FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of

OpenAI GP LLC, a limited liability company, also d/b/a OpenAI; and

OpenAI Global, LLC, a limited liability company, also d/b/a OpenAI.

Complaint and Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center (EPIC)

I. Summary

1. This complaint[1] concerns the development, deployment, and dissemination of OpenAI's generative artificial intelligence ("AI") products, including its various custom GPTs[2] and third-party Application Programming Interface ("API") integrations. OpenAI purports to advance "safe and beneficial"[3] AI through an opaque, proprietary AI model developed using millions of consumer data points—including personally identifiable information—and consumer-generated content scraped from the web at unprecedented rates.[4] In addition to its direct consumer offerings, OpenAI has continued to market its AI products to millions of third-party developers and deployers, including companies in the financial services and real estate industries, via API integrations and their GPT Store.[5]

2. OpenAI has failed to demonstrate that its AI products meet established public policy standards for responsible development and use of AI systems, including those set out in Executive Order

[1] EPIC would like to thank our spring 2024 law clerk, Sara Correa, for her contributions to this complaint.
[2] *See Introducing GPTs*, OpenAI (Nov. 6, 2023), https://openai.com/index/introducing-gpts/.
[3] *About*, OpenAI, https://openai.com/about (last visited Aug. 19, 2024).
[4] Isaiah Poritz, *OpenAI Hit with Class Action Over 'Unprecedented' Web Scraping*, Bloomberg Law (June 28, 2023), https://news.bloomberglaw.com/ip-law/openai-hit-with-class-action-over-unprecedented-web-scraping.
[5] *See* Press Release, OpenAI, Introducing the GPT Store (Jan. 10, 2024), https://openai.com/blog/introducing-the-gpt-store; Press Release, OpenAI, OpenAI API (June 11, 2020), https://openai.com/blog/openai-api; *The rise of AI in banking and finance industry: Exploring use cases and applications*, LeewayHertz, https://www.leewayhertz.com/ai-use-cases-in-banking-and-finance (last visited Aug. 19, 2024); Mae Rice et al., *AI in Real Estate: 20 Companies Defining the Industry*, Built In (June 26, 2023), https://builtin.com/artificial-intelligence/ai-real-estate.

14110 on the Safe, Secure, and Trustworthy Development and Use of AI[6] and the White House's Blueprint for an AI Bill of Rights.[7]

3. OpenAI has engaged in unfair and deceptive trade practices, both directly and by providing the means and instrumentalities for unfair and deceptive trade practices to companies via API integrations and their GPT Store, in violation of Section 5 of the Federal Trade Commission Act ("FTC Act").[8]

4. For the reasons set out below, the Federal Trade Commission should open an investigation; secure an injunction against the offending business practices; seek deletion, disgorgement, or destruction of biased, discriminatory, or improperly obtained data and AI models; implement stringent informed consumer consent measures; require ongoing testing and risk monitoring; and provide such other relief as the Commission deems necessary and appropriate.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has played a substantial role in developing Federal Trade Commission authority to address emerging privacy issues and to safeguard the privacy rights of consumers.[9]

[6] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023) [hereinafter "Executive Order 14110"].

[7] White House Off. Sci. & Tech. Pol'y, Blueprint for an AI Bill of Rights (2022), https://whitehouse.gov/ostp/ai-bill-of-rights/.

[8] 15 U.S.C. § 45.

[9] *See, e.g.*, EPIC, Comments on FTC Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; Consumer Reps. & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/ [hereinafter "EPIC FTC Commercial Surveillance Comment"]; EPIC, Comments on Proposed Consent Order, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (Oct. 8, 2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; EPIC et al., Comments on Proposed Consent Order, *In re Zoom Video Communications, Inc.*, FTC File No. 192-3167 (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; EPIC, Comments on Proposed Consent Order, *In re Unrollme, Inc.*, FTC File No. 172-3139 (Sept. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; EPIC, Comments on Proposed Consent Agreements, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (Sept. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; EPIC, Comments on FTC Rule Setting Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (proposed Apr. 4, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf; EPIC, Comments on Proposed Consent Order, *In re Uber Technologies, Inc.*, FTC File No. 152-3054 (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-Revised-Uber-Settlement.pdf; EPIC, Comments on Proposed Consent Order, *In re Paypal, Inc.*, FTC File No. 162-3102 (Mar. 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Google Inc.* (July 31, 2017), https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; Complaint and Request for Investigation, Injunction, and Other Relief, *In re Genesis Toys and Nuance Communications* (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

EPIC is also a longstanding advocate for the transparent, ethical, and responsible development and use of artificial intelligence and automated decision-making.[10]

5. OpenAI is a major U.S.-based AI research and development organization consisting of the 501(c)(3) non-profit, OpenAI Incorporated ("OpenAI Inc."); multiple intermediary and holding companies, including OpenAI GP LLC; and its for-profit subsidiary corporation, OpenAI Global, LLC ("OpenAI LLC") (hereinafter, collectively, "OpenAI").[11] Its headquarters are located at 3180 18th Street, San Francisco, California, United States.[12] OpenAI develops, operates, and markets generative AI products to consumers and millions of third-party AI deployers, including entities in sensitive consumer markets like financial services and real estate. OpenAI's primary generative AI products are GPT-4o, DALL-E, Sora, and Whisper, but it also maintains other ChatGPT API integrations and custom products through its GPT Store.[13]

6. The Federal Trade Commission ("FTC" or "Commission") is an independent agency of the United States government given statutory authority and responsibility by the FTC Act, 15 U.S.C. §§ 41–58. The Commission is charged, *inter alia*, with enforcing Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts or practices in or affecting commerce. The FTC regularly pursues unfair and deceptive acts or practices facilitated by AI technologies.[14]

[10] *See, e.g.*, EPIC, Generating Harms: Generative AI's Impact & Paths Forward (2023), https://epic.org/gai. [hereinafter "GenAI Report I"]; EPIC, Generating Harms II: Generative AI's New & Continued Impacts (2024), https://epic.org/wp-content/uploads/2024/05/EPIC-Generative-AI-II-Report-May2024-1.pdf [hereinafter "GenAI Report II"]; EPIC, Comments on Notice of Proposed Rulemaking, *In re Access to Video Conferencing*, CG Docket No. 23-161 (Sept. 6, 2023), https://epic.org/documents/in-re-access-to-video-conferencing/; EPIC, Comments on Proposed Parental Consent Method Submitted by Yoti, Inc., Under the Voluntary Approval Processes Provisions of the Children's Online Privacy Protection Rule, 88 Fed. Reg. 46705 (Aug. 21, 2023), https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-submitted-by-yoti-inc-under-coppa-rule/.

[11] *Our Structure*, OpenAI (June 28, 2023), https://openai.com/our-structure.

[12] *See* Evan Symon, *OpenAI Announces Nearly 500,000 Square Foot Office Lease in San Francisco*, Cal. Globe (Oct. 31, 2023), https://californiaglobe.com/fr/openai-announces-nearly-500000-square-foot-office-lease-in-san-francisco/.

[13] *Transforming Work and Creativity with AI*, OpenAI, https://openai.com/product (last visited Apr. 1, 2024); Introducing the GPT Store, *supra* note 5.

[14] *See, e.g.*, Ashley Gold, *FTC Consumer Chief Fires Warning on False AI Claims*, Axios Pro (June 10, 2024), https://www.axios.com/pro/tech-policy/2024/06/10/ftc-consumer-chief-fires-warning-on-false-ai-claims; Administrative Decision and Order at 6-7, *In re Rite Aid Corp.*, FTC File No. 072-3121 (2023); FTC, Comments to the U.S. Copyright Office regarding Artificial Intelligence and Copyright, 88 Fed. Reg. 59942 (Oct. 30, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p241200_ftc_comment_to_copyright_office.pdf;

III. Established Public Policies for the Use of Artificial Intelligence

A. The OECD AI Principles

7. In 2019, the member nations of the Organization for Economic Cooperation and Development ("OECD"), including the United States,[15] promulgated the OECD Principles on Artificial Intelligence.[16] The United States has expressly endorsed the OECD Principles.[17]

8. According to the OECD AI Principle on Human-Centered Values and Fairness, "AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity, and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labour rights."[18]

9. According to the OECD AI Principle on Transparency and Explainability, AI actors should "provide meaningful information, appropriate to the context, and consistent with the state of art (i) to foster a general understanding of AI systems, (ii) to make stakeholders aware of their interactions with AI systems, including in the workplace, (iii) to enable those affected by an AI system to understand the outcome, and (iv) to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[19]

10. According to the OECD AI Principle on Robustness, Security, and Safety, "AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk."[20]

11. According to the OECD AI Principle on Accountability, "[o]rganisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles."[21]

12. The OECD Principles on Artificial Intelligence are "established public policies" within the meaning of the FTC Act.[22]

[15] *Timeline*, OECD, https://www.oecd.org/60-years/timeline/ (last visited Dec. 18, 2023).

[16] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[17] Press Release, Fiona Alexander, NTIA, U.S. Joins with OECD in Adopting Global AI Principles (May 22, 2019), https://www.ntia.gov/blog/us-joins-oecd-adopting-global-ai-principles.

[18] OECD Principle 1.2(a), *supra* note 16.

[19] OECD Principle 1.3, *supra* note 16.

[20] OECD Principle 1.4(a), *supra* note 16.

[21] OECD Principle 1.5, *supra* note 16.

[22] 15 U.S.C. § 45(n).

B. The Blueprint for an AI Bill of Rights

24. On October 4, 2022, the White House Office of Science and Technology Policy ("OSTP") published its Blueprint for an AI Bill of Rights ("Blueprint"), a set of principles meant to guide the development, deployment, and use of automated systems and protect the rights of the American public.[23] OSTP designed the Blueprint for an AI Bill of Rights to be "fully consistent" with public policies that govern the development, deployment, and use of AI—including the OECD AI Principles.[24]

25. According to the Blueprint's Principle of Safe and Effective Systems, AI and automated systems should "undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards."[25]

26. According to the Blueprint's Principle of Algorithmic Discrimination Protections, "designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way. This protection should include proactive equity assessments as part of the system design, use of representative data and protection against proxies for demographic features, ensuring accessibility or people with disabilities in design and development, pre-deployment and ongoing disparity testing and mitigation, and clear organizational oversight."[26]

27. According to the Blueprint's Principle of Data Privacy, "[d]esigners, developers, and deployers of automated systems should seek your permission and respect your decisions regarding collection, use, access, transfer, and deletion of your data in appropriate ways and to the greatest extent possible" and "[c]onsent should only be used to justify collection of data in cases where it can be appropriately and meaningfully given."[27]

29. The principles outlined by OSTP's Blueprint for an AI Bill of Rights are "established public policies" within the meaning of the FTC Act.[28]

[23] *What is the Blueprint for an AI Bill of Rights?*, OSTP (Oct. 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/.

[24] *See Relationship to Existing Law and Policy*, OSTP (Oct. 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/relationship-to-existing-law-and-policy/.

