer services, including travel, finance, and shopping.

The CAIDP Complaint quoted extensively from the GPT-4 Technical Report in which OpenAI acknowledged the specific dangers of "Disinformation and influence operations," "Proliferation of conventional and unconventional weapons," and "Cybersecurity." The Complaint highlighted that the outputs of ChatGPT cannot be proven or replicated. No independent assessment was undertaken prior to deployment.

CAIDP also relied on scientific evidence to highlight specific risks of bias, deception, harms to children, privacy, cybersecurity, and consumer protection. The Complaint set out established frameworks for AI governance – the OECD AI Principles, the Universal Guidelines for AI, which recommend the guardrails sought as relief in our complaint.

CAIDP emphasized that there should be independent oversight and evaluation of commercial AI products offered in the United States prior to release in the market. The specific relief sought in our complaint was:

- Halt further commercial deployment of GPT by OpenAI;

[3] CAIDP, *Complaint to the FTC - In re OpenAI and ChatGPT*, (Mar. 30, 2024), https://www.caidp.org/app/download/8450269463/CAIDP-FTC-Complaint-OpenAI-GPT-033023.pdf

- Require the establishment of independent assessment of GPT products prior to future deployment;
- Require compliance with FTC AI Guidance prior to further deployment of GPT
- Require independent assessment throughout the GPT AI lifecycle
- Establish a publicly accessible incident reporting mechanism for GPT-4 similar to the FTC's mechanisms to report consumer fraud;
- Initiate a rulemaking to establish baseline standards for products in the Generative AI market sector; and
- Provide such other relief as the Commission finds necessary and appropriate.

Summary of the First Supplement[4]

In the first Supplement, CAIDP highlighted that subsequent to the filing of the Complaint, consumer agencies around the world launched investigations of ChatGPT and AI experts called for regulation of AI services. The supplement covered the enforcement actions initiated in Italy, Canada, France, Australia, Germany, Spain, Japan, and the UK.

The First Supplement provided additional evidence from AI experts. It highlighted calls for regulation by federal agencies like CISA, NSA, and Department of Defense's Chief AI and Digital Officer who warned about the potential for generative artificial intelligence systems like ChatGPT to deceive citizens and threaten national security. The CAIDP Supplement cited corporate policies of Amazon, Samsung, Bank of America, Goldman Sachs, Wells Fargo, Citigroup and Deutsche Bank restricting employees from using ChatGPT due to privacy and data security concerns.

The First Supplement restated the prayer for relief sought in the Complaint. CAIDP urged the FTC to act without delay.

Summary of the Second Supplement[5]

In the Second Supplement, CAIDP described additional enforcement actions initiated in Korea, Brazil, Netherlands, Poland. The Second Supplement highlighted the aggressive business practices of OpenAI, contrary to warnings and cautions regarding accelerated deployment by AI experts. For example, OpenAI released GPTbot to scrape

[4] CAIDP, *Supplement to the Original Complaint to the FTC - In re OpenAI and ChatGPT,* (Jul. 10, 2023), https://www.caidp.org/app/download/8466615863/CAIDP-FTC-Supplement-OpenAI-07102023.pdf

[5] CAIDP, *Second Supplement to the Original Complaint to the FTC - In re OpenAI and ChatGPT,* (Nov. 14, 2023), https://www.caidp.org/app/download/8485816363/CAIDP-Supplement-FTC-OpenAI-11142023.pdf

the entire internet and the absence of any provenance measures for DALL-E3 and the propensity for generating 'racy content'.

Given the text to image capabilities being commercialized by OpenAI, the Second Supplement expanded upon the risks to democracy and elections, public safety risks, consumer concerns over deepfakes, voice clones, biometric privacy, fraud, and copyright abuse.

In the Second Supplement, CAIDP summarized a spate of class action lawsuits against OpenAI concerning the lack of transparency and unfair data practices. CAIDP also highlighted OpenAI's expansion of GPT-4 integration and the launch of voice, image capabilities of ChatGPT. CAIDP explained that these business practices raise concerns under FTC's Policy Statement on Biometric Information.

CAIDP urged the FTC to act. CAIDP cited OpenAI's accelerated deployment of GPT-4 notwithstanding documented and admitted risks is contrary to OpenAI's commitments to the administration and FTC's own business guidance.

II. The FTC Investigation into ChatGPT

In July 2023, the New York Times reported that the FTC had launched the investigation into OpenAI and ChatGPT sought by the Center for AI and Digital Policy.[6] The detailed document request made public by the Washington Post also indicated that the FTC identified copyright concerns in addition to the privacy and security risks CAIDP highlighted in its complaint.[7] The Wall Street Journal (WSJ) reported "In a civil subpoena to the company made public Thursday, the FTC says its investigation of ChatGPT focuses on whether OpenAI has "engaged in unfair or deceptive practices relating to risks of harm to consumers, including reputational harm."[8]

[6] New York Times, *F.T.C. Opens Investigation Into ChatGPT Maker Over Technology's Potential Harms,* (Jul. 13, 2023), https://www.nytimes.com/2023/07/13/technology/chatgpt-investigation-ftc-openai.html

[7] The Washington Post, *FTC investigates OpenAI over data leak and ChatGPT's inaccuracy*, (Jul. 13, 2023), https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/

[8] The Wall Street Journal, *ChatGPT Comes Under Investigation by the Federal Trade Commission*, (Jul.13, 2023), https://www.wsj.com/articles/chatgpt-under-investigation-by-ftc-21e4b3ef

In the document[9] made public by Washington Post, the FTC asked OpenAI to provide information about the data practices underlying the training of its large language model (LLM), the pre-release safety and risk assessment measures, the company's consumer marketing and advertising practices, its handling of users' personal information, and how the company offers downstream integrations of its GPT-4 product.

However, since that initial report of the investigation there is no further information on the investigation. The FTC's silence and delay is all the more troublesome because OpenAI, like many big tech firms, is cutting safety and security teams at the same time competition is increasing. Remarkably, experts inside and outside the company warn that the problems are far greater than the public is aware.[10]

IV. Consumer Concern over ChatGPT and LLM commercialization

When OpenAI released ChatGPT into the market, there were only 11 plugins available.[11] In a little over the year, the commercialization of its LLM GPT-4 has increased exponentially.

Accelerated commercialization and deployment

When the Washington Post reported on FTC investigating OpenAI, it noted "Analysts have called OpenAI's ChatGPT the fastest-growing consumer app in history, and its early success set off an arms race among Silicon Valley companies to roll out competing chatbots."[12]

AI products are evolving rapidly and being deployed downstream in consumer facing services. For example, ChatGPT is integrated with Snapchat used by many children and OpenAI has released GPTs which allows customization for any direct consumer use.

