FEDERAL TRADE COMMISSION
Washington, DC 20580

In the matter of	)
	)
OpenAI, Inc.	)
	)

Supplement to the Original Complaint

Submitted by

The Center for Artificial Intelligence and Digital Policy (CAIDP)

I. Summary

1. On March 30, 2023, the Center for AI and Digital Policy filed a Complaint with the Federal Trade Commission regarding the company OpenAI and the AI product GPT-4.[1] CAIDP alleged that OpenAI's business practices constitute "unfair and deceptive practices" under Section 5 of the FTC Act and violate FTC's published guidance for AI products.[2]

2. CAIDP urged the Commission to open an investigation into OpenAI and to halt the further deployment of ChatGPT pending compliance with the FTC's announced practices.

3. CAIDP stated that it would reserve the right to amend the Complaint, "as other information, relevant to this matter, becomes available."[3]

[1] Center for AI and Digital Policy, https://www.caidp.org/
[2] CAIDP, *FTC Complaint, in the matter of Open AI, Inc*. (March 30, 2023), https://www.caidp.org/app/download/8450269463/CAIDP-FTC-Complaint-OpenAI-GPT-033023.pdf. Background concerning this matter is available at CAIDP, In the Matter of OpenAI, https://www.caidp.org/cases/openai/
[3] Id. at par. 166.

4. ChatGPT is the fastest growing consumer product in history.[4] According to the FTC, "[w]ithin just a few months, generative AI chatbots and applications have launched and scaled across industries and reached hundreds of millions of people. AI is increasingly becoming a basic part of daily life."[5]

5. At the time CAIDP filed the original complaint, there were no formal investigations of OpenAI and ChatGPT or legal proceedings in the U.S. or elsewhere.

6. Subsequent to the filing of the CAIDP Complaint, consumer agencies around the world have launched investigations of ChatGPT.[6]

7. Subsequent to the filing of the CAIDP Complaint, many AI experts have called for regulation of ChatGPT.

8. Subsequent to the filing of the CAIDP Complaint, public support for the regulation of AI products such as ChatGPT has increased.

9. Subsequent to the filing of the CAIDP Complaint, the Senator Majority Leader has made bipartisan legislation on Artificial Intelligence a top legislative priority.

10. Subsequent to the filing of the CAIDP Complaint, FTC Commissioners and the FTC Chair has stated that the Commission has the authority to investigate and prosecute AI products.

---

[4] Sawadah Bhaimiya, *ChatGPT may be the fastest-growing consumer app in internet history, reaching 100 million users in just over 2 months, UBS report says*, Business Insider (Feb. 2, 2023), https://www.businessinsider.com/chatgpt-may-be-fastest-growing-app-in-history-ubs-study-2023-2?r=US&IR=T

[5] FTC, *Generative AI Raises Competition Concerns* (Jun. 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns

[6] Stephanie Borg Psaila, *Governments vs. ChatGPT: Investigations around the world,* Diplo, Blog Post, (Jun. 16, 2023), https://www.diplomacy.edu/blog/governments-chatgpt-investigations/

11. However, the US Federal Trade Commission has failed to even acknowledge the CAIDP Complaint of March 30, 2023 or to state whether it has opened an investigation.

12. The FTC's silence on the OpenAI raises substantial concerns about the agency's ability to safeguard the public as new challenges emerge.

13. CAIDP now files a Supplement to the original Complaint to (1) bring to the Commission's attention new developments since the filing of the original Complaint; (2) raise additional issues that were not fully discussed in the original Complaint; and (3) propose additional remedies that were not included in the original Complaint.