[25] OSTP, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 5 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[26] *Id.*

[27] *Id.* at 6.

[28] 15 U.S.C. § 45(n).

C. NIST AI Risk Management Framework

30. On January 26, 2023, the National Institute of Standards and Technology ("NIST") published its AI Risk Management Framework ("AI RMF"), alongside various companion resources.[29] The AI RMF is "designed to equip organizations and individuals…with approaches that increase the trustworthiness of AI systems, and to help foster the responsible design, development, deployment, and use of AI systems over time."[30] It is "intended to be practical, to adapt to the AI landscape as AI technologies continue to develop, and to be operationalized by organizations in varying degrees and capacities so society can benefit from AI while also being protected from its potential harms."[31]

31. Under Section 5.1 of the AI RMF, NIST states that AI risk management processes and outcomes should be "established through transparent policies, procedures, and other controls based on organizational risk priorities" and that "organizational policies and practices [should be] in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts."[32]

32. Section 5.1 of the AI RMF also recommends that "organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly."[33]

33. Section 5.1 of the AI RMF further states that "[o]rganizational practices [should be] in place to enable AI testing, identification of incidents, and information sharing" and that "policies and procedures [should be] in place that address AI risks associated with third-party entities, including risks of infringement on third-party's intellectual property or other rights."[34]

34. Under Section 5.2 of the AI RMF, NIST states that organizations developing, selling, or using AI should examine and document the "potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness."[35]

35. Section 5.2 of the AI RMF also recommends that AI "[d]esign decisions take socio-technical implications into account to address AI risks"[36] and "[i]nternal risk controls for components of the AI system, including third-party AI technologies, are identified and documented."[37]

36. Under Section 5.3 of the AI RMF, NIST states that (1) "AI system performance or assurance criteria [should be] measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s)," (2) "the functionality and behavior of the AI system and its

[29] *See* Nat'l Inst. Standards & Tech., Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[30] *Id.* at 2.

[31] *Id.* at 2.

[32] *Id.* at 22–23.

[33] *Id.* at 24.

[34] *Id.*

[35] *Id.* at 27.

[36] *Id.* at 26.

[37] *Id.* at 27.

components… [should be] monitored when in production," (3) "the AI system to be deployed [should be] demonstrated to be valid and reliable," (4) "the AI system [should be] evaluated regularly for safety risks," and (5) "[AI system] fairness and bias… [should be] evaluated and results [should be] documents."[38]

37. Under Section 5.4 of the AI RMF, NIST recommends that (1) AI organizations should follow "procedures… to respond to and recover from a previously unknown risk when it is identified," (2) "mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use," (3) "post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management," and (4) "incidents and errors are communicated to relevant AI actors, including affected communities."[39]

38. NIST's AI RMF is an "established public policy" within the meaning of the FTC Act.[40]

D. Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of AI

37. On October 30, 2023, the White House published Executive Order 14110, setting out comprehensive guidelines to manage the development, procurement, and use of AI.[41] These guidelines include both restrictions on how federal agencies develop, procure, and use AI technologies and provisions encouraging responsible private-sector development and deployment of AI through federal funding restrictions and federal agency enforcement priorities.[42]

38. Under Section 5.3 of Executive Order 14110, the White House encourages the FTC 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."[43]

39. Section 2 of Executive Order 14110 sets out eight guiding principles and priorities concerning responsible AI development and use. These policy priorities include, but are not limited to:

    a. Ensuring that AI is safe and secure through "robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as

[38] *Id.* at 29–30.
[39] *Id.* at 32–33.
[40] 15 U.S.C. § 45(n).
[41] Executive Order 14110.
[42] *See id.* at 75196–98, 75204–05, 75209–75218.
[43] *Id.* at 75209.

appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use";[44]

b. Ensuring that AI policies are consistent with the White House's dedication to advancing equity and civil rights, including efforts to combat the "use of AI to disadvantage those who are already too often denied equal opportunity and justice"[45] and to "hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse";[46]

c. Protecting the "interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives," including efforts to "enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms of AI";[47] and

d. Protecting "American's privacy and civil liberties," including efforts to "ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks."[48]

40. Executive Order 14110 builds on earlier White House policies on responsible AI development and use, including the OSTP's Blueprint for an AI Bill of Rights and the NIST AI RMF.[49]

41. Executive Order 14110 is an "established public policy" within the meaning of the FTC Act.[50]

IV. Factual Background

A. The Development of "Nonprofit" OpenAI and its Massive $80 Billion Valuation

42. On December 11, 2015, Sam Altman, Elon Musk, and others founded OpenAI with $1 billion as a non-profit AI research company.[51] The organization's stated mission was to "advance digital intelligence in the way that is most likely to benefit humanity as a whole, unconstrained by a need to generate financial return."[52] Its stated work focus was on making a "positive human impact."[53]

[44] *Id.* at 75191.
[45] *Id.* at 75192.
[46] *Id.*
[47] *Id.*
[48] *Id.* at 75193.
[49] *Id.* at 75192.
[50] 15 U.S.C. § 45(n).
[51] Press Release, OpenAI, Introducing OpenAI (Dec. 11, 2015), https://openai.com/blog/introducing-openai.
[52] *Id.*
[53] *Id.*

43. In 2019, OpenAI launched its partnership with Microsoft.[54] In the intervening five years, Microsoft has invested approximately $13 billion into OpenAI,[55] and OpenAI's valuation has ballooned to $80 billion.[56] In the $66 billion generative AI market, OpenAI dominates with 39% of the market share.[57]

44. That same year, on March 11, 2019, OpenAI created "OpenAI LP as a hybrid of a for-profit and nonprofit–which [they] are calling a 'capped-profit' company."[58] While still being characterized as a nonprofit, this for-profit arm has enabled OpenAI to attract corporate investments and maintain its competitive advantage over market rivals like Google and Amazon.[59]

45. In 2019, OpenAI also shifted from an open-source model development approach to a closed-source approach. In a February 14, 2019, press release, OpenAI stated that, due to concerns around the malicious misuse of its models, it was changing it open-source model policy and would not publicly release their newly trained GPT-2 model.[60] Since then, OpenAI's newer models, GPT-3 and GPT-4, have remained closed-source.[61] As noted by changes to OpenAI's business structure and practices, OpenAI has been "trolled for its name,"[62] and "is now everything it promised not to be: corporate, closed-source, and for-profit."[63]

[54] *See* Press Release, OpenAI, OpenAI and Microsoft Extend Partnership (Jan. 23, 2023), https://openai.com/index/openai-and-microsoft-extend-partnership/.

[55] *See* Jordan Novet, *Microsoft's $13 billion bet on OpenAI carries huge potential along with plenty of uncertainty* (Apr. 8, 2023), https://www.cnbc.com/2023/04/08/microsofts-complex-bet-on-openai-brings-potential-and-uncertainty.html.

[56] Cade Metz et al., *OpenAI Completes Deal That Values the Company at $80 Billion*, The New York Times (Feb. 16, 2024), https://www.nytimes.com/2024/02/16/technology/openai-artificial-intelligence-deal-valuation.html.

[57] *See Generative AI Market Surpasses $66 Billion, with OpenAI and Meta AI Dominating 56% Share*, Focus On Business (Jan. 13, 2024), https://focusonbusiness.eu/en/news/generative-ai-market-surpasses-66-billion-with-open-ai-and-meta-ai-dominating-56-share/6001; *see also* Muhammad Zulhusni, *OpenAI poised for potential leap to a US$100 billion valuation*, Tech Wire Asia (Dec. 28, 2023), https://techwireasia.com/12/2023/is-openai-on-the-brink-of-reaching-a-us100-billion-valuation/.

[58] Press Release, OpenAI, OpenAI LP (Mar. 11, 2019), https://openai.com/blog/openai-lp.

[59] *See* James Broughel, *OpenAI Is Now Unambiguously Profit-Driven, and That's a Good Thing*, Forbes (Dec. 9, 2023), https://www.forbes.com/sites/jamesbroughel/2023/12/09/openai-is-now-unambiguously-profit-driven-and-thats-a-good-thing/; Devin Coldewey, *OpenAI Shifts from Nonprofit to 'Capped-Profit' to Attract Capital*, TechCrunch (Mar. 11, 2019), https://techcrunch.com/2019/03/11/openai-shifts-from-nonprofit-to-capped-profit-to-attract-capital/.

[60] Press Release, OpenAI, Better language models and their implications (Feb. 14, 2019), https://openai.com/research/better-language-models.

[61] *See* Braeden Cullen, *OpenAI: Was the Shift to Closed Source Justified?*, Hadron (Feb. 3, 2021), https://sites.imsa.edu/hadron/2021/02/03/openai-was-the-shift-to-closed-source-justified/; Alec Radford et al., *Language Models are Unsupervised Multitask Learners*, OpenAI, https://cdn.openai.com/better-language-models/language_models_are_unsupervised_multitask_learners.pdf (last visited Feb. 21, 2024); *GPT-4 is OpenAI's Most Advanced System, Producing Safer and More Useful Responses*, OpenAI (Mar. 14, 2023), https://openai.com/research/gpt-4.

[62] Steve Mollman, *OpenAI is getting trolled for its name after refusing to be open about its A.I.*, Fortune (Mar. 17, 2023), https://fortune.com/2023/03/17/sam-altman-rivals-rip-openai-name-not-open-artificial-intelligence-gpt-4/.

[63] Chloe Xiang, *OpenAI Is Now Everything It Promised Not to Be: Corporate, Closed-Source, and For-Profit*, Vice (Feb. 28, 2023), https://www.vice.com/en/article/5d3naz/openai-is-now-everything-it-promised-not-to-be-corporate-closed-source-and-for-profit.

46. In the intervening years, OpenAI has collaborated with major companies including Shutterstock, BuzzFeed, Salesforce, Atlassian, Bain & Company, Neo, and Consensus.[64] These partnerships seek to license user content as training data, further develop and train OpenAI's models, create new content, develop chatbots, and, more broadly, "'us[e] OpenAI technology' in an undefined capacity."[65]

B. FTC Scrutiny Over OpenAI's Practices

47. Since 2019, Microsoft and OpenAI have worked closely to develop AI products and services, challenging major technology rivals like Google and Amazon.[66] These major investments, along with the companies' questionable intermingling of authority,[67] have raised antitrust scrutiny and pushed the FTC to launch formal antitrust investigations into both Microsoft and OpenAI.[68]

48. In 2023, the FTC also launched an investigation into OpenAI's potential violations of consumer protection laws.[69] The initial investigation has targeted whether OpenAI has "run afoul of consumer protection laws by putting personal reputations and data at risk" by examining OpenAI's privacy and data collection practices, as well as the tendency for its GPT products to produce false information.[70] While the FTC's investigation extends to OpenAI's third-party API integrations and partnerships, the focus has, upon information and belief, remained on OpenAI's potential direct violations of antitrust or consumer laws.