---

[9] Federal Trade Commission, *Civil Investigative Demand Schedule*, (FTC File No. 232-3044), https://www.washingtonpost.com/documents/67a7081c-c770-4f05-a39e-9d02117e50e8.pdf?itid=lk_inline_manual_4

[10] Merve Hickok, Christabel Randolph, Marc Rotenberg, *It's time for the FTC to act on ChatGPT*, Opinion, (Jun. 14, 2024), https://thehill.com/opinion/technology/4722343-its-time-for-the-ftc-to-act-on-chatgpt/

[11] CAIDP, *Complaint to the FTC - In re OpenAI and ChatGPT*, (Mar. 30, 2024), para.9 https://www.caidp.org/app/download/8450269463/CAIDP-FTC-Complaint-OpenAI-GPT-033023.pdf

[12] The Washington Post, *FTC investigates OpenAI over data leak and ChatGPT's inaccuracy*, (Jul. 13, 2023), https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/

ChatGPT's now augmented, multi-modal capabilities pose a significant threat to consumer safety, public safety, and election integrity.[13]

Following a proposed ban on using news publications and books to train AI chatbots in the U.K., OpenAI submitted a plea to the House of Lords communications and digital committee stating that it would be "impossible" to train AI models without using copyrighted materials, and that they believe copyright law "does not forbid training."[14]

Currently, OpenAI APIs are integrated into platforms such as Quizlet with more than 60 million students using it to study,[15] OpenAI launched a GPT store,[16] announced a new model GPT-4o that is multi-modal in input and output.[17] There are reports of GPT store being filled with spam and "several GPTs ripped from popular movie, TV and video game franchises"[18] and most recently, the eerie similarity of GPT-4o "Sky" voice with that of Scarlett Johansson resurfaced existing concerns over the business practices of AI companies in training their AI models.[19]

The Atlantic, Vox Media, Slack, Reddit, GitHub deals also show the aggressive commercialization practices that will now by default opt-in user data to train AI models.[20] What is more insidious is the anthropomorphization[21] of these systems which further augments the "dark pattern" effect and deceptive potential of GPT-4 tools.

---

[13] Statement of CAIDP and Encode Justice Re the FTC OpenAI Investigation, (Jan. 18, 2024), https://www.linkedin.com/posts/center-for-ai-and-digital-policy_aigovernance-consumerprotection-delayiscostly-activity

[14] TechCrunch, *ChatGPT: Everything you need to know about the AI-powered chatbot,* (Jun.17, 2024), https://techcrunch.com/2024/06/17/chatgpt-everything-to-know-about-the-ai-chatbot/

[15] OpenAI, *Introducing APIs for GPT-3.5 Turbo and Whisper*, (Apr. 24, 2024), https://openai.com/index/introducing-chatgpt-and-whisper-apis/

[16] OpenAI, *Introducing the GPT Store,* (Jan. 10, 2024), https://openai.com/index/introducing-the-gpt-store/

[17] OpenAI, *Hello GPT-4o,* (May 13, 2024), https://openai.com/index/hello-gpt-4o/

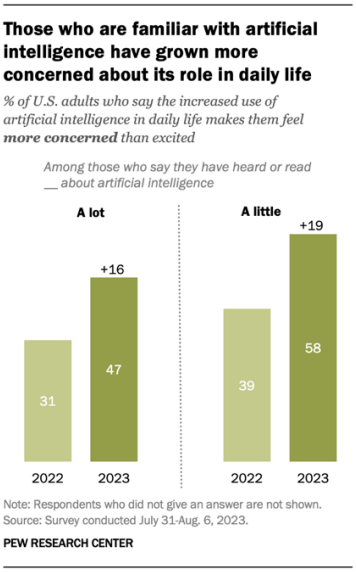
[18] TechCrunch, *OpenAI's chatbot store is filling up with spam,* (Mar. 20, 2024), https://techcrunch.com/2024/03/20/openais-chatbot-store-is-filling-up-with-spam/

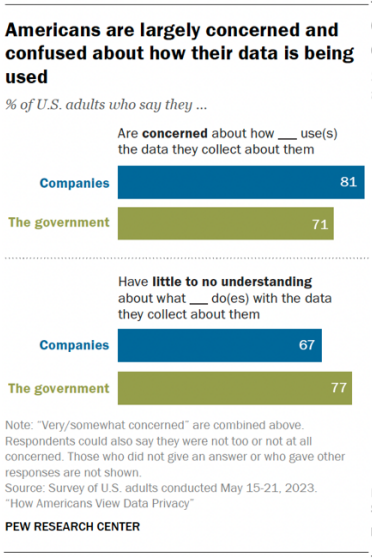
[19] New York Times, *Scarlett Johansson's Statement About Her Interactions With Sam Altman,* (May 20, 2024), https://www.nytimes.com/2024/05/20/technology/scarlett-johansson-openai-statement.html

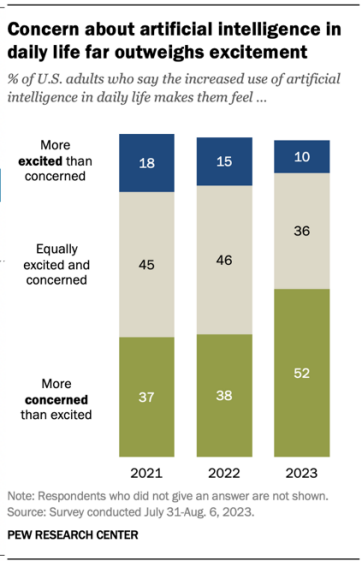
[20] TechCrunch, *ChatGPT: Everything you need to know about the AI-powered chatbot,* (Jun.17, 2024), https://techcrunch.com/2024/06/17/chatgpt-everything-to-know-about-the-ai-chatbot/

[21] Axios, *GPT-4o delivers human-like AI interaction with text, audio, and vision integration*, (May 14, 2023), https://www.artificialintelligence-news.com/2024/05/14/gpt-4o-human-like-ai-interaction-text-audio-vision-integration/

Public Opinion Surveys







The Pew Research Center in August 2023 reported that "Of those who have heard of ChatGPT, majorities of Democrats and Republicans say their greater concern is not enough regulation."[22] Just two months later in October 2023 Pew surveys showed that, "People's views on artificial intelligence (AI) are marked with distrust and worry about their data…As AI raises new frontiers in how people's data is being used, unease is high. Among those who've heard about AI, 70% have little to no trust in companies to make responsible decisions about how they use it in their products."[23]

The Pew polls all show growing public support for the regulation of AI products and services. "Democrats and Republicans alike are more concerned about insufficient government regulation of chatbots than excessive regulation."[24] Of those polled, 67% said the government would not go far enough to safeguard the public.

[22] Pew Research Center, *Most Americans haven't used ChatGPT; few think it will have a major impact on their job*, (Aug. 28, 2023), https://www.pewresearch.org/short-reads/2023/08/28/most-americans-havent-used-chatgpt-few-think-it-will-have-a-major-impact-on-their-job/
[23] Pew Research Center, *How Americans View Data Privacy*, (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/
[24] Pew Research Center, *Democrats and Republicans alike are more concerned about insufficient government regulation of chatbots than excessive regulation* (Aug. 28, 2023), https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/sr_23-11-21_ai-roundup_5-png/

Advocacy of EU Consumer Groups

On the other side of the Atlantic, following the CAIDP complaint to the FTC, the European Consumer Organisation (BEUC) called for EU and national authorities to launch an investigation into ChatGPT and similar chatbots.[25] The Norwegian Consumer Council (NCC) released an extensive report on the consumer harms of generative AI products which CAIDP cited in its supplementary complaint.[26] In the press release accompanying the report, the NCC stated "As long as the EU's AI Act is not applicable, authorities need to investigate where new generative AI-driven products and services may be harming consumers and enforce existing data protection, safety and consumer protection legislation."[27]

In March 2024, BEUC – the European consumer organization released the report on "Digital Fairness for Consumers"[28] which carefully lays out the agility required from consumer protection law to address economic and non-economic harm to consumers in the digital environment and considering the "engineering of consumer behavior" through AI systems.