14. CAIDP urges the agency to open the investigation it should have pursued when CAIDP filed the original Complaint.

15. CAIDP incorporates by reference all points set out in the original Complaint.'

II. Consumer Agencies Around the World have Launched Investigations of GPT

A. The Investigation of GPT in Italy

16. In contrast to the FTC, the Italian privacy agency demonstrated an effective and efficient response to ChatGPT.

17. On March 31, 2023, one day after CAIDP filed the original Complaint with the Federal Trade Commission, the Italian Supervisory Authority the Garante banned ChatGPT and launched an investigation of OpenAI for breaches of EU data protection rules.[7]

[7] Luca Bertuzzi, *Italian data protection authority bans ChatGPT citing privacy violations* (Mar. 31, 2023), https://www.euractiv.com/section/artificial-intelligence/news/italian-data-protection-authority-bans-chatgpt-citing-privacy-violations/

18. The Garante ordered OpenAI to temporarily cease processing Italian Users' data amid a probe into a suspected breach of the GDPR following a data breach which exposed private chat histories and payment information of users.[8]

19. The Garante also opened investigations into OpenAI for failings check the age of ChatGPT users and the "absence of any legal basis that justifies the massive collection and storage of personal data" to train the chatbot."[9]

20. The Garante expressed concerns over "a lack of age restrictions on ChatGPT and how the chatbot can serve factually incorrect information in its responses." The Italian authorities have also said that "since there was no way to verify the age of users, ChatGPT "exposes minors to absolutely unsuitable answers compared to their degree of development and awareness."[10]

21. On April 12, 2023, less than two weeks after CAIDP filed the Complaint with the Commission, the Italian Supervisory Authority set out the circumstances under which OpenAI could resume ChatGPT in Italy.[11]

---

[8] Ryan Browne, *Italy became the first Western country to ban ChatGPT. Here's what other countries are doing,* CNBC (Apr. 4, 2023), https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html; Clothilde Goujard, *Italian privacy regulator bans ChatGPT, Calls have grown to suspend new releases of popular AI tool,* Politico (Mar. 31, 2023), https://www.politico.eu/article/italian-privacy-regulator-bans-chatgpt/

[9] Supanta Mukherjee, Elvira Pollina and Rachel More, *Italy's ChatGPT ban attracts EU privacy regulators,* Reuters (Apr. 3, 2023), https://www.reuters.com/technology/germany-principle-could-block-chat-gpt-if-needed-data-protection-chief-2023-04-03/

[10] BBC, *ChatGPT banned in Italy over privacy concerns* (Apr. 1, 2023), https://www.bbc.com/news/technology-65139406

[11] GPDP, ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola, (Apr. 12, 2023), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751; Elvira Pollina, *ChatGPT can resume in Italy if meets data watchdog's demands*, (Apr. 13, 2023), https://www.reuters.com/technology/italy-lift-curbs-chatgpt-if-openai-meets-demands-by-end-april-data-protection-2023-04-12/

22. The Garante set out several concrete measures. The Garante stated that OpenAI will need to provide certain information to the public:

> OpenAI will have to draft and make available, on its website, an information notice describing the arrangements and logic of the data processing required for the operation of ChatGPT along with the rights afforded to data subjects (users and non-users). The information notice will have to be easily accessible and placed in such a way as to be read before signing up to the service.
>
> Users from Italy will have to be presented with the notice before completing their registration, when they will also be required to declare they are aged above 18.
>
> Registered users will have to be presented with the notice at the time of accessing the service, once it is reactivated, when they will also be required to pass through an age gate filtering out underage users on the basis of the inputted age.

23. Regarding the legal basis for the processing of information, a requirement of the GDPR,[12] the Italian Supervisory Authority ordered OpenAI to "remove all references to contractual performance and to rely – in line with the accountability principle – on either consent or legitimate interest as the applicable legal basis. This will be without prejudice to the exercise the SA's investigatory and enforcement powers in this respect."[13]

24. Regarding data subject rights, a further requirement of the GDPR,[14] the Italian Supervisory Authority stated, "OpenAI will have to make available easily accessible tools to allow non-users to exercise their right to object to the processing of their personal data as relied upon for the operation of the algorithms. The same right will have to be afforded to users if legitimate interest is chosen as the legal basis for processing their data."[15]