C. OpenAI's Products Were Developed Via Unprecedented Web-Scraping and the Collection, Utilization, and Dissemination of Stolen Data from Millions of Consumers

49. Since launching, OpenAI has set the stage for the rapid development of generative AI technologies like natural language processing models ("NLPs"), large-language models ("LLMs"), and multimodal models using extensive consumer data.[71] One prominent example

[64] Silvia Pellegrino, *Which companies have partnered with OpenAI?*, Tech Monitor (May 15, 2023), https://techmonitor.ai/technology/companies-partnered-with-openai.

[65] *See id*.

[66] *See* Karen Weise, *How Microsoft's Satya Nadella Kept the 'Best Bromance in Tech' Alive*, N.Y. Times (Nov. 22, 2023), https://www.nytimes.com/2023/11/20/technology/openai-microsoft-altman-nadella.html.

[67] *See* Charles Duhigg, *The Inside Story of Microsoft's Partnership with OpenAI*, New Yorker (Dec. 1, 2023), https://www.newyorker.com/magazine/2023/12/11/the-inside-story-of-microsofts-partnership-with-openai.

[68] *See* Emilia David, *FTC and DOJ Reportedly Opening Antitrust Investigations into Microsoft, OpenAI, and Nvidia*, Verge (June 6, 2024), https://www.theverge.com/2024/6/6/24172868/ftc-doj-antitrust-openai-microsoft-nvidia-investigations; Harshita Mary Varghese et al., *DOJ and FTC Push to Investigate Microsoft's OpenAI Partnership – Politico*, Reuters (Jan. 19, 2024), https://www.reuters.com/technology/doj-ftc-push-investigate-microsofts-openai-partnership-politico-2024-01-19/.

[69] David Hamilton, *FTC Investigating ChatGPT Creator OpenAI Over Consumer Protection Issues*, Assoc. Press (July 13, 2023), https://apnews.com/article/openai-chatgpt-investigation-federal-ftc-76c6218c506996942282d7f5d608088e.

[70] Cat Zakrzewski, *FTC Investigates OpenAI Over Data Leak and ChatGPT's Inaccuracy*, Wash. Post (July 13, 2023), https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/; *see also* Hamilton, *supra* note 69.

[71] Ross Gruetzemacher, *The Power of Natural Language Processing*, Harv. Bus. Rev. (Apr. 19, 2022), https://hbr.org/2022/04/the-power-of-natural-language-processing.

is OpenAI's GPT-4 multimodal model, which has an estimated 1.8 trillion parameters[72] trained on both licensed content[73] and data scraped indiscriminately from the public web, such as transcriptions of millions of hours of YouTube videos.[74]

50. OpenAI has capitalized on its market position to create several AI products that take advantage of OpenAI's extensive research and training datasets. To date, OpenAI's consumer-facing products include, but are not limited to:

    (1) The GPT (Generative Pre-trained Transformer) Series (GPT-1, 2, 3, 3.5, 4, and 4o): a set of models, each trained with increasingly larger datasets, that can understand as well as generate natural language or code.[75]

    a. GPT-1: the initial model series with the ability to generate and understand natural language when given a prompt or context.
    b. GPT-2: notable for its text generation capabilities, including generating coherent and realistic sequences of text.
    c. GPT-3: improved the ability to understand the context of a given text and generate appropriate responses with natural-sounding text, write computer code, create art; and introduced few-shot learning, a machine learning framework that enables pre-trained models to make accurate predictions with only a small number of examples per class.
    d. GPT-3.5 and GPT-3.5 Turbo: optimized NLP for rapid and inexpensive chat completions and other chat-related tasks.
    e. GPT-4 and GPT-4 Turbo: improved multimodal capabilities (i.e., accepting images as inputs and processing image inputs like a text prompt) and advanced comprehension of complex prompts with human-level performance; exclusive to ChatGPT Plus users.
    f. GPT-4o: improved processing speed, performance across non-English languages, and comprehension of multiple inputs and outputs (e.g., combinations of text, audio, and images).

    (2) OpenAI Codex: an AI model trained on code, capable of understanding and translating natural language to code.[76]

    (3) OpenAI DALL-E: a model that can generate and edit images when given a natural language prompt.[77]

    (4) Whisper: a model that can convert audio into text.[78]

[72] *See* Maximilian Schreiner, *GPT-4 Architecture, Datasets, Costs and More Leaked*, Decoder (July 11, 2023), https://the-decoder.com/gpt-4-architecture-datasets-costs-and-more-leaked/.
[73] *See* Sarah E. Needleman, *Reddit to Give OpenAI Access to its Data in Licensing Deal*, Wall St. J. (May 16, 2024), https://www.wsj.com/tech/ai/reddit-signs-data-licensing-deal-with-openai-14993757.
[74] Wes Davis, *OpenAI Transcribed Over a Million Hours of YouTube Videos to Train GPT-4*, Verge (Apr. 6, 2024), https://www.theverge.com/2024/4/6/24122915/openai-youtube-transcripts-gpt-4-training-data-google.
[75] *Models*, OpenAI, https://platform.openai.com/docs/models/overview (last visited Feb. 21, 2024).
[76] Press Release, OpenAI, OpenAI Codex (Aug. 10, 2021), https://openai.com/blog/openai-codex.
[77] *Models*, *supra* note 75.
[78] *Id*.

(5) OpenAI API: a programming interface that enables third parties to integrate OpenAI models into their products and services, as well as train and develop their own AI applications.[79]

51. Using its GPT-3.5 model series as a foundation, OpenAI released ChatGPT in 2022.[80] The consumer-facing ChatGPT product was designed to enable human-like conversational dialogue,[81] but began to produce convincing fabrications and falsifications.[82] Although OpenAI's then-Chief Scientist, Ilya Sytskever, claimed that OpenAI could train ChatGPT not to hallucinate, these errors may be inherent to LLMs like ChatGPT; Yann LeCun, Silver Professor of the Courant Institute of Mathematical Sciences at New York University and Chief AI Scientist at Meta, has stated that because LLMs are designed to generate grammatically and semantically believable text that satisfies statistical consistency with a user prompt and training data, they are fundamentally incapable of functioning without hallucinating.[83]

52. On November 6, 2023, OpenAI "roll[ed] out custom versions of ChatGPT that [any user] can create for a specific purpose."[84] Through these custom GPTs, third-party developers all over the world have the ability to use OpenAI's GPT models to create their own chatbots and integrate GPT models into third-party products and services.[85]

53. After OpenAI's launch of custom GPTs, over 3 million custom chatbots were created by third-party developers, prompting OpenAI to launch the GPT Store, a uniform platform for developers to share their custom GPTs and where consumers could easily find and access them, on January 10, 2024.[86] While third-party developers are "mostly" unable to see the chats consumers input via custom GPTs, they "can access, store, and potentially utilize some other kinds of personal data [shared by users]."[87]

54. Data privacy risks stem not only from third-party GPT use, but also from OpenAI's own development, operation, and maintenance of its AI products. OpenAI's AI models rely heavily on vast data collected from and about millions of people around the world. While OpenAI has entered into several expensive content licensing deals with companies like Reddit,[88] Vox

[79] OpenAI API, *supra* note 5.
[80] *See* Press Release, OpenAI, Introducing ChatGPT (Nov. 30, 2022), https://openai.com/blog/chatgpt.
[81] Sabrina Ortiz, *What is ChatGPT and why does it matter? Here's what you need to know*, ZDNET (Feb. 20, 2024), https://www.zdnet.com/article/what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/.
[82] *See, e.g.*, Cade Metz, *Chatbots May 'Hallucinate' More Often Than Many Realize*, N.Y. Times (Nov. 16, 2023), https://www.nytimes.com/2023/11/06/technology/chatbots-hallucination-rates.html;
[83] Craig S. Smith, *Hallucinations Could Blunt ChatGPT's Success*, IEEE Spectrum (Mar. 13, 2023), https://spectrum.ieee.org/ai-hallucination.
[84] *See* Press Release, OpenAI, Introducing GPTs (Nov. 6, 2023), https://openai.com/blog/introducing-gpts.
[85] *Id*.
[86] Introducing the GPT Store, *supra* note 5.
[87] Nate Nelson, *OpenAI's New GPT Store May Carry Data Security Risks*, Dark Reading (Jan. 11, 2024), https://www.darkreading.com/cyber-risk/openai-new-gpt-store-data-security-risks.
[88] *OpenAI and Reddit Partnership*, OpenAI (May 16, 2024), https://openai.com/index/openai-and-reddit-partnership/; Sarah E. Needleman, *Reddit to Give OpenAI Access to Its Data in Licensing Deal*, Wall St. J. (May 16, 2024), https://www.wsj.com/tech/ai/reddit-signs-data-licensing-deal-with-openai-14993757.

Media,[89] and The Atlantic,[90] its training data is more often scraped from the internet without informed consent or a single notification to consumers.[91] This data includes personally identifiable information from and relating to millions of people, including children and other individuals in protected categories.[92] Of note, the data collected through indiscriminate scraping likely includes personal data released by people other than the subject of that personal data – like family members posting photos or malicious actors posting information to dox individuals. This means the individuals tied to that personal data may be wholly unaware that the information was ever public in the first place.

55. Several data theft lawsuits have been filed against OpenAI from plaintiffs alleging the company had a duty to warn and seek consumers' consent prior to scraping their personal data off the web, and for retaining, utilizing, and disseminating their data.[93] According to a recent class action lawsuit filed against OpenAI, OpenAI "secretly scrap[ed] 300 billion words from the internet, tapping 'books, articles, websites and posts–including personal information obtained without consent.'"[94] This scraped data is held in mass training datasets that have already been exposed through testing, subjecting all personal data contained within those datasets to the same heightened security risks.[95]

56. In addition to the data OpenAI stole by engaging in web scraping, it further retains and uses the data that consumers input into versions of ChatGPT and DALL-E.[96] These AI products have been shown to "regurgitate this sensitive [personal] data to others" through data leaks, undermining consumer privacy.[97] To make matters worse, an individual's personal data cannot be effectively extracted from an AI model trained on the data without retraining the model, leaving sensitive personal data vulnerable within many of OpenAI's AI products and API integrations.[98]

57. While OpenAI alleges that they "do not use or share user content for marketing or advertising purposes,"[99] they do in fact attest to the fact that consumer data is stored and used to train and

[89] *A Content and Product Partnership with Vox Media*, OpenAI (May 29, 2024), https://openai.com/index/a-content-and-product-partnership-with-vox-media/.

[90] *A Content and Product Partnership with The Atlantic*, OpenAI (May 29, 2024), https://openai.com/index/enhancing-news-in-chatgpt-with-the-atlantic/.

[91] Melissa Heikkilä, *OpenAI's Hunger for Data is Coming Back to Bite It*, MIT Technology Review (Apr. 19, 2023), https://www.technologyreview.com/2023/04/19/1071789/openais-hunger-for-data-is-coming-back-to-bite-it/.