V. Growing Concerns relating to OpenAI

As more individuals use AI to seek relationship advice, medical information or psychological counseling, experts say the risks to individuals are growing. In addition to potentially sharing specific pieces of data, generative AI tools can draw connections, or inferences providing a chillingly detailed understanding of our personhood.[29]

Amidst these growing concerns over accelerated commercialization of generative AI systems, the events surrounding OpenAI's leadership in November last year signals

[25] BEUC, *Investigation by EU authorities needed into ChatGPT technology,* (Mar. 30, 2023), https://www.beuc.eu/press-releases/investigation-eu-authorities-needed-chatgpt-technology
[26] CAIDP, *Supplement to the Original Complaint to the FTC - In re OpenAI and ChatGPT,* (Jul. 10, 2023), para. 110, https://www.caidp.org/app/download/8466615863/CAIDP-FTC-Supplement-OpenAI-07102023.pdf
[27] FORBRUKERRADET, *New report: Generative AI threatens consumer rights,* (Jun. 20, 2023), https://www.forbrukerradet.no/side/new-report-generative-ai-threatens-consumer-rights/
[28] BEUC, *Digital Fairness for Consumers*, (Mar. 2024), https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf
[29] Axios, *Generative AI's privacy problem,* (Mar. 14, 2024), https://www.axios.com/2024/03/14/generative-ai-privacy-problem-chatgpt-openai

the growing governance concerns relating to concentration of power both within and outside the company.[30]

Concerns on internal governance

Those most closely associated with OpenAI are now warning about a culture of recklessness and secrecy at the company at the same time it is racing to build the most powerful A.I. systems ever created.[31] Just this month, the New York Times reported,

> The members say OpenAI, which started as a nonprofit research lab and burst into public view with the 2022 release of ChatGPT, is putting a priority on profits and growth as it tries to build artificial general intelligence, or A.G.I., the industry term for a computer program capable of doing anything a human can.
>
> They also claim that OpenAI has used hardball tactics to prevent workers from voicing their concerns about the technology, including restrictive nondisparagement agreements that departing employees were asked to sign.[32]

Several current and former OpenAI and Google DeepMind employees warned about the lack of oversight for the artificial intelligence industry in a recent public letter.[33] The letter states "AI companies possess substantial non-public information about the capabilities and limitations of their systems, the adequacy of their protective measures, and the risk levels of different kinds of harm." This letter has been endorsed by leading AI experts Yoshua Bengio, Geoffrey Hinton, and Stuart Russell.

The letter from OpenAI employees echoed concerns raised by Helen Toner, a former OpenAI board member. Toner stated in an interview that OpenAI CEO Sam Altman was fired by the former board of directors because he provided inaccurate information about safety mechanisms, did not clear major product releases with the board and kept related investments confidential.[34]

---

[30] Dave Lee, *Sam Altman Exposes the Charade of AI Accountability,* Opinion, Bloomberg, (Nov. 20, 2023), https://www.bloomberg.com/opinion/articles/2023-11-20/openai-sam-altman-exposes-the-charade-of-ai-accountability

[31] The New York Times, *Insiders Warn of a 'Reckless' Race for Dominance*, The Shift, (Jun. 5, 2024), https://www.nytimes.com/2024/06/04/technology/openai-culture-whistleblowers.html

[32] *Id.*

[33] A Right to Warn about Advanced Artificial Intelligence, https://righttowarn.ai

[34] Merve Hickok, Christabel Randolph, Marc Rotenberg, It's time for the FTC to act on ChatGPT, Opinion, (Jun. 14, 2024), https://thehill.com/opinion/technology/4722343-its-time-for-the-ftc-to-act-on-chatgpt/

Concerns on safety policies and practices

The widely reported concerns about a culture of gagging and chilling speech affects not only employment practices but safety assessments and evaluations -critical for advancing safe, secure, and trustworthy AI. The concerns of employees and insiders are mirrored by concerns on assurances of red-teaming and safety testing at AI companies. OpenAI's current usage policy prohibits outside researchers from intentionally circumventing safeguards and mitigations "unless supported by OpenAI," and yet advocates for AI companies like OpenAI to create more opportunities for researchers to scrutinize their models. OpenAI does deploy a network of third-party red teamers to conduct adversarial research of their models, but researchers must apply to be part of the program, and OpenAI ultimately sets the rules of engagement. [35]

MIT led an open call by 350+ AI, legal, and policy experts for "A Safe Harbor for Independent AI Evaluation" citing concerns over current practices and policies of AI companies that can chill independent evaluation.[36]

VI. Enforcement in other jurisdictions

Overall, there have been **over a dozen** investigations of OpenAI in different countries, targeting various aspects of its services.[37] The range of enforcement actions can be categorized into three broad clusters:

- **Consumer Data Privacy**: Privacy violation due to the collection and processing of data to train AI models.
- **Inaccurate Content**: Harm arising from inaccurate content generated by OpenAI services.
- **Competition**: Consolidation of market share through Microsoft's investment in OpenAI.

Even where enforcement actions have not yet concluded, investigations act as important information collection mechanisms for regulators to clarify the practices of OpenAI and other AI services and to prepare for more targeted legal standards. Significantly, these actions demonstrate that consumer protection and competition

[35] Cyberscoop, *AI companies promise to protect our elections. Will they live up to their pledges?,* (May 15, 2024), https://cyberscoop.com/ai-companies-election-transparency/
[36] A Safe Harbor for Independent AI Evaluation, https://sites.mit.edu/ai-safe-harbor/
[37] Stephanie Psaila, *Governments vs ChatGPT: Investigations around the world*, DIPLO (Jun. 16, 2023), https://www.diplomacy.edu/blog/governments-chatgpt-investigations/.

enforcement are not alternative choices but rather complementary routes for ensuring consumer safeguards and preventing market concentration.

Since the launch of ChatGPT in 2022, Data Protection Authorities (DPAs) in France, Germany, Italy, Ireland, Netherlands, Poland, and Spain have all initiated their respective investigation against ChatGPT.[38] Other countries, including Canada and Brazil, have also initiated their investigations based on their own data security laws in response to public complaints.[39] The Canadian complaint focused on the use and collection of data without consent, while the Brazilian complaint focused on accessing personal data retained by ChatGPT and information about how they are utilized.[40] There have been no further updates since these countries launched their investigations in 2023.

Inaccurate content generated by AI models also comes under the purview of EU data privacy laws. For instance, the GDPR[41] requires data processor to accurately process personal data and grants data subjects the right to rectify incorrect personal data.[42] Inaccurate content generated by AI models could violate Art. 5, while the inability to rectify personal data may go against data subjects' right to rectify.

OpenAI has an "extended partnership" with Microsoft. Since 2019, OpenAI has received over $13 billion in investment from Microsoft.[43] The two companies also cooperate in supercomputing, AI service, and cloud service.[44] Such deals have raised concerns about whether Microsoft has effectively acquired OpenAI or achieved

[38] See Psaila, supra note 37; Reuters, *Dutch privacy watchdog seeks information from OpenAI, flags concerns*, (Jun. 7, 2023), https://www.reuters.com/technology/dutch-privacy-watchdog-seeks-information-openai-flags-concerns-2023-06-07/; TechCrunch, *Poland opens privacy probe of ChatGPT following GDPR complaint*, (Sept. 21, 2023), https://techcrunch.com/2023/09/21/poland-chatgpt-gdpr-complaint-probe/.