---

[12] CAIDP, *FTC Complaint in the matter of Open AI, Inc*, para. 91.
[13] GPDP, ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola, (Apr. 12, 2023), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751
[14] CAIDP, *FTC Complaint in the matter of Open AI, Inc* paras. 91, 92
[15] GPDP, ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola, (Apr. 12, 2023), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751

25. Regarding the protection of children, the Italian Supervisory Authority ordered OpenAI to "immediately implement an age gating system for the purpose of signing up to the service and to submit, within the 31st of May, a plan for implementing, by 30 September 2023, an age verification system to filter out users aged below 13 as well as users aged 13 to 18 for whom no consent is available by the holders of parental authority."[16]

26. The enforcement action by the Italian Supervisory Authority of ChatGPT was concluded in less than two months from the initiation of the investigation of OpenAI.

27. The US Federal Trade Commission has thus far failed to state whether it has even opened an investigation of ChatGPT.

B. The Investigation of GPT in Canada

28. The ChatGPT investigation in Canada demonstrated that privacy concerns are not simply related to violations of the GDPR.

29. On April 4, 2023, the Office of the Office of the Privacy Commissioner (OPC) of Canada announced that it too had launched an investigation into ChatGPT.[17]

30. The Privacy Commissioner of Canada Philippe Dufresne stated, "AI technology and its effects on privacy is a priority for my Office. We need to keep up with – and stay ahead of – fast-moving technological advances, and that is one of my key focus areas as Commissioner."[18]

[16] Id
[17] Office of the Privacy Commissioner of Canada, OPC launches investigation into ChatGPT, (Apr. 4, 2023), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/
[18] Id.

31. According to the OPC, "The investigation into OpenAI, the operator of ChatGPT, was launched in response to a complaint alleging the collection, use and disclosure of personal information without consent."[19]

32. The OPC is now conducting a joint investigation with provincial privacy authorities into ChatGPT. The joint investigation will determine whether OpenAI:

- has obtained valid and meaningful consent for the collection, use and disclosure of the personal information of individuals based in Canada via ChatGPT;
- has respected its obligations with respect to openness and transparency, access, accuracy, and accountability; and
- has collected, used and/or disclosed personal information for purposes that a reasonable person would consider appropriate, reasonable or legitimate in the circumstances, and whether this collection is limited to information that is necessary for these purposes.[20]

[19] Id.
[20] Office of the Privacy Commissioner of Canada, *OPC to investigate ChatGPT jointly with provincial privacy authorities,* Announcement (May 25, 2023), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023

C. The Investigation of GPT in France

33. The ChatGPT investigation in France demonstrates that public agencies act in response to complaints received.

34. The CNIL, the French Data Protection Agency, has also launched an investigation of ChatGPT, following the filing of several consumer complaints.[21]

35. Zoe Vilain of Janus International, a campaign group, filed the first complaint. She wrote in her submission that when she tried to sign up for a ChatGPT account she was not asked for consent to any general terms of use of privacy policy. "We are not anti-tech, but we want ethical technology," she told AFP[22].

36. The second complaint came from David Libeau, a developer who wrote in his submission he had found personal information about himself when he asked ChatGPT about his profile. "When I asked for more information, the algorithm started to make up stories about me, creating websites or organising online events that were totally false," he wrote.

37. The third complaint was initiated by member of parliament Eric Bothorel under Article 5.1. (d) of the GDPR for the inaccuracy of information generated by ChatGPT about him.[23]

D. The Investigation of GPT in Australia

---

[21] Barrons, *AI Bot ChatGPT Faces Growing Scrutiny In Europe*, Agence France-Presse (Apr. 5, 2023), https://www.barrons.com/news/ai-bot-chatgpt-faces-growing-scrutiny-in-europe-89b322bd

[22] RFI, *AI bot ChatGPT faces growing scrutiny in Europe,* Agence France-Presse (Apr. 5, 2023), https://www.rfi.fr/en/business-and-tech/20230405-ai-bot-chatgpt-faces-growing-scrutiny-in-europe