[92] Tonya Riley, *OpenAI Lawsuit Reignites Privacy Debate over Data Scraping*, Cyberscoop (June 30, 2023), https://cyberscoop.com/openai-lawsuit-privacy-data-scraping/.

[93] Complaint at 11, *Plaintiffs v. OpenAI, Inc.,* Case No. 3:23-cv-03199 (N.D. Cal. 2023).

[94] Teresa Xie et al., *Creator of Buzzy ChatGPT is Sued for Vacuuming Up 'Vast Amounts' of Private Data to Win the 'A.I. Arm's Race,'* Fortune (June 28, 2023), https://fortune.com/2023/06/28/openai-chatgpt-sued-private-data/; *see Plaintiffs v. OpenAI, Inc.,* Case No. 3:23-cv-03199 (N.D. Cal. 2023), https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rIZH4FXwShJE/v0.

[95] Milad Nasr et al., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv (Nov. 28, 2023, 6:43 PM), https://arxiv.org/abs/2311.17035.

[96] Heikkilä, *supra* note 91; *see also Enterprise Privacy at OpenAI*, OpenAI, https://openai.com/enterprise-privacy/ (last visited Aug. 1, 2024).

[97] *Id*.

[98] *Id*.

[99] *Data Usage for Consumer Services FAQ*, OpenAI, https://help.openai.com/en/articles/7039943-data-usage-for-consumer-services-faq (last visited Oct. 8, 2024).

improve their products. Further, their Privacy Policy is devoid of any assurance that consumer data will not be shared with other users, third parties, service providers, or affiliates for non-marketing.[100] On the contrary, OpenAI asserts that it "may provide [users'] Personal information to third parties without further notice to [users], unless required by the law."[101] OpenAI's conflicting and surreptitious data use and sharing policy statements may, themselves, constitute unfair or deceptive acts or practices under recent FTC interpretations.[102]

58. OpenAI's GPT models and API integrations magnify these risks as they continue to collect, incorporate, disseminate, and expose consumer data to third parties without independently verifying third parties' data privacy and security practices.[103] These practices not only expose personal data to third-party end-users, but also enable third-party developers to "access, store, and potentially utilize some other kinds of personal data [consumers] share" without restrictions or guardrails.[104]

D. OpenAI's Products Are Known to Produce Confabulations and Biased or Discriminatory Outputs

59. AI confabulations (colloquially referred to as "hallucinations' or "fabrications")[105] occur when generative AI language models like GPT-4 generate semantically credible but ultimately false information in response to a user prompt.[106] Because these large language models function by analyzing the semantic meaning of user prompts and stringing word tokens together from training data to answer the prompt, they can produce confabulations when there are mismatches or ambiguities between user prompts and training data, or when the model has "insufficient, outdated, or low-quality training data" on the topic of the user prompt.[107]

60. AI confabulations not only erode user trust, but also raise serious concerns for anyone seeking reliable and accurate information—including from third parties that may use OpenAI's AI products. For example, OpenAI's ChatGPT has been shown to combine words, names, and ideas that appear semantically connected—but were in fact not connected and therefore erroneous—into false simulacrums of important public records.[108] In one instance, ChatGPT

[100] *Privacy Policy*, OpenAI (Nov. 14, 2023), https://openai.com/policies/privacy-policy.
[101] *Id.*
[102] *See, e.g.*, FTC Off. Tech. & Div. Priv. & Identity Prot., *AI (and other) Companies: Quietly Changing Your Terms of Service Could be Unfair or Deceptive*, FTC Tech. Blog (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.
[103] Nelson, *supra* note 87.
[104] *Id.*
[105] EPIC has chosen to refer to these errors as confabulations to conform with NIST's approach and avoid anthropomorphizing generative AI technologies. *See* NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* 4 (NIST AI 600-1, July 2024), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.
[106] *See* NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1, 3 (2024), https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf (initial public draft); Elena Alston, *What Are AI Hallucinations and How Do You Prevent Them?*, Zapier (Sept. 5, 2023), https://zapier.com/blog/ai-hallucinations/.
[107] *Id.*
[108] David Schardt, *ChatGPT is Amazing. But Beware its Hallucinations!*, Ctr. for Sci. Pub. Int. (Mar. 20, 2023), https://www.cspinet.org/blog/chatgpt-amazing-beware-its-hallucinations.

recently "cited a half dozen fake court cases while [a lawyer was] writing a 10-page legal brief."[109]

61. Although OpenAI has amassed massive amounts of data from millions of people around the world, the data it uses to develop and train its AI products still lacks demographic representation such that they systematically produce outputs biased against historically disadvantaged groups of people.[110] In addition, the lack of review and curation associated with mass data scraping often leads to false, offensive, biased, and discriminatory data being included in the training dataset. Because all of OpenAI's AI products are trained using similar datasets, the biases, exclusions, and negative stereotypes present within biased training data are baked into their models and difficult to effectively remove without retraining the models.[111]

62. Because the data used to train OpenAI's models are not representative of all groups of people, the outputs and decisions made by OpenAI's models are inherently biased.[112] These biases extend beyond facially biased outputs; "algorithmic bias [also] occurs when algorithms make decisions that systematically disadvantage certain groups of people."[113]

63. These systemic biases not only magnify confabulations within OpenAI's AI products, but also "create unfair outcomes, such as privileging one arbitrary group of users over others."[114] For example, banks' integration and application of OpenAI's models to assist in determining the creditworthiness of individuals based on subjective questions or biased credit data can have serious ramifications for low-income people of color.[115]

64. Of note, in an analysis of more than 5,000 AI images, it was found that "images associated with higher-paying job titles featured people with lighter skin tones, and that results for most professional roles were male-dominated."[116] In a similar example, a request for images of "a person at social services" resulted in images predominantly featuring people of color, while a request for "a productive person" resulted in white males only.[117]

[109] Metz, *supra* note 82.
[110] Cheyenne DeVon, *'AI doesn't know good from wrong,' says tech expert–why AI bias happens, and how to fix it*, CNBC (Dec. 16, 2023), https://www.cnbc.com/2023/12/16/how-to-reduce-ai-bias-according-to-tech-expert.html.
[111] Abid Ali Awan, *What is Algorithmic Bias?*, Data Camp (July 17, 2023), https://www.datacamp.com/blog/what-is-algorithmic-bias.
[112] *Understanding algorithmic bias and how to build trust in AI*, PWC (Jan. 18, 2022), https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html.
[113] Simon Friss et al., *Eliminating Algorithmic Bias Is Just the Beginning of Equitable AI*, Harv. Bus. Rev. (Sept. 29, 2023), https://hbr.org/2023/09/eliminating-algorithmic-bias-is-just-the-beginning-of-equitable-ai.
[114] *Id.*
[115] Nicol Turner Lee et al., *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings Inst. (May 22, 2019), https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.
[116] Victoria Turk, *How AI Reduces the World to Stereotypes*, Rest of World (Oct. 10, 2023), https://restofworld.org/2023/ai-image-stereotypes/
[117] Nitasha Tiku et al., *These Fake Images Reveal How AI Amplifies our Worst Stereotypes*, Wash. Post (Nov. 1, 2023), https://www.washingtonpost.com/technology/interactive/2023/ai-generated-images-bias-racism-sexism-stereotypes/.

65. These biases extend beyond AI image generation as well. A study recently published by the U.S. Department of Commerce found that racial and ethnic minorities are misidentified by AI technologies more often than white people.[118] Similarly, NLPs (natural language processors) "have been found to demonstrate racial, gender and disability bias."[119]

66. OpenAI's DALL-E, a generative AI image system that "can create realistic images and art from a description in natural language,"[120] has produced biased images of this type.[121] As with ChatGPT, the source of the bias in DALL-E is rooted in the data OpenAI scrapes from the web, namely "billions of pairs of images and their captions,"[122] as well as licensed images from third-party sources like Shutterstock.[123] While OpenAI acknowledged this issue and proposed a solution, it still fails to address the root cause of model bias, which is grounded in the biased datasets OpenAI uses to train its models.[124]

E. Through API Integration, OpenAI's Products Are Made Accessible to Millions of Third-Party Developers and Tech Giants at an Alarming Rate

67. On June 11, 2020, OpenAI released an API for third-party developers to access new AI models developed by OpenAI.[125] In other words, OpenAI's API serves as the "bridge" for third parties to access and incorporate OpenAI's generative AI models into their own existing products or for use in developing entirely new products.[126]

68. OpenAI's API integration grants businesses around the world the opportunity to build their own chatbots and deploy them in consumer-facing settings across industries.[127] At $0.20 per 1 Gigabyte per day for Assistants API (the platform that allows developers to build AI assistants such as chatbots within their own applications), the costs incurred by developers are relatively low, especially considering the potential profitability of such systems when disseminated widely.[128]

69. This developer's "gold rush" has magnified the consumer protection issues surrounding OpenAI's AI products, including data security, privacy, transparency, and accountability,[129]

[118] Victoria Burton-Harris et al., *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart.
[119] *Understanding algorithmic bias and how to build trust in AI*, *supra* note 112.
[120] *DALL-E2*, OpenAI, https://openai.com/dall-e-2 (last visited Oct. 8, 2024).
[121] Press Release, OpenAI, Reducing bias and improving safety in DALL-E2 (July 18, 2022), https://openai.com/blog/reducing-bias-and-improving-safety-in-dall-e-2.
[122] *Id.*
[123] *See* Emma Roth, *OpenAI's DALL-E Will Train on Shutterstock's Library for Six More Years*, Verge (July 11, 2023), https://www.theverge.com/2023/7/11/23791528/openai-shutterstock-images-partnership.
[124] *Id.*
[125] OpenAI API, *supra* note 5.
[126] Arunn Thevapalan, *A Beginner's Guide to The OpenAI API: Hands-On Tutorial and Best Practices*, Data Camp (Oct. 18, 2023), https://www.datacamp.com/tutorial/guide-to-openai-api-on-tutorial-best-practices.
[127] *Id.*
[128] *Pricing*, OpenAI, https://openai.com/pricing (last visited Oct. 8, 2024); *see also* Cade Metz et al., *supra* note 56.
[129] *See* Sean Lee, *Be VERY Concerned by the GPT Store*, Summit Sec. Group (Jan. 29, 2024), https://summitinfosec.com/blog/be-very-concerned-by-the-gpt-store/.

because the pre-trained AI models that OpenAI offers for API integrations are all models trained on the same biased datasets described above. The myriad data OpenAI scrapes indiscriminately from the web, which often includes personally identifiable and sensitive information, is now being disseminated to third-party developers and deployers that can exploit OpenAI's AI products to access, mishandle, and misuse such sensitive data.[130]