[39] Office of the Privacy Commissioner of Canada [OPC], *OPC launches investigation into ChatGPT*, (Apr. 4, 2023), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/; Pedrp Spadoni, *Após denúncia, agência brasileira vai fiscalizar ChatGPT*, Olhar Digital (Jul. 26, 2023), https://olhardigital.com.br/2023/07/26/seguranca/agencia-brasileira-vai-fiscalizar-chatgpt-apos-denuncia/.

[40] OPC, supra note 16; Luca Belli, *Why ChatGPT does not comply with the Brazilian Data Protection Law and why I petitioned the Regulator*, MEDIANAMA (May 25, 2023), https://www.medianama.com/2023/05/223-chatgpt-brazilian-data-protection-law-ai-regulation/.

[41] 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC [hereinafter GDPR]

[42] GDPR arts. 5(1)(d), 16.

[43] See Jason Karaian, *Microsoft's Stock Hits Record High After Hiring OpenAI Outcasts*, The New York Times (Nov. 20, 2023), https://www.nytimes.com/2023/11/20/business/microsoft-stock-openai.html.

[44] Microsoft, *Microsoft and OpenAI extend partnership*, Microsoft Corporate Blogs (Jan. 23, 2023), https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/.

dominance within the AI market. In the United States, the Federal Trade Commission has launched a general inquiry into generative AI investments and is reported to specifically launch an antitrust investigation of the OpenAI-Microsoft partnership.[45]

Both the United Kingdom and the European Union have initiated early-stage reviews of the partnership, based on their respective antitrust laws. In December 2023, the Competition and Markets Authority of the UK, its principal antitrust regulator, announced that it was inviting public comments on the OpenAI-Microsoft partnership.[46] The investigation focused on whether Microsoft's investment in OpenAI constitutes a merger under the UK Enterprise Act of 2002, and whether the partnership substantially hindered market competition.[47] The UK CMA has since not issued any updates.

Similarly, in January 2024, the European Commission officials signaled that it was considering whether Microsoft's investment in OpenAI would be subject to review under the EU merger rule, as well as the market impact of the OpenAI-Microsoft partnership.[48] In April 2024, Reuters reported that the investment would avoid a formal EU merger review, but Microsoft could still face an antitrust investigation.[49]

Example #1: Italy's Enforcement against OpenAI

Italy was the first to take enforcement action against OpenAI. The Garante, Italy's DPA, launched its investigation of OpenAI in March 2023 and *temporarily banned ChatGPT* in Italy.[50] The enforcement action was initiated after a data breach of ChatGPT user information on March 20, 2023.

---

[45] FTC, *FTC Launches Inquiry into Generative AI Investments and Partnerships*, Press Release, (Jan. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships; Matt O'Brien, *US antitrust enforcers will investigate leading AI companies Microsoft, Nvidia and OpenAI*, AP (Jun. 6, 2024), https://apnews.com/article/nvidia-openai-microsoft-ai-antitrust-investigation-ftc-doj-0adc9a4a30d4b581a4f07894473ba548.

[46] Competition and Markets Authority, *Microsoft / OpenAI partnership merger inquiry*, GOV.UK (Dec. 8, 2023), https://www.gov.uk/cma-cases/microsoft-slash-openai-partnership-merger-inquiry.

[47] Id.

[48] European Commission, *Commission launches calls for contributions on competition in virtual worlds and generative AI*, (Jan. 9, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_85.

[49] Foo Yun Chee, *Exclusive: Microsoft's OpenAI partnership could face EU antitrust probe, sources say*, Reuters, https://www.reuters.com/technology/microsofts-openai-partnership-could-face-eu-antitrust-probe-sources-say-2024-04-18/

[50] Garante per la protezione dei dati personali [GPDP], *Artificial intelligence: stop to ChatGPT by the Italian SA*, (Mar. 31, 2023), https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9872832.

The announcement alleged several data privacy violations of ChatGPT, including:

- the lack of user access to information about what and how personal data are collected and used (GDPR Art. 12);
- the collection of personal information without legal basis (GDPR Art. 5);
- the processing of inaccurate personal information (GDPR Art. 6), and;
- the lack of age verification system (GDPR Art. 8).[51]

Along with the ban, the Garante has required OpenAI to clarify its GDPR compliance measures and implement a series of compliance measures, such as:

- Implement an age verification system by September 2023 that filters users under 13 and users between 13 to 18 without parental consent.
- Provide accessible notice on the OpenAI website on how data are processed for the operation of ChatGPT, as well as the data subjects' rights (users and non-users).
- Remove all reference to "contractual performance," which is a legal basis for processing data under GDPR Art. 6, and rely instead on "consent" or "legitimate interests" as the legal basis for processing data.
- Create a mechanism for data subjects, including users and non-users, to submit objection to the processing of personal data, and request rectification or erasure of personal data.[52]

As a result, OpenAI announced its improvement measures, including displaying required information on its website, and adding options for EU ChatGPT users to remove personal data or opt out of using their own data to train AI models through ChatGPT's privacy portal.[53] OpenAI has also implemented an age verification feature for Italian users later in 2023.[54]

The Garante lifted the temporary ban on April 28, 2023, after OpenAI "addressed or clarified" concerns of the Garante.[55] In its press release after lifting the ban, the Garante

---

[51] *Id.*
[52] GPDP, *ChatGPT: Italian SA to lift temporary limitation if OpenAI implements measures*, (Apr. 12, 2023), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751.
[53] GPDP, *ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for European users and non-users*, (Apr. 28, 2024), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490.
[54] Frank Hersey, *ChatGPT adds age verification in Italy to satisfy privacy enforcement*, MLEX (Oct. 13, 2023), https://mlexmarketinsight.com/news/insight/chatgpt-adds-age-verification-in-italy-to-satisfy-privacy-enforcement.
[55] GPDP, *supra* note 27.

welcomed the changes made by OpenAI, but vowed to continue its factfinding on OpenAI's compliance.[56]

In January 2024, the Garante concluded that available evidence showed that OpenAI *has violated* several GDPR provisions but did not specify the provisions violated in the announcement.[57]

In addition, after OpenAI launched Sora, its new text-to-video AI model, in March 2024, Garante launched another investigation to request clarification from OpenAI.[58] The Italian DPA required OpenAI to provide information on whether the new AI model will be available to EU users, how data is collected, processed, and used to train Sora algorithms, and whether sensitive personal data are collected.[59] If OpenAI intends to provide the service to EU Users, Garante also required information on Sora's legal basis for processing data and how it would inform users about their data rights.[60]

Example #2: Korea's Enforcement Action concerning ChatGPT data breach

On July 27, 2023, PIPC, the South Korean national data protection authority, announced an enforcement action against OpenAI concerning a breach of ChatGPT Plus subscriber information.[61] On March 20, 2023, subscriber information including user names, email addresses, payment addresses, and credit card information was made available to other ChatGPT subscribers, due to a bug in an open-source library used by OpenAI.[62] 687 South Korean users were impacted by the data breach.