[23] Tech & Co, *FAUSSES INFORMATIONS: LE DÉPUTÉ ERIC BOTHOREL DÉPOSE UNE PLAINTE CONTRE CHATGPT AUPRÈS DE LA CNIL,* (Apr. 12, 2023), https://www.bfmtv.com/tech/intelligence-artificielle/fausses-informations-le-depute-eric-bothorel-depose-une-plainte-contre-chat-gpt-aupres-de-la-cnil_AV

38. In Australia, OpenAI may face legal proceedings for defamation. "Brian Hood, who was elected mayor of Hepburn Shire, 120km (75 miles) northwest of Melbourne, last November, became concerned about his reputation when members of the public told him ChatGPT had falsely named him as a guilty party in a foreign bribery scandal involving a subsidiary of the Reserve Bank of Australia in the early 2000s."[24] The lawyer issuing the legal notice on behalf of Brian Hood, also mentioned that the ChatGPT tool was "very opaque"[25] referring to transparency and explainability concerns of the tool.

39. The information generated by ChatGPT regarding the Australian Mayor was false and inaccurate producing information that he served prison time for bribery concerning an entity of the Reserve Bank of Australia when he was actually the whistleblower. The Mayor, Brian Hood, "has not only never been in prison, but he was the whistleblower who flagged the bribery in the first place."[26]

E. The GPT Inquiry in Germany

40. The investigation of ChatGPT in Germany demonstrates that once investigations are initiated, new issues are likely to emerge. Indeed, that is a key characteristic of an investigation.

---

[24] Byron Kaye, *Australian mayor readies world's first defamation lawsuit over ChatGPT content,* Reuters (Apr. 5, 2023), https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/

[25] Id.

[26] Prarthana Prakash, *ChatGPT falsely accused a mayor of bribery when he was actually the whistleblower—now he wants to sue in what could be the first defamation case against a bot,* Fortune (Apr. 5, 2023), https://fortune.com/2023/04/05/chatgpt-falsely-accused-australian-mayor-bribery-openai-defamation/

41. Germany's data protection conference (DSK) the body of independent German data protection supervisory authorities of its federal and state governments, opened an inquiry into ChatGPT.[27]

42. "Regional data protection authorities in Europe's top economy have compiled a questionnaire for OpenAI and expect a response by 11 June… German authorities want to verify whether OpenAI under EU law sufficiently informs people whose data is used by ChatGPT that they "have rights, for example to access, correct or even delete their data".[28]

43. "Germany's federal commissioner for data protection and freedom of information, Ulrich Kelber, said the country could, in theory, also temporarily halt ChatGPT if it decides to probe whether the technology violates the European Union's General Data Protection Regulation (GDPR)."[29]

F. The Investigation of GPT in Spain

44. The investigation of ChatGPT in Spain reveals a primary concern with the protection of fundamental rights.

---

[27] Stephanie Borg Psaila, *Governments vs. ChatGPT: Investigations around the world,* Diplo, Blog Post (Jun. 16, 2023), https://www.diplomacy.edu/blog/governments-chatgpt-investigations/
[28] The Journal, *Germany launches data protection inquiry over ChatGPT,* (Apr. 24, 2023), https://www.thejournal.ie/germany-investigates-chatgpt-over-data-privacy
[29] Katyanna Quach, *Euro privacy regulators sniff Italy's ChatGPT ban, consider a pizza the action, Germany may follow, France and Ireland look for guidance from Rome,* The Register, (Apr. 4, 2023), https://www.theregister.com/2023/04/04/italy_chatgpt_ban_attracts_interest/ ; Supanta Mukherjee, Elvira Pollina and Rachel More, *Italy's ChatGPT ban attracts EU privacy regulators,* Reuters (Apr. 3, 2023), https://www.reuters.com/technology/germany-principle-could-block-chat-gpt-if-needed-data-protection-chief-2023-04-03/

45. Spain's Data Protection Agency the AEPD (Agencia Española de Protección de Datos), announced a preliminary investigation of Open AI over suspected violations of the GDPR.[30]

46. The Agency stated that, "[t]he AEPD initiated ex officio preliminary investigation proceedings against the U.S. company Open Ai, owner of the ChatGPT service, for possible non-compliance with the norms."[31]

47. The AEPD added that it proposed the development and implementation of innovative technologies, such as AI based on the respect to the enacted legislation (…) as a condition for technological development that is compatible with the rights and freedom of individuals.