70. For example, when consumers using one custom GPT developed by a third party using OpenAI's baseline offerings uploaded "any file" to the custom GPT, the third-party developer and other malicious actors competent in prompt engineering could immediately gain access to that file without the consumer's knowledge.[131] Prompt engineering enables anyone with "enough know-how [to] manipulate the [GPT] into providing the system prompt, files, and resources it has been given by the creator [i.e., the user]."[132] To illustrate this, the CEO of Harmonic Security, Alastair Paterson, recently discovered that data submitted to Doc Maker (a GPT available on the GPT Store) "ends up at aidocmaker.com's servers" and is accessible to other Doc Maker users.[133]

71. The number of custom GPTs has skyrocketed since the launch of OpenAI's GPT Store on January 10, 2024. There are already over 3 million custom GPTs, many in the form of virtual assistants, image recognition systems, or other ChatGPT-styled chatbots.[134]

72. Third-party developers do not always create custom GPTs alone, either. With a mission to maximize their profits, OpenAI has partnered with several major companies like Snap, Spotify, Stripe, Slack, and Microsoft to engage in coordinated API integrations.[135] Through these integrations, OpenAI gathers, *inter alia*, image and location data from Snapchat, music preferences from Spotify, financial information from Stripe, and private conversations from Slack and Microsoft Teams.[136]

73. OpenAI's partnership with Microsoft led to the development of Azure OpenAI Service, a platform that now enables third-party developers to design and build their own AI chatbots.[137] For example, TikTok spent roughly $20 million per month to access OpenAI's models through the Azure OpenAI Service and integrate them into the TikTok platform.[138] Other Azure OpenAI Service clients include TurboTax's Intuit and Walmart.[139]

[130] *See, e.g.*, Vilius Petkauskas, *Anti-Scam Firm Exposes OpenAI API Key*, Cybernews (Mar. 22, 2024), https://cybernews.com/security/certyai-leaks-openai-api-keys/.

[131] Ian Perez, *The Hidden Risks of Uploading Files to Custom GPT Models on the GPT Store*, LinkedIn (Jan. 17, 2024), https://www.linkedin.com/pulse/hidden-risks-uploading-files-custom-gpt-models-store-ian-perez-9qooc/.

[132] *Id.*

[133] Erik van Klinken, *"GPT Store poses threat to privacy and security,"* TechZine (Jan. 12, 2024), https://www.techzine.eu/news/privacy-compliance/115284/gpt-store-poses-threat-to-privacy-and-security/.

[134] Introducing the GPT Store, *supra* note 5.

[135] Poritz, *supra* note 4.

[136] *Id.*

[137] *Azure AI Bot Service*, Microsoft Azure, https://azure.microsoft.com/en-us/products/ai-services/ai-bot-service (last visited Oct. 9, 2024).

[138] Aaron Holmes, *TikTok Spending Drove Microsoft's Booming AI Business*, Info. (July 31, 2024), https://www.theinformation.com/articles/tiktok-spending-drove-microsofts-booming-ai-business.

[139] *Id.*

74. Similarly, in February 2023, Snap used a partnership with OpenAI to build and deploy their own AI-enabled chatbot, "My AI."[140] A few months later, Snap's partnership with OpenAI led to the development of a ChatGPT Remote API for Snapchat Lenses,[141] which allowed Snapchat users to leverage the features of ChatGPT in Snapchat's lens and filter features.[142]

75. With over 750 million free Snapchat users who can access My AI and the free ChatGPT Remote API for Snapchat Lenses,[143] the consumer privacy and safety risks of OpenAI's models were magnified. Currently, approximately 20 million teenagers—46% of thirteen to seventeen-year-olds in the United States—use Snapchat almost daily.[144]

76. Snap conceded in a press release that "[a]s with all AI-powered chatbots, My AI is prone to hallucinations and can be tricked into saying just about anything."[145] Rather than confirming they were working on fixing the issue, or, better yet, delaying the launch of their OpenAI API integrations to resolve the issue, Snap simply told its users, "sorry in advance!"[146]

77. This flippant response is especially concerning for minors using My AI. Since the launch of Snap's collaboration with OpenAI in early 2023, Snapchat users have shared public anecdotes relating how My AI has scared them through "horrifying hallucinations"[147] and "weird"[148] or "creepy"[149] messages. For instance, My AI was found to have instructed a 13-year-old child

[140] Alex Kantrowitz, *Snapchat's New AI Chatbot Shows: It's All About the APIs*, LinkedIn Post (Feb. 28, 2023), https://www.linkedin.com/pulse/snapchats-new-ai-chatbot-shows-its-all-apis-alex-kantrowitz/.

[141] Dina Bass, *OpenAI Makes ChatGPT Available for Companies to Integrate in Apps*, Bloomberg Law (Mar. 1, 2023), https://www.bloomberg.com/news/articles/2023-03-01/openai-makes-chatgpt-available-for-companies-to-integrate-in-apps.

[142] Aisha Malik, *Snap's latest version of its AR development tool includes a ChatGPT API, boosted productivity and more*, TechCrunch (Nov. 9, 2023), https://techcrunch.com/2023/11/09/snaps-latest-version-of-its-ar-development-tool-includes-a-chatgpt-api-boosted-productivity-and-more/.

[143] Alex Heath, *Snapchat is releasing its AI chatbot to everyone for free*, Verge (Apr. 19, 2023), https://www.theverge.com/2023/4/19/23688913/snapchat-my-ai-chatbot-release-open-ai.

[144] *See* Clare Duffy, *Snapchat isn't just for teens anymore. Now it needs to make some real money*, CNN (Oct. 19, 2023), https://www.cnn.com/2023/10/19/tech/snapchat-user-growth/index.html.

[145] Press Release, Snap, Say Hi to My AI (Feb. 27, 2023), https://newsroom.snap.com/say-hi-to-my-ai.

[146] *Id.*

[147] *See* Satyen K Bordoloi, *The hilarious & horrifying hallucinations of AI*, Sify.com (Feb. 7, 2023), https://www.sify.com/ai-analytics/the-hilarious-and-horrifying-hallucinations-of-ai/.

[148] *See* Tim Marcin, *Microsoft's Bing AI chatbot has said a lot of weird things. Here's a list.*, Mashable (Feb. 12, 2023), https://mashable.com/article/microsoft-bing-ai-chatbot-weird-scary-responses; *Alright, time to fess up, what's the WEIRDEST conversations you had with the AI?*, Reddit (May 2023), https://www.reddit.com/r/CharacterAI/comments/147sd0p/alright_time_to_fess_up_whats_the_weirdest/.

[149] Daswin de Silva, *Snapchat's 'creepy' AI blunder reminds us that chatbots aren't people. But as the lines blur, the risks grow*, Conversation (Aug. 18, 2023), https://theconversation.com/snapchats-creepy-ai-blunder-reminds-us-that-chatbots-arent-people-but-as-the-lines-blur-the-risks-grow-211744.

"how to lie to her parents about a trip with a 31 [year old] man," and "how to make losing her virginity on her 13th bday special (candles and music)."[150]

78. Moreover, Snap's My AI raises severe user privacy and safety concerns because it collects and stores conversations—including those of minors—"indefinitely."[151] These conversations cannot be deleted without manually changing a setting in the Snapchat app, and even then, Snap's My AI data use policy suggests that user data may be used to train and improve Snap products in ways that cannot be deleted or reverted when user data is deleted.[152]

79. In addition to the data users input into My AI, Snapchat also tracks users' precise location,[153] despite many users who "are desperately trying to delete it."[154] For instance, users allege that "Snapchat's new AI knows your current location at all times with location services off, and immediately lies to you when you ask how it knows."[155]

80. Because OpenAI retains control over the underlying technology and operation of ChatGPT, the GPT Store, and OpenAI's API, all third parties are required to go through OpenAI to purchase an "API key" to access the ChatGPT API, after which developers can modify and integrate the underlying model within consumer-facing products as desired. Given limitations in API integration—and considering ChatGPT is the "world's most comprehensive [LLM]"[156]—third party developers are limited in their options and largely forced to utilize OpenAI's technology. For example, neither custom GPTs nor API integrations permit third party customers to correct OpenAI's underlying model, which serves as the source of most data security vulnerabilities, confabulations, and other errors and misrepresentations within third-party chatbots.

[150] @tristanharris, Twitter (Mar. 10, 2023, 4:07 PM), https://twitter.com/tristanharris/status/1634299911872348160.

[151] Sachin Ravikumar, *Snapchat's AI chatbot may pose privacy risk to children, says UK watchdog*, Reuters (Oct. 6, 2023), https://www.reuters.com/technology/uk-regulator-issues-notice-snapchat-over-privacy-risks-posed-by-ai-chatbot-2023-10-06/.

[152] *What is My AI on Snapchat and How Do I Use It?*, Snapchat Support, https://help.snapchat.com/hc/en-us/articles/13266788358932-What-is-My-AI-on-Snapchat-and-how-do-I-use-it (last visited Aug. 1, 2024); *see also UK watchdog alerts: Snap's AI chatbot jeopardizes privacy, especially for children*, AdGuard (Oct. 10, 2023), https://adguard.com/en/blog/uk-snapchat-privacy-children-myai.html; *Does Snap save content shared with My AI?* Snapchat Support, https://help.snapchat.com/hc/en-us/articles/15682296562836-Does-Snap-save-content-shared-with-My-AI (last visited Feb. 22, 2024).

[153] *How My AI Uses Location Data*, Snapchat, https://help.snapchat.com/hc/en-us/articles/15051407058068-How-My-AI-Uses-Location-Data (last visited Oct. 8, 2024).

[154] Saqib Shah, *Snapchat's My AI chatbot is making people paranoid as it 'knows your current location,* Standard (Apr. 28, 2023), https://www.standard.co.uk/news/tech/snapchat-my-ai-chatbot-making-people-paranoid-b1076287.html.

[155] @J_Lee_Design, Twitter/X (Apr. 20, 2023, 2:07 AM), https://twitter.com/J_Lee_Design/status/1648931393651572736.

[156] Justin Davis, *Navigating the Rising Challenges of ChatGPT*, Forbes (Feb. 29, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/02/29/navigating-the-rising-challenges-of-chatgpt/.