The legal basis of the enforcement is the Korean Personal Information Protection Act (PIPA). Article 29 of PIPA specifies a duty for "personal information controller[s]" to

---

[56] *Id.*
[57] Garante also stated that it will also consider the EDPB ChatGPT Task Force Determination. *See,* GPDP, *ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI*, (Jan. 29, 2024), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9991867.
[58] GPDP*, Artificial intelligence: the Italian Data Protection Authority opens an investigation into OpenAI's 'Sora'*, (Mar. 8, 2024), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9991867.
[59] *Id.*
[60] *Id.*
[61]Personal Information Protection Commission [PIPC], *PIPC Imposes Administrative Sanctions on OpenAI, Issuing Recommendations to Improve Data Privacy Practices*, (Jul. 27, 2024), https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2271.
[62] The information was leaked through incorrectly addressed subscription confirmation emails, or through displaying. OpenAI*, March 20 ChatGPT outage: Here's what happened*, (Mar. 24, 2023), https://openai.com/index/march-20-chatgpt-outage/.

take "technical managerial, and physical measures" to safeguard personal information.[63] Meanwhile, Article 39-4 of PIPA requires notification by "a provider of information and communications services" to "relevant users" and PIPC no later than 24 hours "since he or she became aware of such fact."[64]

PIPC determined that OpenAI failed to meet the data breach notification requirement under PIPA.[65] Furthermore, PIPC also found other deficiencies and statutory violations of PIPA upon investigation.[66] These violations include the "failure to meet the statutory requirements for obtaining proper user consent" and "unclear descriptions about data controller-processor relationship and data disposal."[67]

PIPC imposed an administrative fine of 3.6 million Korean Won (approximately $3,000) against OpenAI for failing to meet the notification requirement.[68] PIPC also provided unspecified recommendations to OpenAI for PIPA compliance and declared to continue monitoring the implementation of these recommendations.[69]

PIPC has also requestioned information to assess the data privacy risks of OpenAI's services, including:

- How OpenAI collects and processes data;
- How it uses Korean language data to train its models;
- How it addresses legal and ethical concerns, and;
- How it handles data requests by users.[70]

Example #3: GDPR complaints against ChatGPT alleging hallucination

Two GDPR complaints in Austria and Poland were filed on the basis of outputs generated by ChatGPT.

NOYB – European Center for Digital Rights, a non-profit organization founded by Max Schrems, an Austrian privacy activist, submitted a complaint to the Austrian DPA in April 2024.[71] The complaint specifically targets the issue of hallucination, alleging that:

[63] Gaeinjeongbo bohobeop [Personal Information Protection Act] art. 29 (S. Kor.).
[64] *Id. at* art. 39-4.
[65] PIPC, *supra* note 38.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] NOYB – European Center for Digital Rights, *Complaint* (Apr. 29, 2024), https://noyb.eu/sites/default/files/2024-04/OpenAI%20Complaint_EN_redacted.pdf

- The lack of viable access to personal data collected by OpenAI violates the transparency principle under Art. 12 and the right to access under Art. 15;
- The impossibility of erasing or rectifying inaccurate personal information generated by ChatGPT violates the obligation to accurately process personal information under Art. 5(1)(d). [72]

Polish privacy activist, Lukasz Olejnik, extensively corresponded with OpenAI via emails on issues concerning his data subject's rights, after ChatGPT generated inaccurate information about him.[73] He then filed a complaint to the Polish DPA against OpenAI in August 2023, alleging that:

- The inaccurate processing of personal information violated the obligations to process data with "lawfulness, fairness, and transparency" under Art. 5(1)(a) and the transparency principle under Art. 12;
- OpenAI failed to provide sufficient information about the sources, processing, and recipients of Olejnik's data, and violated his right to access under Art. 15;
- The inability of OpenAI to rectify inaccurate processed data about Olejnik's data violated his right to rectify under Art. 16;
- These blatant incompatibilities of ChatGPT with GDPR violated the "privacy by design" principle required under Art. 25(1).[74]

Both complaints requested their respective DPA to initiate investigations of Open AI and corrective measures (similar to injunctive relief), and the NOYB complaint has also requested fines.[75] The Polish DPA has since launched an investigation in response to the complaint, while the Austrian DPA has yet to respond.[76]

[72] *Id.* at 4.
[73] Maciej Gawronski, *Complaint Against Unlawful Processing of Personal Data,* (Aug. 29, 2023), https://lukaszolejnik.com/stuff/OpenAI_GDPR_Complaint_LO.pdf.
[74] *Id.* at 7.
[75] NOYB, *supra* note. 48 at 6; Gawronski, *supra* note 50 at 1.
[76] URZĄD OCHRONY DANYCH OSOBOWYCH [UODO], *The technology has to be compliant with the GDPR*, https://uodo.gov.pl/pl/138/2823.

Example #4: European Data Protection Board Taskforce Report on ChatGPT

The European Data Protection Board (EDPB) convened a ChatGPT Task Force to share information and coordinate investigations between DPAs. The EDPB Task Force released a preliminary report in May 2024.[77] In the report, the EDPB emphasized that:

> technical impossibility cannot be invoked to justify non-compliance with these requirements, especially considering that the principle of data protection by design set out in Article 25(1) GDPR shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself.[78]

In its report the EDPB set out "preliminary views" of the investigation into ChatGPT and OpenAI's operations in the EU. In assessing the "lawfulness" of processing personal data it considered: "i) collection of training data (including the use of web scraping data or reuse of datasets), ii) pre-processing of the data (including filtering), iii) training, iv) prompts and ChatGPT output as well as v) training ChatGPT with prompts."[79] Among the observations of the EDPB, the following are worth emphasizing:

- [A]dequate safeguards play a special role in reducing undue impact on data subjects. Such safeguards could inter alia be technical measures, defining precise collection criteria and ensuring that certain data categories are not collected or that certain sources (such as public social media profiles) are excluded from data collection. Furthermore, measures should be in place to delete or anonymise personal data that has been collected via web scraping before the training stage. [80]

- If ChatGPT is made available to the public, it should be assumed that individuals will sooner or later input personal data. If those inputs then become part of the data model and, for example, are shared with anyone asking a specific question, OpenAI remains responsible for complying with the GDPR and should not argue that the input of certain personal data was prohibited in first place.[81]

- [D]ue to the probabilistic nature of the system, the current training approach leads to a model which may also produce biased or made up outputs. In addition, the

[77] European Data Protection Board [EDPB], Report of the work undertaken by the ChatGPT Taskforce (2024). [EDPB Report]
[78] EDPB Report, pg. 5
[79] EDPB Report, pg. 6
[80] EDPB Report, pg. 6
[81] EDPB Report, pg. 7

outputs provided by ChatGPT are likely to be taken as factually accurate by end users, including information relating to individuals, regardless of their actual accuracy.[82]

VII. FTC's Mandate and Guidance on AI Products

The FTC is perhaps one of the most empowered consumer protection agencies in the world. Its broad mandate to protect consumers and ensure fair competition allows the agency to "prosecute any inquiry necessary to its duties in any part of the United States," FTC Act Sec. 3, 15 U.S.C. Sec. 43. The FTC is authorized "to gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting banks, savings and loan institutions . . . Federal credit unions . . . and common carriers . . . ." FTC Act Sec. 6(a), 15 U.S.C. Sec. 46(a).[83] The FTC has authority to investigate, prosecute, and prohibit "unfair or deceptive acts or practices in or affecting commerce."[84]

There is little question that the FTC's authorities apply to AI services. In New York Times op-ed, FTC Chair Lina Khan wrote, "Although these tools are novel, they are not exempt from existing rules, and the FTC will vigorously enforce the laws we are charged with administering, even in this new market."[85] Chair Khan has on several occasions reaffirmed that the FTC will ensure that "claims of innovation are not used as cover for lawbreaking".[86]