G. The European Data Protection Board Task Force on ChatGPT

48. The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.[32] The EDPB is established by the General Data Protection Regulation (GDPR), and is based in Brussels.

49. Upon a request of Spain, the issue of ChatGPT was added to the EDPB agenda of the plenary session for discussion at request of Spain.

50. "The EDPB members discussed the recent enforcement action undertaken by the Italian Data Protection Authority against Open AI about the ChatGPT service"

---

[30] Natasha Lomas, *Spain's privacy watchdog says it's probing ChaGPT too, Techcrunc* (Apr. 13, 2023), https://techcrunch.com/2023/04/13/chatgpt-spain-gdpr/

[31] AEPD, *La AEPD inicia de oficio actuaciones de investigacion a OpenAI, propietaria de ChatGPT* (Apr.13, 2023), https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-inicia-de-oficio-actuaciones-de-investigacion-a-openai

[32] EDPB, *Who We Are*, https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_en

51. The EDPB announced the launch of a dedicated task force to "foster cooperation and to exchange information on possible enforcement actions conducted by data protection authorities"[33]

H. The Swiss Statement on ChatGPT

52. On April 4, 2023, the Switzerland data protection regulator, Federal Data Protection and Information Commissioner (FDPIC) issued a statement on the use of ChatGPT and AI applications. [34]

53. FDPIC warned that that organizations must ensure that data protection requirements are complied with when using AI-supported apps. This includes, the FDPIC noted, ensuring users are informed in a transparent and understandable manner about which data is processed, for which purpose, and in what way.[35]

I. Review of AI Models in the United Kingdom

54. On May 4, 2023, The Competition and Markets Authority (CMA) of the United Kingdom announced that it was opening an initial review of competition and consumer protection considerations in the development and use of large language models, such as GPT.[36]

55. The CMA stated that:

> foundation models, which include large language models and generative artificial intelligence (AI), that have emerged over the past five years, have

[33] EDPB, E*DPB resolves dispute on transfers by Meta and creates task force on Chat GPT* (Apr. 13, 2023), https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en ; Isabelle Roccia, *A view from Brussels: EDPB hammers at transborder data flow, ChatGPT,* IAPP (Apr. 13, 2023), https://iapp.org/news/a/a-view-from-brussels-edpb-hammers-at-transborder-data-flow-chatgpt/

[34] *Switzerland: FDPIC issues statement on ChatGPT and AI-supported apps (*Apr. 4, 2023), https://www.dataguidance.com/news/switzerland-fdpic-issues-statement-chatgpt-and-ai

[35] Id.

[36] UK Government, Competition and Markets Authority, CMA launches initial review of artificial intelligence models (May 4, 2023), https://www.gov.uk/government/news/cma-launches-initial-review-of-artificial-intelligence-models

> the potential to transform much of what people and businesses do. To ensure that innovation in AI continues in a way that benefits consumers, businesses, and the UK economy, the government has asked regulators, including the Competition and Markets Authority (CMA), to think about how the innovative development and deployment of AI can be supported against five overarching principles: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

56. The CMA added that its initial review is in line with the government's AI white paper and the CMA's role to support open, competitive markets. The review will examine how the competitive markets for foundation models and their use could evolve, explore what opportunities and risk these scenarios could bring for competition and consumer protection, and produce guiding principles to support competition and protect consumers as AI foundation models develop.

57. The Chief Executive of the CMA, Sarah Cardell, said "It's crucial that the potential benefits of this transformative technology are readily accessible to UK businesses and consumers while people remain protected from issues like false or misleading information. Our goal is to help this new, rapidly scaling technology develop in ways that ensure open, competitive markets and effective consumer protection."[37]

J. Japan's Privacy Guidance to OpenAI

58. On June 1, 2023 Japan's privacy agency the Personal Information Protection Commission issued guidance regarding the protection of personal information by generative AI companies. The guidance was issued to OpenAI pursuant to Article 147 of the Personal Information Protection Law (2003) of Japan.[38]

---

[37] Id.