F. OpenAI's Flawed Data Security and Business Practices Have Placed the Personally Identifiable Information of Millions of People at Risk

81. In addition to scraping millions of data points from the web in order to train and develop its models, OpenAI also collects data from the approximately 180.5 million people who currently use ChatGPT (of whom around 100 million use it on a weekly basis).[157] As stated in its Privacy Policy, OpenAI collects personal information including, but not limited to, users' names, contact information, payment card information, input or file uploads, the contents of any messages users send through OpenAI's AI products, social media information, and analytics including a user's IP address, browser type and settings, and precise location.[158] OpenAI asserts that it "may provide [users'] Personal information to third parties without further notice to [users], unless required by the law."[159]

82. In its Privacy Policy, OpenAI details the purported rights users have when using its services, but these purported rights are typically only available to users based on their location and citizenship. For example, OpenAI is required to comply with the European Union's General Data Protection Regulation ("GDPR"), which provides strong data use, collection, and security measure requirements for processing EU users' personal data. However, even with these protections, OpenAI's compliance with the GDPR appears to be deficient. For example, after temporarily banning ChatGPT and a multi-month investigation, Italy's Data Protection Authority raised serious allegations of GDPR violations by OpenAI.[160]

83. In particular, the GDPR requires that entities processing personally identifiable information—such as OpenAI—do so under one of the recognized valid legal bases.[161] For example, OpenAI has never sought consent for its personal data processing from millions of web users, much less notified consumers that their data was being collected. Instead, OpenAI has broadly relied on showing a "legitimate interest" for processing user data—a notoriously ill-defined and highly litigated legal basis under the GDPR.[162] Further, OpenAI gives no public legal basis for the data scraping at all. As a result, OpenAI has received significant and ongoing scrutiny from European regulators for violating European privacy laws.[163]

84. Furthermore, OpenAI's Privacy Policy states that "individuals *may* have" certain privacy rights in relation to their personal information, including the right to request deletion of it, to correct it, or to know the specific pieces of data OpenAI has of them.[164] To request removal of users' personal data, OpenAI creates a false illusion that anyone can submit a removal request form and have their data successfully deleted. However, this service is severely restricted to only

[157] Fabio Duarte, *Number of ChatGPT Users (Feb 2024)*, Exploding Topics (Feb. 2, 2024), https://explodingtopics.com/blog/chatgpt-users.

[158] *Privacy Policy*, *supra* note 100.

[159] *Id.*

[160] Natasha Lomas, *ChatGPT is violating Europe's privacy laws, Italian DPA tells OpenAI*, Tech Crunch (Jan. 29, 2024), https://techcrunch.com/2024/01/29/chatgpt-italy-gdpr-notification/.

[161] *Id.*

[162] *Europe Privacy Policy,* OpenAI, (Dec. 15, 2023), https://openai.com/policies/eu-privacy-policy/ (see Section 8).

[163] Natasha Lomas, *supra* note 160.

[164] *Privacy Policy*, *supra* note 100.

citizens and residents of certain jurisdictions.[165] Of note, only a select 35 countries are listed, with the United States not being one of them.[166]

85. OpenAI's data removal request form also imposes undue burdens for users, as it requires users to show clear evidence of any data processing and relevant prompts, screenshots, and sworn statements. Importantly, OpenAI includes an acknowledgment that even where this evidence is provided "OpenAI may not, in all cases, delete the data."[167] Moreover, OpenAI only allows users to delete their prompt data and related data from answers that ChatGPT provides to other users; it does not permit users to request the deletion of their personal data included in OpenAI's training datasets.[168]

86. Another avenue for potential data breaches and security risks is OpenAI's GPT Store, which enables and promotes millions of third-party developers to design and deploy their own custom chatbots using OpenAI's technology. While OpenAI claims that "[third-party] builders will not have access to specific [user] conversations [exchanged] with the GPTs to ensure user privacy,"[169] examples of OpenAI data leaks and AI confabulations[170] suggest that data privacy and security risks remain in custom GPTs within the GPT Store.

87. Third-party developers can integrate OpenAI's GPT API into their own applications or systems, thus enabling third-party users to interact with the GPT model directly. When using OpenAI's APIs, much, if not all, of the end-user data being processed by the third-party developer is shared back with the API provider, OpenAI.[171]

88. As a result of these data privacy and security vulnerabilities, OpenAI places the personal information of millions of individuals at risk each day. The consequences of these risks were witnessed in 2023, when OpenAI experienced a data leak to its source code. This compromised the personally identifiable information and credit card data of millions of consumers worldwide, allowing ChatGPT users to see other active users' information.[172]

89. Considering OpenAI's data leak occurred only a few days after launching its then-newest model, GPT-4, these risks are likely to persist across OpenAI's existing and forthcoming

[165] Matt Burgess, *How to Delete Your Data From ChatGPT*, Wired (May 9, 2023), https://www.wired.com/story/how-to-delete-your-data-from-chatgpt/.
[166] *OpenAI Personal Data Removal Request*, OpenAI, https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30 (last visited Oct. 9, 2024).
[167] Burgess, *supra* note 165.
[168] *See OpenAI Privacy Request Portal*, OpenAI (Jan. 12, 2024), https://privacy.openai.com/policies; MacsHeadroom, *OpenAI Personal Data Removal Request Form*, Hacker News, https://news.ycombinator.com/item?id=35814480 (last visited Oct. 9, 2024).
[169] *GPTs Data Privacy FAQs*, OpenAI, https://help.openai.com/en/articles/8554402-gpts-data-privacy-faqs (last visited Oct. 9, 2024).
[170] *See* Cade Metz, *A Hacker Stole OpenAI Secrets, Raising Fears That China Could, Too*, N.Y. Times (July 4, 2024), https://www.nytimes.com/2024/07/04/technology/openai-hack.html; Anuj Mudaliar, *ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack*, Spiceworks (Feb. 1, 2024), https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/.
[171] Nelson, *supra* note 87.
[172] Press Release, OpenAI, March 20 ChatGPT Outage: Here's What Happened Blog (Mar. 24, 2023), https://openai.com/blog/march-20-chatgpt-outage.

models. Importantly, unlike with GPT-3 and older models, OpenAI has ceased publication of any details regarding the data being used to train these newer and larger models.[173] Without transparency or regulation, OpenAI's business practices pose serious risks and concerns for the public at large.

G. OpenAI's API Enables the Integration of OpenAI's Biased Technology into the Real Estate and Financial Services Industries

90. When an inherently biased AI algorithm is integrated into massive industries like financial services and real estate, the consequences can be disastrous for systematically disadvantaged groups of people.[174] In the financial services industry, for example, AI is currently being implemented to aid in a variety of tasks, including, but not limited to, fraud detection, real-time transaction monitoring, automating credit checks, and establishing chatbot virtual assistants.[175] This technology is also being used to analyze a host of data including customer behavior, market trends, and investment portfolios.[176]

91. Recently, Microsoft's $13 billion investment in OpenAI gave the company an edge as a supplier of generative AI technologies for financial institutions because of its "deep pockets"—and because many financial institutions already use Microsoft's Azure cloud computing platform.[177] For example, in September 2023, Morgan Stanley launched their own AI assistant—using OpenAI's technology—to streamline administrative and research tasks for financial advisors and support staff.[178]

92. Morgan Stanley's launch of AI assistants, along with similar launches by major banks like JPMorgan Chase & Co., Citigroup Inc., and Goldman Sachs, comes after the launch of OpenAI's enterprise tier of AI products, which "provides businesses with GPT-4 access featuring no usage caps, faster performance, and API credits."[179]

93. The consequences of integrating OpenAI's AI products into financial products and services have already begun. For example, "[t]he [2023] MeridianLink ransomware breach spotlighted the risks for banks relying on fintechs that haven't been fully vetted by accepted standards and protocols."[180]

94. Similarly, OpenAI's technology is being used in the real estate industry to identify investors, handle documentation, engage with customers, make hyperlocal zoning regulations, conduct

[173] Burgess, *supra* note 165.
[174] Friss, *supra* note 113.
[175] *The rise of AI in banking and finance industry: Exploring use cases and applications*, LeewayHertz, https://www.leewayhertz.com/ai-use-cases-in-banking-and-finance (last visited Oct. 9, 2024).
[176] *Id.*
[177] *See* Kate Fitzgerald, *Microsoft maneuvers to a prime role with banks in OpenAI upheaval*, American Banker (Nov. 20, 2023), https://www.americanbanker.com/news/microsoft-maneuvers-to-a-prime-role-with-banks-in-openai-upheaval.
[178] *Morgan Stanley pioneers AI assistant usage in major banks*, Yahoo Finance (Sep. 19, 2023), https://finance.yahoo.com/news/morgan-stanley-pioneers-ai-assistant-105750802.html.
[179] *Id.*
[180] Fitzgerald, *supra* note 177.

property valuations, and conduct demand forecasting.[181] Because OpenAI's API integrations rely on AI models developed and trained on unrepresentative data, real estate applications using the OpenAI API can produce or exacerbate consumer harms like discrimination, hindering consumers' ability to, *inter alia*, rent and shop for homes.[182]

95. In May 2023, OpenAI launched several specialized plugins for real estate portals that integrate OpenAI GPT functionality. However, OpenAI quickly and quietly deactivated them just one month after release after research demonstrated that the chatbots posed discrimination risks to consumers in the real estate and financial services industries.[183] For example, a 2023 report published by Redfin found evidence that OpenAI's ChatGPT could be prompted to give responses that enabled consumers to search for and filter real estate listings in ways that plainly violated the Fair Housing Act.[184]

H. OpenAI's Privacy Policy Misrepresents the Security and Accessibility of Personal Data Used to Train ChatGPT

96. Beyond the shortcomings of OpenAI's Privacy Policy listed above, OpenAI represents that "ChatGPT does not copy or store training information" and its models "do not have access to training information after they have learned from it."[185] However, a 2023 joint research study by Google DeepMind and five universities revealed that "[a]ll models… memorize at least some [training] data" and that low-cost adversarial attacks on OpenAI's deployed GPT models are effective at collecting up to a gigabyte of ChatGPT's training dataset.[186] These results suggest that not only does ChatGPT store training information in ways that it can continue to access during deployment, but also that ChatGPT may improperly disclose personally identifiable training data to third parties.

V. Legal Analysis

A. The Federal Trade Commission Act

97. Section 5 of the FTC Act prohibits unfair and deceptive acts and practices.[187]

[181] *See* Rice et al., *supra* note 5; *see also* Alison Ipswich, *Transforming Financial Services with AI in 2023: Top Technologies, Innovative Startups, and Future Trends*, Traction Technology, https://www.tractiontechnology.com/blog/openai-transforming-financial-services-top-technologies-innovative-startups-and-future-trends (last visited Oct. 9, 2024).

[182] *Id.*

[183] Harvey Hancock, *OpenAI Deactivates all Real Estate Plugins – Redfin and Zillow Affected*, Online Marketplaces (Sep. 29, 2023), https://www.onlinemarketplaces.com/articles/openai-deactivates-all-real-estate-plugins/.

[184] *See id.*; Nate Bek, *Redfin CEO recounts encounter with OpenAI's Sam Altman to warn about impact of AI on housing tech*, GeekWire (Sep. 28, 2023), https://www.geekwire.com/2023/redfin-ceo-recounts-encounter-with-openais-sam-altman-to-warn-about-impact-of-ai-on-housing-tech/.

[185] *See How ChatGPT and Our Language Models are Developed*, OpenAI, https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed (last visited Aug. 8, 2024).

[186] Nasr et al., *supra* note 95.

[187] 15 U.S.C. § 45.