The FTC has issued several business guidance in relation to AI products and services.[87]

---

[82] EDPB Report, pg. 8

[83] FTC, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority

[84] 15 U.S.C. §45 (a)(1), (2), (4)(A), 4(B); (m)(1)(A); m(1)(B) ("Declaration of unlawfulness; power to prohibit unfair practices); (b) (proceedings by the Commission")

[85] Lina Khan, *We Must Regulate A.I. Here's How.*, Opinion, New York Times, (May 3, 2023), https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html

[86] Kyrsten Crawford, *FTC's Lina Khan warns Big Tech over AI,* SIEPR, (Nov. 3, 2023), https://siepr.stanford.edu/news/ftcs-lina-khan-warns-big-tech-over-ai

[87] FTC, *Chatbots, deepfakes, and voice clones: AI deception for sale*, (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale; FTC, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues,* FTC Report, (January 2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report; FTC, *Using Artificial Intelligence and Algorithms*, Business Guidance, (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial- intelligence-and-algorithms; FTC, *Aiming for truth, fairness, and equity in your company's use of AI* , Business Guidance, (April 2021), https://www.ftc.gov/business-

2020-2021

In 2020, the FTC issued the Statement *Using Artificial Intelligence and Algorithm*.[88] In the 2020 statement, the Director of the FTC Consumer Protection Bureau said, "The FTC's law enforcement actions, studies, and guidance emphasize that the use of AI tools should be transparent, explainable, fair, and empirically sound, while fostering accountability."[89]

The 2020 FTC Statement set out recommended best practices, including:

> (a) Don't deceive consumers about how you use automated tools ("But, when using AI tools to interact with customers (*think chatbots*), be careful not to mislead consumers about the nature of the interaction.") (emphasis added)
> (b) Be transparent when collecting sensitive data ("Secretly collecting audio or visual data – or any sensitive data – to feed an algorithm could also give rise to an FTC action.")
> (c) Ensure that your data and models are robust and empirically sound.
> (d) Make sure that your AI models are validated and revalidated to ensure that they work as intended, and do not illegally discriminate
> (e) Consider your accountability mechanism ("Consider how you hold yourself accountable, and whether it would make sense to use independent standards or independent expertise to step back and take stock of your AI.")

In 2021, the FTC issued the *Statement Aiming for Truth, Fairness, and Equity in Your Company's use of AI*.[90] The 2021 FTC Statement said to businesses offering products with the AI techniques: "*As your company launches into the new world of artificial*

---

guidance/blog/2021/04/aiming-truth-fairness-equity-your- companys-use-ai; FTC, *For Business Opportunity Sellers, FTC says "AI" Stands for "Allegedly Inaccurate"*, FTC Business Blog (Aug. 22, 2023), https://www.ftc.gov/business-guidance/blog/2023/08/business-opportunity-sellers-ftc-says-ai-stands-allegedly-inaccurate; *Generative AI Raises Competition Concerns,* FTC Blog, (Jun. 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns

[88] FTC, *Using Artificial Intelligence and Algorithms*, Business Guidance, (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial- intelligence-and-algorithms

[89] Id.

[90] FTC, *Aiming for truth, fairness, and equity in your company's use of AI* , Business Guidance, (April 2021) (emphasis below in the original), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your- companys-use-ai;

intelligence, keep your practices grounded in established FTC consumer protection principles." The 2021 FTC Statement set out recommended best practices, including:

> (a) Start with the right foundation ("design your model to account for data gaps, and – in light of any shortcomings – limit where or how you use the model.")
> (b) Watch out for discriminatory outcomes ("It's essential to test your algorithm – both before you use it and periodically after that – to make sure that it doesn't discriminate on the basis of race, gender, or other protected class.")
> (c) Embrace transparency and independence ("As your company develops and uses AI, think about ways to embrace transparency and independence – for example, by using transparency frameworks and independent standards, by conducting and publishing the results of independent audits, and by opening your data or source code to outside inspection."
> (d) Don't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results ("your statements to business customers and consumers alike must be truthful, non-deceptive, and backed up by evidence.")
> (e) Tell the truth about how you use data (describing recent enforcement actions against Facebook and Everalbum for misleading consumers)
> (f) Do more good than harm
> (g) Hold yourself accountable – or be ready for the FTC to do it for you.

2022-2023

In February 2023, following the widespread public awareness of GPT-4, the FTC warned, "false or unsubstantiated claims about [an AI] product's efficacy are our bread and butter. . . You don't need a machine to predict what the FTC might do when those claims are unsupported."[91]

The FTC's March 2023 business guidance on AI deception makes clear the risk of cyber-crime, financial fraud using generative AI tools, and states "The FTC Act's prohibition on deceptive or unfair conduct can apply if you make, sell, or use a tool that is effectively designed to deceive – even if that's not its intended or sole purpose."[92] The guidance also sets out risks that developers should consider, primarily, "whether there are reasonably foreseeable risks of fraud or harm" and whether "developers are taking measures to effectively mitigate those risks" or whether "developers are over-relying on post-release detection".

---

[91] FTC, *Keep your AI claims in check,* (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check
[92] FTC, *Chatbots, deepfakes, and voice clones: AI deception for sale,* (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

In the May 2023 business guidance on consumer trust and generative AI tools, the FTC states that, "Design or use of a product can also violate the FTC Act if it is unfair."[93] The guidance also states that: FTC staff is focusing intensely on how companies may choose to use AI technology, including new generative AI tools, in ways that can have actual and substantial impact on consumers.

In the October 2023 Guidance[94] the FTC specifically addressed the risks of large language models and stated:

> AI models are susceptible to bias, inaccuracies, "hallucinations," and bad performance. At the end of the day, AI model accuracy is dependent on a number of factors including the input data, training techniques, and context of deployment. Further, companies design applications to be efficient (using less resources, while yielding more output) in order to optimize for scalability and profit. This often means reducing the number of humans involved, leaving consumers to engage with their AI replacements.
>
> With the increasing sophistication of large language models, image generation systems, and more, it is becoming harder to distinguish human from machine. AI products could be used by malicious actors to increase the scale or sophistication of existing scams, another issue the FTC has written about before.[95]

The FTC has also issued business guidance that would guide the downstream uses and integrations of LLM products.[96] Relevant to the downstream integration of AI products, the recent deals with services like Slack, Reddit, and the automatic opt-in of user data for training AI models, the FTC states, "It may be unfair or deceptive for a company to adopt more permissive data practices—for example, to start sharing consumers' data with third parties or using that data for AI training—and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy."[97]

---

[93] FTC, *The Luring Test: AI and the engineering of consumer trust,* (May 1, 2023), https://www.ftc.gov/consumer-alerts/2023/05/luring-test-ai-and-engineering-consumer-trust
[94] FTC, *Consumers Are Voicing Concerns About AI,* (Oct. 3, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/10/consumers-are-voicing-concerns-about-ai
[95] Id.
[96] FTC, *AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, (Feb. 13, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive
[97] Id.