[38] Policy Research Institute, *The first administrative guidance to generative AI platform and Alerts regarding the use of generative AI services issued by the PPC* (Jun. 8, 2023),

59. The warning addresses two primary concerns. First, the PPC requires that Open AI take necessary steps to ensure that it does not collect sensitive personal information for machine learning purposes without the consent of the affected individual. If such information is collected, Open AI must delete it as soon as possible, and at least before processing it into datasets for training purposes.[39]

60. Additionally, the guidance requires that the purpose of using personal information must be within purpose notified to the affected individual or made public.

61. This is a sampling of the investigations of OpenAI that have been launched by consumer protection agencies around the world since CAIDP filed the original Complaint with the FTC.

III. Additional Developments that Favor the Launch of the OpenAI investigation by the Federal Trade Commission

A. President Biden's Views on Consumer Protection and AI Products

62. President Biden has made clear that companies should not release products that are not safe.

63. The President's Council of Advisors on Science and Technology (PCAST) "consists of distinguished individuals from sectors outside of the Federal Government who advise the President on policy matters where the understanding of science, technology, and innovation is key."[40]

64. In opening remarks to the PCAST at a meeting in April, shortly after the filing of the CAIDP Complaint concerning OpenAI, President Biden emphasized the importance of "ensuring responsible innovation and appropriate guardrails to protect America's rights and

[39] Id.
[40] The White House, PCAST, https://www.whitehouse.gov/pcast/

safety, and protecting their privacy, and to address the bias and disinformation that is possible as well."[41]

65. The President spoke directly to the issue set forth in this complaint – the need to ensure that AI products are safe before they are released to the public. President Biden said:

> I look forward to today's discussion about ensuring responsible innovation and appropriate guardrails to protect America's rights and safety, and protecting their privacy, and to address the bias and disinformation that is possible as well.
>
> And so, *tech companies have a responsibility, in my view, to make sure their products are safe before making them public*.[42]

66. President Biden restated this view when Vice President Harris and senior Administration officials met with CEOs of four American companies at the forefront of AI innovation. According to the Readout of the White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation:

> President Biden dropped by the meeting to underscore that companies have a fundamental responsibility to make sure their products are safe and secure before they are deployed or made public.[43]

B. Cybercrime and Cybersecurity

67. In the original Complaint, CAIDP cited a wide range of sources on the risk that deployment of GPT would pose to cybersecurity.[44]

---

[41] The White House, *Remarks by President Biden in Meeting with the President's Council of Advisors on Science and Technology* (Apr. 4, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/04/remarks-by-president-biden-in-meeting-with-the-presidents-council-of-advisors-on-science-and-technology/

[42] Id. (emphasis added)

[43] The White House, *Readout of White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation* (May 4, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/readout-of-white-house-meeting-with-ceos-on-advancing-responsible-artificial-intelligence-innovation/

[44] CAIDP, *FTC Complaint, in the matter of Open AI, Inc.*, pars. 60-70

68. Since the filing of the CAIDP Complaint, new concerns about generative AI and cybersecurity have emerged.

69. Legal experts at the American Bar Association have noted that "cybercriminals and other bad actors now have a tool at their fingertips to make scam-ready content with a sheen of legitimacy."[45]

70. "From a hacker's perspective," wrote one business executive, "ChatGPT is a game changer, affording hackers from all over the globe a near fluency in English to bolster their phishing campaigns. Bad actors may also be able to trick the AI into generating hacking code."[46] ChatGPT increases the risk of cyber-crimes targeted at vulnerable groups like senior citizens who would not have the capability to detect phishing emails generated by tell-tale signs of poor grammar or misspellings

71. Even where possible beneficial use-cases of ChatGPT are assessed, cybersecurity experts state that the "risk of inaccurate results is too great to deploy it broadly."[47] Furthermore experts have also stated "the potential for inaccuracies from generative AI brings risk for companies hoping to use it for important decisions without human supervision.