98. A company engages in an unfair trade practice if the "act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[188]

99. The Commission may consider established public policies along with other evidence to determine whether a trade practice is unfair.[189]

100. Deceptive acts and practices include material representations, omissions, or practices that are likely to mislead a consumer acting reasonably in the circumstances.[190]

101. The Commission has stated that a company also violates Section 5 of the FTC Act when it furnishes others with the means and instrumentalities for the commission of unfair and deceptive acts and practices.[191]

VI. OpenAI's Apparent Violations of the FTC Act

A. OpenAI's Development, Operation, and Deployment of its Generative AI Products Constitute Direct Unfair Trade Practices Under Section 5 of the FTC Act

102. OpenAI's development, operation, and dissemination of generative AI products constitute unfair trade practices because these acts or practices cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

103. OpenAI's indiscriminate web scraping, widespread data retention, development of biased algorithms, and failure to adopt appropriate data security and accuracy testing measures are unfair because they cause, or are likely to cause, substantial injury to consumers which is neither reasonably avoidable nor outweighed by countervailing benefits to consumers or competition.

104. OpenAI's data collection practices cause, or are likely to cause, substantial injury to consumers. In the process of indiscriminately scraping, processing, and using billion of data points from the public internet, including personally identifiable information and data relating

[188] 15 U.S.C. § 45(n); *see also* FTC, Policy Statement on Unfairness (1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [hereinafter "FTC Unfairness Policy Statement"].

[189] *Id.*

[190] FTC, Policy Statement on Deception (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[191] Complaint at 41, *FTC v. Neora, LLC, Signum Biosciences, Inc., Signum Nutralogix, Jeffrey Olson, Maxwell Stock, and Jeffry Stock*, FTC File No. 162-3099 (2019), https://www.ftc.gov/system/files/documents/cases/1623099_nerium_complaint_11-1-19.pdf (deceptive acts or practices); *see also* Complaint at 24, *FTC v. Office Depot, Inc., and Support.com, Inc.*, FTC File No. 172-3023 (2019), https://www.ftc.gov/system/files/documents/cases/office_depot_complaint_3-27-19.pdf (deceptive acts or practices); Complaint at 7, *In re DesignerWare, LLC*, FTC File No. 112-3151 (2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf (unfair acts or practices); Complaint at 10–11, *FTC v. CyberSpy Software, LLC, and Trace R. Spence*, No. 08-cv-01872, 2008 WL 5157718 (M.D. Fl. Nov. 5, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf (unfair acts or practices).

to minors,[192] OpenAI continuously subjects millions of consumers to potential data leaks, data breaches, and other forms of data misuse by both OpenAI and third parties. These data practices not only deprive consumers of their ability to control their own personal data, but also increase the risk of consumer injuries resulting from harmful deepfakes, consumer fraud, reputational damage, identity theft, harassment, exploitation, discrimination, intellectual property rights violations, and more.[193]

105. OpenAI's AI development and training practices also cause, or are likely to cause, substantial injury to consumers. By training its AI models on data scraped indiscriminately from the web—without meaningful processes to test for or control data quality, accuracy, or bias—OpenAI incorporates the inaccuracies and biases of its training data into its generative AI products and services,[194] increasing the likelihood of AI-generated confabulations, errors, and biased outputs. Despite being aware of common limitations of scraped training data,[195] OpenAI has continued to rely on indiscriminately scraped data to train its models.

106. Moreover, OpenAI's failure to employ reasonable and appropriate measures to protect consumers' data—including verification of third-party data security measures—or test, evaluate, and validate its models' performance exposes consumers to harm that cannot be reasonably avoided. The nature of OpenAI's web scraping and data collection practices, its model development and deployment, and its dissemination of custom AI tools and API integrations to third parties makes avoiding harm nigh impossible. A consumer would not only need to discover that their personal data was collected and used by OpenAI to train AI models *before* a data leak, breach, or harmful use occurred through *any* impacted AI models or integrated services, but they would also need to convince OpenAI to remove their data and retrain any impacted models; due to the nature of OpenAI's AI model development, training data cannot be extracted from a model without fully retraining or deleting the model.[196]

[192] Tonya Riley, *supra* note 92.

[193] *See generally* GenAI Report I; GenAI Report II.

[194] The most clear example of this is the current phenomenon of inaccurate AI-generated data being scraped and fed back into training data sets, producing increasingly inaccurate outputs and eventual model collapse. *See, e.g.,* Aatish Bhatia, *When A.I.'s Output is a Threat to A.I. Itself,* NYT (Aug. 25, 2024), https://www.nytimes.com/interactive/2024/08/26/upshot/ai-synthetic-data.html; Elizabeth Gibney, *AI models fed AI-generated data quickly spew nonsense,* Nature (July 24, 2024), https://www.nature.com/articles/d41586-024-02420-7; Devika Rao, *AI is cannibalizing itself. And creating more AI.,* The Week (Aug. 29, 2024), https://theweek.com/tech/ai-cannibalization-model-collapse.

[195] *See, e.g.*, Deepa Seetharaman, *For Data-Guzzling AI Companies, the Internet is Too Small*, Wall St. J. (Apr. 1, 2024), https://www.wsj.com/tech/ai/ai-training-data-synthetic-openai-anthropic-9230f8d8.

[196] *See* Antonio A. Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning*, 33rd Conf. on Neural Info. Processing Sys. (Dec. 8, 2019), https://proceedings.neurips.cc/paper_files/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf ("For many standard ML models, the only way to completely remove an individual's data is to retrain the whole model from scratch on the remaining data, which is often not computationally practical."); Stephen Pastis, *A.I.'s Un-Learning Problem: Researchers Say It's Virtually Impossible to Make an A.I. Model 'Forget' The Things it Learns from Private User Data*, Fortune (Aug. 30, 2023), https://fortune.com/europe/2023/08/30/researchers-impossible-remove-private-user-data-delete-trained-ai-models/.

107. Additionally, OpenAI has provided no meaningful recourse or remedial procedure for consumers to avoid harms caused or facilitated by OpenAI's AI products and data practices. OpenAI locks consumers into high-risk circumstances in at least four ways:

a. First, while OpenAI does provide limited deletion requests for user prompt data, this affordance does not extend to personally identifiable information scraped, collected, and used for model training purposes. Consumers cannot reasonably avoid having their personally identifiable information collected, retained, and used by OpenAI.

b. Second, OpenAI does not publicize or explain in specific detail what data they have, how it is being used, and with whom that data is shared. Even if consumers did have processes to remove their data from OpenAI's products, no reasonable consumer would have access to the information they need to make an informed deletion request.

c. Third, even in instances where OpenAI does remove personally identifiable information, any AI models trained on that data can still generate outputs based on the removed data—including data leaks involving removed training data.[197] Even if a consumer could convince OpenAI to delete their personal data, any deployed AI systems trained on that data could still leak the consumer's data or misuse that data to produce harmful outputs.

d. Fourth, even if OpenAI remedies these data privacy and security concerns, it has still failed to implement effective AI testing, evaluation, or risk management procedures to mitigate inaccuracies and biases within its AI products. OpenAI's "safety practices," published on May 21, 2024, do not align with established public policies for AI risk management—which center on transparency, accuracy testing, and bias reduction measures—but instead focus on improving an undefined metric of model safety through alignment with, *inter alia*, OpenAI's Preparedness Framework, a limited risk management framework targeting only cybersecurity risks; chemical, biological, radiological, and nuclear threats; model persuasiveness; and model autonomy.[198] Addressing far-flung existential risks of AI does not mitigate the AI accuracy and bias risks facing consumers today.

108. OpenAI's data collection, model development, and model dissemination practices expose consumers to serious harm without providing countervailing benefits to consumers or competition. OpenAI collects wide swaths of personally identifiable information, including consumer names, contact information, payment card information, user content, consumer communications, and social media data, to train its various AI models without meaningful

[197] *See* Anuj Mudaliar, *ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack*, Spiceworks (Feb. 1, 2024), https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/; Cat Zakrzewski, *FTC Investigates OpenAI Over Data Leak and ChatGPT's Inaccuracy*, Wash. Post (July 13, 2023), https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/.

[198] *OpenAI Safety Update*, OpenAI (May 21, 2024), https://openai.com/index/openai-safety-update/.

consumer notice, consent, or compensation.[199] Furthermore, OpenAI's data practices have not produced AI products that are demonstrably safe for consumers; time and time again, OpenAI's AI models have leaked sensitive consumer information or produced wholly false outputs. Additionally, malicious actors can and do exploit vulnerabilities within OpenAI's AI products to intentionally deceive consumers.[200] Blinded by a desire to dominate the generative AI marketplace,[201] OpenAI has failed to adequately mitigate the risks of consumer harms that its voracious data collection practices and unconstrained AI model development produce.

109. Consumers have received no benefit for unknowingly providing the data foundation from which OpenAI has developed its various generative AI models and grown into a multi-billion-dollar company. Consumers in the U.S., specifically, are also given only minimal protection or means to opt out or request their data be removed.[202] For example, OpenAI limits its "privacy request" process, which is meant to request the removal of consumer data, to only a limited subset of data points.[203] In sum, OpenAI has collected scores of consumer data and produced unsafe AI models in order to enrich itself—without passing on any noticeable benefits to consumers or competition that would not remain with more protective data collection, AI development, and risk management practices in place.

110. Moreover, in determining whether any act or practice is unfair, the Federal Trade Commission may also consider established public policies as evidence to be considered in addition to all other evidence. Along those lines, protecting consumers' data, especially when it has been stolen without consent and subsequently utilized to develop new technologies with documented consumer risks, is crucial to upholding consumers' rights, maintaining trust and confidence in the digital marketplace, preventing the exploitation or disadvantage of consumers, imposing safeguards and regulations to promote fairness and accountability, and encouraging OpenAI to prioritize privacy, security, and ethical considerations.

111. In conclusion, OpenAI's business practices cause or are likely to cause substantial injury to consumers which are not reasonably avoidable by consumers themselves and are not outweighed by countervailing benefits to consumers or competition, thus constituting a violation of Section 5 of the FTC Act.

B. OpenAI's Engages in Deceptive Acts in Violation of Section 5 of the FTC Act When It Misrepresents its Data Collection and Use Practices and When It Knowingly Deploys AI Products that Mislead Consumers

112. Throughout its Terms of Use, Privacy Policy, and other public-facing explanatory and marketing materials, OpenAI engages in material misrepresentations and omissions that

[199] *Privacy Policy*, *supra* note 100.

[200] *See OpenAI Has Stopped Five Attempts to Misuse its AI For 'Deceptive Activity'*, Reuters (May 30, 2024), https://www.reuters.com/technology/cybersecurity/openai-has-stopped-five-attempts-misuse-its-ai-deceptive-activity-2024-05-30/.

[201] *Cf.* Dan Milmo, *Microsoft, OpenAI and Nvidia Investigated Over Monopoly Laws*, Guardian (June 6, 2024), https://www.theguardian.com/business/article/2024/jun/06/microsoft-openai-and-nvidia-investigated-over-possible-breach-of-antitrust-laws.

[202] *See* Burgess, *supra* note 165; *see also OpenAI Personal Data Removal Request*, *supra* note 166.