Apart from business guidance, since 2019, the FTC has proposed five disgorgement orders including against Cambridge Analytica and Amazon.[98] In the 2023 Privacy and Security Report to Congress, the FTC stated:

> Artificial Intelligence: The Commission has been leading efforts to ensure that AI and similar technologies are not deployed in harmful ways. In addition to obtaining orders against Rite Aid, Ring, and Amazon to ensure that companies are disincentivized from using data that was wrongfully collected or trained to develop AI, we have initiated a market study of social media and video streaming platforms on the use of AI, announced a public contest to develop new approaches to protect consumers from AI-enabled voice cloning harms, proposed rules to crack down on AI-fueled impersonator and fake review fraud, and issued numerous business guidance alerts.[99]

The FTC has the mandate, the tools to enforce against generative AI systems, and has put companies on notice through its business guidance.

VIII. Limited AI legislation to protect people

There has been a lot of activity in Congress, but little action in advancing AI guardrails. "[M]ore than 300 AI-related proposed bills were introduced in this congressional session [beginning in January 2023]. They range all over the place, from controlling misinformation to how we can stimulate AI innovation and research."[100] However, only about 20 have moved passed a second reading at the respective committees. With a narrow window of meaningful congressional action remaining in the current session, it is imperative on regulatory agencies like the FTC to exercise their legislative mandate in the public interest.

In the absence of congressional action on AI legislation, what we are left with is a repeat of patchwork of legislative proposals for AI. As the National Conference of State Legislatures report: "In the 2024 legislative session, at least 40 states, Puerto Rico, the Virgin Islands and Washington, D.C., introduced AI bills, and six states, Puerto Rico and

---

[98] William Simpson, *AI Regulatory Enforcement Around the World*, IAPP News, (Aug. 2, 2023), https://iapp.org/news/a/ai-regulatory-enforcement-around-the-world

[99] The Federal Trade Commission, *2023 Privacy and Data Security Update,* pg. 1, https://www.ftc.gov/reports/federal-trade-commission-2023-privacy-data-security-update

[100] Nicola Jones, *The US Congress is taking on AI — this computer scientist is helping*, News Q&A, Nature, (May 9, 2024), https://www.nature.com/articles/d41586-024-01354-4#:~:text=There%20have%20been%20more%20than,stimulate%20AI%20innovation%20and%20research.

the Virgin Islands adopted resolutions or enacted legislation."[101] However, the ambit and content of the legislation also differs widely. While "Colorado required developers and deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination and mandated disclosures to consumers"[102], "Tennessee required the governing boards of public institutions of higher education to promulgate rules and required local education boards and public charter schools to adopt policies, regarding the use of AI by students, teachers, faculty and staff for instructional purposes."[103]

President Biden's AI Executive Order on Safe, Secure, and Trustworthy AI[104] (AI EO), as commendable and extensive as it is, applies only to federal agencies. It introduces key guardrails for the government use of AI and establishes oversight on such use. The guidance from the Office of Management and Budget (OMB) builds on these protections by setting out clear criteria for "rights-impacting" and "safety-impacting" AI systems in the government and requires lifecycle assessment of AI systems.

There is some optimism that the federal government through the powers of its purse will be able to set some rules of the road for the private sector.[105] However, the AI EO doesn't apply to the private sector outside of certain water-marking and safety obligations, it cannot mandate any pre-deployment or priore impact assessments, or rules requiring that companies disclose training data sources, model size and other important details.[106] The durability of the Executive Order is also uncertain given that a change in administration could see the EO reversed.

But what is significant for the purposes of this report is that the Biden AI EO also calls upon the FTC to exercise its existing authorities to ensure that consumers and workers are protected from AI harms.[107]

---

[101] National Conference of State Legislatures, *Artificial Intelligence 2024 Legislation*, (Jun. 3, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation
[102] Id.
[103] Id
[104] Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 75209 (Oct. 30, 2023), https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf
[105] Sorelle Friedler, Janet Haven, Brian J. Chen, *How the AI Executive Order and OMB memo introduce accountability for artificial intelligence,* Commentary, Brookings Institution, (Nov. 16, 2023), https://www.brookings.edu/articles/how-the-ai-executive-order-and-omb-memo-introduce-accountability-for-artificial-intelligence/
[106] Axios, *What's in Biden's AI executive order — and what's not*, (Nov.1, 2023), https://www.axios.com/2023/11/01/unpacking-bidens-ai-executive-order
[107] Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 75209 (Oct. 30, 2023), https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

> In particular, the Federal Trade Commission is encouraged to consider, as it deems appropriate, whether to exercise the Commission's existing authorities, including its rulemaking authority under the Federal Trade Commission Act, 15 U.S.C. 41 et seq., to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI.[108]

IX. FTC Enforcement: The most viable solution for guardrails

CAIDP President, Merve Hickok, testified at one of the first congressional hearings last year and stated, "We do not have the guardrails in place, the laws that we need, the public education, or the expertise in government to manage the consequences of the rapid changes that are now taking place."[109]

At the House Oversight and Accountability Committee hearing in July last year, Chair Khan, stated

> *"As the nation's primary consumer protection agency, the FTC has a broad mandate to protect the public from unfair or deceptive practices throughout the economy…. The Commission will vigorously use the full range of our authorities to protect consumers from deceptive and unfair conduct and maintain open, fair, and competitive markets in this rapidly evolving technology. Through blog posts and other public pronouncements, the agency is providing timely analysis to market participants and the public. The Commission is poised to move aggressively against businesses that engage in deceptive or unfair acts involving AI and to help ensure that illegal practices do undermine competition and innovative uses of AI."*[110]

---

[108] Id. at sec. 5.3.s

[109] Testimony and statement for the record of CAIDP President Merve Hickok, Advances in AI: Are We
Ready For a Tech Revolution?, House Committee on Oversight and Accountability: Subcommittee on
Cybersecurity, Information Technology, and Government Innovation (Mar. 8, 2023), https://oversight.house.gov/wp-content/uploads/2023/03/Merve-Hickok_testimony_March-8th-2023.pdf

[110] Prepared Statement of the Federal Trade Commission, Hearing on "Oversight of the Federal Trade Commission", Committee on the Judiciary, United States House of Representatives, (Jul. 13, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/khan-testimony.pdf

In November 2023, the FTC adopted an omnibus resolution to streamline the agency's ability to issue civil investigative demands relating to "products and services that use or are produced using artificial intelligence."[111]

In comments to the U.S. Copyright Office, the FTC stated "The FTC has been exploring the risks associated with AI use, including violations of consumers' privacy, automation of discrimination and bias, and turbocharging of deceptive practices, imposters schemes and other types of scams."[112] Most recently the National Association of Voice Actors (NAVA) issued a public statement in support of the CAIDP complaint regarding OpenAI and ChatGPT and called upon the FTC to complete its investigation with urgency.[113]

ChatGPT was released in the market in November 2022.[114] ChatGPT released its GPT-4 system card in March 2023[115], when it had already amassed an estimated 100 million monthly users.[116] The technical report setting out the risks of the product was issued only after the product was commercially released in the market and OpenAI began monetizing it. This was clearly contrary to FTC's established business guidance to ensure compliant products prior to release.