[203] *OpenAI Privacy Request Portal*, *supra* note 168.

constitute deceptive acts or practices under the FTC Act. For example, OpenAI falsely claims that it has implemented security protections for personal data that are not, in fact, in place. Additionally, OpenAI has claimed to comply with global privacy regulations while providing no actual means for individuals to exercise all of their data protection rights. and (2) claiming to comply with global privacy regulations while providing no actual means for individuals to exercise all of their data protection rights.

113. In its FAQ article on how ChatGPT and language models are developed, OpenAI claims repeatedly that "[m]odels do not contain or store copies of information that they learn from", "ChatGPT does not copy or store training information in a database", "[i]t does not 'copy and paste' training information", and "our models do not have access to training information after they have learned from it."[204] This is demonstrably false. An experiment by technologists and academic researchers demonstrated that certain prompts can easily get ChatGPT to reveal megabytes of raw training data.[205] This demonstrates that contrary to OpenAI's public claims, ChatGPT is, in fact, still able to directly access and reveal raw data from its training dataset—including personal data.

114. OpenAI's Privacy Policy informs individuals that they may have certain rights over their personal information. However, it also explicitly states that they may not be able to correct inaccurate information or fully remove personal data due to "the technical complexity of how our models work."[206] Privacy and consumer protection laws do not include an exception for respecting data subject rights if a company says that it's hard. Furthermore, the actual steps required to attempt to exercise data subject rights include clicking through several links in multiple web pages and the only option individuals without an OpenAI account may request is removal of output data.[207] To submit this request, you must provide your email, first and last name, the specific personal information output by ChatGPT, relevant ChatGPT prompts, the reason for removal, and place of residency. Unless an individual's raw personal data is revealed through an output, there is no method for individuals to request removal of their personal data from training datasets.

115. OpenAI also engages in deceptive acts under Section 5 of the FTC Act by developing and deploying AI products that it knows will mislead consumers. Rather than attempt to mitigate the risk of consumer deception or misrepresentation within its offerings, OpenAI simply notes on its website that "ChatGPT sounds convincing, but it might give you incorrect or misleading information" or "misrepresent different sides of an argument." These general disclaimers, without any efforts to ensure that specific outputs generated by its OpenAI's AI products do not, in fact, mislead a reasonable consumer, are insufficient to free OpenAI from any liability for deceptive acts or practices.

[204] *How ChatGPT and our language models are developed*, *supra* note 185.
[205] Nasr et al., *supra* note 95.
[206] *Privacy Policy*, *supra* note 100, at Section 2.
[207] *OpenAI Privacy Request Portal*, *supra* note 168.

C. OpenAI Provides the Means and Instrumentalities for Unfair and Deceptive Acts and Practices by Disseminating its AI Products to Third-Party Developers and Clients without Providing Safeguards to Combat Harmful Uses

116. As stated previously, a company violates Section 5 of the FTC Act not only when it pursues unfair or deceptive acts or practices itself, but also when it provides others with the means and instrumentalities for unfair and deceptive acts and practices.[208]

117. OpenAI provides the means and instrumentalities for unfair and deceptive trade practices by disseminating and integrating faulty and misrepresentation-generating AI products and services into third-party applications through, e.g., API integrations and custom GPTs.

118. OpenAI furnished third-party developers and users with the means and instrumentalities for unfair and deceptive acts and practices by developing, selling, and otherwise disseminating its API integrations, custom GPTs, and other AI products to third parties with knowledge that its AI models exhibited data security vulnerabilities and tended to produce false, biased, or misleading outputs. Without robust monitoring and mitigation procedures in place, these AI model flaws can produce or exacerbate third-party unfair and deceptive trade practices when placed in the stream of commerce. For example, faulty AI chatbots have been shown to, e.g., deceive consumers about airline deals[209] and make biased hiring and recruitment decisions.[210] When third-party chatbots are built atop OpenAI's API, OpenAI's model development practices not only facilitate unfair and deceptive practices by end-users, but also limit well-meaning end-users from mitigating—via technical interventions—any consumer harms that result.

119. Despite having knowledge of security vulnerabilities, accuracy issues, and biases within its AI models,[211] OpenAI continues to disseminate its AI products to third parties without resolving

[208] Complaint at 41, *FTC v. Neora, LLC, Signum Biosciences, Inc., Signum Nutralogix, Jeffrey Olson, Maxwell Stock, and Jeffry Stock*, FTC File No. 162-3099 (2019), https://www.ftc.gov/system/files/documents/cases/1623099_nerium_complaint_11-1-19.pdf (deceptive acts or practices); *see also* Complaint at 24, *FTC v. Office Depot, Inc., and Support.com, Inc.*, FTC File No. 172-3023 (2019), https://www.ftc.gov/system/files/documents/cases/office_depot_complaint_3-27-19.pdf (deceptive acts or practices); Complaint at 7, *In re DesignerWare, LLC*, FTC File No. 112-3151 (2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf (unfair acts or practices); Complaint at 10–11, *FTC v. CyberSpy Software, LLC, and Trace R. Spence*, No. 08-cv-01872, 2008 WL 5157718 (M.D. Fl. Nov. 5, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf (unfair acts or practices).

[209] *See, e.g.*, Maria Yagoda, *Airline Held Liable for its Chatbot Giving Passenger Bad Advice—What This Means for Travellers*, BBC (Feb. 23, 2024), https://www.bbc.com/travel/article/20240222-air-canada-chatbot-misinformation-what-travellers-should-know.

[210] *See* Zhisheng Chen, *Ethics and Discrimination in Artificial Intelligence-Enabled Recruitment Practices*, 10 Hums. & Soc. Scis. Commc'ns, 2023, at 9–10, https://www.nature.com/articles/s41599-023-02079-x; Jeffrey Dastin, *Insight – Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Reuters (Oct. 10, 2018), https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/.

[211] *See Our Approach to AI Safety*, OpenAI (Apr. 5, 2023), https://openai.com/index/our-approach-to-ai-safety/; Press Release, OpenAI, How should AI systems behave, and who should decide? (Feb. 16, 2023), https://openai.com/blog/how-should-ai-systems-behave; Metz, *supra* note 170.

those vulnerabilities, accuracy issues, and biases. These third parties span industries with real and substantial consumer impacts, including real estate and the financial services sector.[212]

120. Third party developers are largely reliant on the generative AI models created and operated by OpenAI. Without the ability to significantly modify OpenAI's underlying technology, third party users cannot meaningfully remedy issues incorporated within OpenAI's models—nor are they restricted from misusing OpenAI's tools to produce scams, convincing consumer misinformation, or other outputs in violation of the FTC Act.

121. Consumers cannot reasonably avoid the harms that OpenAI facilitates when it furnishes its AI products to third parties either. When third parties acquire or incorporate OpenAI's AI products into their own products and services, OpenAI neither validates the data security measures and responsible use policies of those third parties or provide information necessary for those third parties to evaluate the accuracy, reliability, proper uses of OpenAI's AI products,[213] meaning that exploitable flaws and vulnerabilities within OpenAI's models remain within third-party AI products and services.

122. Despite the unresolved consumer risks inherent to OpenAI's dissemination of AI products to third parties, consumers do not receive any corresponding benefit for being subject to AI chatbots and other products or services built atop OpenAI's technologies. While OpenAI collects extensive personal data about consumers—and subjects them to risks of data security vulnerabilities, discrimination, deception, and other consumer harms—the purported benefits of OpenAI's AI products flow only to its corporate clients and funders.

VII. Prayer for Investigation and Relief

123. EPIC urges the Commission to investigate OpenAI to determine if OpenAI, by developing, deploying, selling, and disseminating its generative AI models, has engaged in unfair and deceptive trade practices under Section 5 of the FTC Act. At a minimum, the FTC should investigate to what extent OpenAI, by itself or by providing the means and instrumentalities for third-party deployers of OpenAI's AI products, engages in the following practices:

a. Collecting, retaining, and using personally identifiable information without consumers' awareness, knowledge, or consent;

b. Collecting, retaining, and using consumer data without investigating the data's accuracy, completeness, or bias;

c. Misrepresenting its data collection practices, AI development practices, or the functionality and reliability of its existing AI products;

[212] *See* Rice et al., *supra* note 5; LeewayHertz, *supra* note 175.
[213] Nelson, *supra* note 87.

d. Knowingly developing AI products that can generate unfair or deceptive outputs, either during normal use or after a third party exploits flaws and vulnerabilities within the AI products;

e. Failing to incorporate sufficient AI risk mitigation practices to prevent consumer harm by its deployed AI products;

f. Failing to validate third-party clients' security measures or AI use policies prior to disseminating its AI products for their use; and

g. Filing to provide third-party deployers with information sufficient to responsibly implement or incorporate its AI products without producing consumer harms.

124. EPIC further urges the Commission to:

a. Require OpenAI to comply with established public policy frameworks for responsible AI development and use, including the OECD AI Principles, the Universal Guidelines for AI, and Executive Order 14110;

b. Require OpenAI to halt any unlawful or impermissible data collection, retention, use, and disclosure, including disclosures through data leaks;

c. Require OpenAI to implement and maintain an effective AI testing, evaluation, and monitoring program to detect and mitigate errors or biases within OpenAI's generative AI models both before and during deployment;[214]

d. Require OpenAI to notify any third-party developers and deployers of its AI products about its testing, evaluation, and monitoring obligations;

e. Require OpenAI to facilitate any third-party developer or deployer AI testing, evaluation, or monitoring that is required to ensure OpenAI's compliance with the foregoing obligations;

f. Require OpenAI to delete, disgorge, or destroy any data, models, or algorithms related to their generative AI models that are either derived from illegally collected, retained, or used consumer data or deployed in ways that impose an impermissible risk of errors, biases, or other consumer harms;[215]

g. Prohibit OpenAI from misrepresenting in any manner, expressly or by implication, the accuracy of their generative AI models or the extent or security of their data collection, retention, and use practices;

[214] This monitoring program could mirror similar AI monitoring programs mandated by FTC orders. *See, e.g.,* Administrative Decision and Order at 6-7, *In re Rite Aid Corp*., FTC File No. 072-3121 (2023).

[215] *See id*. at 6–7.

h. Require OpenAI to obtain initial and ongoing AI audits of their generative AI models from a "qualified, objective, independent third-party professional" who "uses procedures and standards generally accepted in the profession;"[216]

i. Require OpenAI to provide such other information or documentation which may be necessary to ensure compliance with the aforementioned monitoring and notice obligations, including but not limited to compliance reports, model cards, and incident reports;[217] and

j. Provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

<u>*/s/ John Davisson*</u>
John Davisson
Director of Litigation
davisson@epic.org

<u>*/s/ Calli Schroeder*</u>
Calli Schroeder
Senior Counsel
schroeder@epic.org

<u>*/s/ Grant Fergusson*</u>
Grant Fergusson
Counsel
fergusson@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

[216] *See id*. at 21–23.
[217] *See id*. at 24–26.