---

[111] Alan Raul, Alexandra Mushka, The U.S. Plans to 'Lead the Way' on Global AI Policy, LAWFARE, (Feb. 13, 2024), https://www.lawfaremedia.org/article/the-u.s.-plans-to-lead-the-way-on-global-ai-policy; *See also*, FTC, FTC Authorizes Compulsory Process for AI-related Products and Services, Press Release, (Nov. 21,2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-authorizes-compulsory-process-ai-related-products-services

[112] FTC, In Comment Submitted to U.S. Copyright Office, FTC Raises AI-related Competition and Consumer Protection Issues, Stressing That It Will Use Its Authority to Protect Competition and Consumers in AI Markets, Press Release (Nov. 7, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/InCommentSubmittedtoUSCopyrightOfficeFTCRaisesAIrelatedCompetitionandConsumerProtectionIssuesStressingThatItWillUseItsAuthoritytoProtectCompetitionandConsumersinAIMarkets

[113] National Association of Voice Actors (NAVA), Public Statement of the National Association of Voice Actors, We need the FTC to act now - Complete the investigation into OpenAI, Press Release (Jun. 18, 2024), https://navavoices.org/press-releases/

[114] OpenAI, *Introducing ChatGPT*, (Nov. 30, 2022), https://openai.com/index/chatgpt/

[115] OpenAI, *GPT-4 Technical Report (2023)*, https://cdn.openai.com/papers/gpt-4.pdf

[116] Reuters, *ChatGPT sets record for fastest-growing user base - analyst note,* (Feb. 2, 2023), https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ ; The Verge, *ChatGPT continues to be one of the fastest-growing services ever,* (Nov. 6, 2023), https://www.theverge.com/2023/11/6/23948386/chatgpt-active-user-count-openai-developer-conference

AI companies including OpenAI have made lofty voluntary commitments, most recently at the Seoul AI Safety Summit.[117] The international scientific report that preceded the Seoul summit led by Yoshua Bengio highlighted that "General-purpose AI can pose severe risks to individual and public safety and wellbeing."[118] The report concludes that, "Despite rapid advances in capabilities, researchers currently cannot generate human-understandable accounts of how general-purpose AI models and systems arrive at outputs and decisions. This makes it difficult to evaluate or predict what they are capable of, how reliable they are, and obtain assurances on the risks they might pose."[119]

These commitments build upon the voluntary commitments by the industry to the Biden-Harris Administration "toward safe, secure, and transparent development of AI technology."[120] However, as OpenAI poignantly notes these "they apply only to generative models that are overall more powerful than the current industry frontier (e.g. models that are overall more powerful than any currently released models, including GPT-4, Claude 2, PaLM 2, Titan and, in the case of image generation, DALL-E 2).[121] Alarmingly, AI companies are already reneging on their voluntary commitments to provide AI safety institutes pre-deployment access to their models.[122]

History shows vague and unenforceable promises are not enough.[123] When Facebook acquired WhatsApp it acquired user data contrary to promises that it would not or could not integrate databases, and also palpably in violation of the terms of the 2011

---

[117] CNBC, Tech giants pledge AI safety commitments — including a 'kill switch' if they can't mitigate risks, (May 21, 2024), https://www.cnbc.com/2024/05/21/tech-giants-pledge-ai-safety-commitments-including-a-kill-switch.html

[118] AI Seoul Summit, International Scientific Report on the Safety of Advanced AI, Interim Report, (May, 2024), pg. 12, 13, https://assets.publishing.service.gov.uk/media/6655982fdc15efdddf1a842f/international_scientific_report_on_the_safety_of_advanced_ai_interim_report.pdf

[119] Id, pg. 83.

[120] The White House, *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, (Jul. 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

[121] OpenAI, *Moving AI Governance Forward*, (Jul.21, 2023), https://openai.com/index/moving-ai-governance-forward/

[122] Politico, *Rishi Sunak promised to make AI safe. Big Tech's not playing ball*, (Apr. 26, 2024), https://www.politico.eu/article/rishi-sunak-ai-testing-tech-ai-safety-institute/

[123] David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?*, Administrative Law, Blog Essay, Harvard Law Rev., (Apr. 4, 2018), https://harvardlawreview.org/blog/2018/04/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/

consent order with the FTC.[124] This was after Marc Zuckerberg publicly apologized to Congress for the Cambridge analytica debacle. At the same time, a New York Times investigation Facebook had secret deals with numerous companies for access to user data, including in some cases the contents of millions of users' private messages.[125] But even after the 2011 consent order, it took the agency almost a decade to act on Facebook's violations and egregious business practices.[126]

We see a repeat of this playbook from the tech industry. Sam Altman testified in Congress asking for AI legislation[127] while OpenAI lobbied against the provisions of the EU AI Act.[128] "A.I. companies are playing governments off one another. In Europe, industry groups have warned that regulations could put the European Union behind the United States. In Washington, tech companies have cautioned that China might pull ahead.[129]

There has been a lot of governance-washing of the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections* in which Companies commit to manage the risks arising from deceptive AI election content "in line with their own policies"[130] and yet Sen. Warner has issued letters including to OpenAI asking them what measures exactly are put in place pursuant to this accord.[131]

Relying on AI companies to police themselves is not only foolhardy but does nothing to advance responsible innovation. "If the FTC had stood behind its commitment

---

[124] Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation,* Worth Magazine, (May 4, 2018), https://worth.com/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/

[125] Marc Rotenberg, *After Latest Facebook Fiasco, Focus Falls on Federal Commission,* Worth Magazine (Dec. 21, 2018), https://worth.com/after-latest-facebook-fiasco-focus-falls-on-federal-commission/; The New York Times, *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, (nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

[126] FTC, *Facebook, Inc., In the Matter of, https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter*

[127] Written Testimony of Sam Altman, Chief Executive Officer, OpenAI, Before the U.S. Senate Committee on the Judiciary Subcommittee on Privacy, Technology, & the Law, (May 15, 2023), https://www.judiciary.senate.gov/imo/media/doc/2023-05-16%20-%20Bio%20&%20Testimony%20-%20Altman.pdf

[128] Time, *Exclusive: OpenAI Lobbied the E.U. to Water Down AI Regulation*, Time Exclusive, (Jun. 20, 2023), https://time.com/6288245/openai-eu-lobbying-ai-act/

[129] *See,* New York Times, *How Nations Are Losing a Global Race to Tackle A.I.'s Harms,* (Dec. 6, 2023), https://www.nytimes.com/2023/12/06/technology/ai-regulation-policies.html?searchResultPosition=9

[130] AI Elections Accord, https://www.aielectionsaccord.com

[131] Letters issued by Sen. Mark Warner, (May 14, 2024), https://www.warner.senate.gov/public/_cache/files/3/e/3e12f60b-3e2f-4ab7-ade4-d819be943bde/7361EB3F33D404A03447E6FBD244D62D.full-munich-letters-pdf-final-3-.pdf

to protect the data of WhatsApp users, there might still be an excellent messaging service, with end-to-end encryption, no advertising and minimal cost, widely loved by internet users around the world. But the FTC failed to act and one of the great internet innovations has essentially disappeared."[132]

History shows that the longer the FTC delays, the more difficult it is to establish the necessary guardrails. Inaction by the agency is costly and FTC enforcement is the most immediate viable option for establishing guardrails for the AI industry. The FTC must act now.

ABOUT CAIDP

The Center for AI and Digital Policy (CAIDP)[133] is a non-profit, independent research, education, and advocacy organization based in Washington D.C. and Brussels. CAIDP aims to ensure that artificial intelligence and digital policies promote a better society, more fair, more just, and more accountable – a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law.

ABOUT THIS REPORT

This report was prepared by CAIDP Associate Director Christabel Randolph with the assistance of Victor Liu, Research Assistant, CAIDP.

[132] Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation,* Worth Magazine, (May 4, 2018), https://worth.com/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/
[133] CAIDP, https://www.caidp.org