72. Jen Easterly, Director of the Cybersecurity and Infrastructure Agency (CISA), speaking on the significant cybersecurity risks and cyberthreats posed by the release of generative AI products, "called for "smart regulation" of AI technology and products, warning

---

[45] Matt Reynolds, *What cybersecurity threats do generative chatbots like ChatGPT pose to lawyers?* ABA Journal (Jun. 21, 2023), https://www.abajournal.com/web/article/what-cybersecurity-threats-do-generative-ai-chatbots-like-chatgpt-pose-to-lawyers

[46] Jim Chilton, *The New Risks ChatGPT Poses to Cybersecurity,* Harvard Business Review (Apr. 21, 2023), https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity

[47] Catherin Stupp, *Mattel Experiments with ChatGPT in Cybersecurity,* The Wall Street Journal (Jun. 8, 2023), https://www.wsj.com/articles/mattel-experiments-with-chatgpt-in-cybersecurity-c80a0965

that tech companies, as with other technologies, are too focused on getting AI products to market quickly and not paying enough attention to safety."[48]

73. Top national security have also warned of the use of AI use to intensify cyberattacks. CISA Director, Jen Easterly stated that "she is "the most pessimistic I've ever been" about the use of AI by hackers to weaponize current cyber capabilities, particularly given the lack of AI regulations."[49]

74. President and CEO of CrowdStrike George Kurtz said that ChatGPT may give hackers the ability to create zero day vulnerabilities — "the worst type of vulnerability that can be used widely against devices to gain access or steal information."[50]

75. National Security and Cybersecurity experts warn of the severe risks of ChatGPT "amid wider concerns about the use of AI and as countries like China and India move to halt the use of AI programs like OpenAI's ChatGPT amid security concerns"[51]

76. Peter Morgan, the co-founder and CSO of Phylum, a cybersecurity firm that focuses on the supply chain said of the ChatGPT plugins, "Plugins are simply code developed by external developers, and must be carefully reviewed before inclusion into systems like the GPTs. There is a significant risk of malicious developers building plugins for the GPTs that undermine the security posture, or weaken the capabilities of the system to respond to user questions."[52]

---

[48] Jeff Seldin, *Key US Official Calls for Tech Companies to 'Do Something' About AI,* Voice of America (VOA) News (May 31, 2023), https://www.voanews.com/a/key-us-official-calls-for-tech-companies-to-do-something-about-ai/7117174.html

[49] Maggie Miller, *Officials warn of AI use to intensify cyberattacks,* PoliticoPro (Apr. 11, 2023), https://www.politicopro.com/premium-news/access/

[50] Id.

[51] Id.

[52] eSecurity planet, *ChatGPT Security and Privacy Issues Remain in GPT-4* (Apr. 27, 2023), https://www.esecurityplanet.com/threats/gpt4-security/

77. Emily Bender, a linguistics professor at the University of Washington said that "ChatGPT's own plugin red team members found they could 'send fraudulent or spam emails, bypass safety restrictions, or misuse information sent to the plugin.'"[53]

78. The Allen Institute of Artificial Intelligence found that ChatGPT can be consistently toxic and harmful. They also found that ChatGPT's toxicity can increase up significantly when assigned a persona and this "presents a vulnerability that increases the likelihood of a user encountering harmful content."[54]

79. In a study commissioned by ELSA – European Lighthouse on Secure and Safe AI, computer security experts studying LLM-Integrated Applications and downstream uses concluded that these integrations "blur the line between data and instructions" due to security flaws of "indirect prompt injections" and render LLMs like ChatGPT vulnerable to "data theft, worming, information ecosystem contamination, and other novel security risks."[55] They urged ongoing security evaluations of LLM-integrated applications due to the ongoing current security risks of these applications.

80. Jen Easterly, CISA Director called for stronger guardrails around new AI technologies such as ChatGPT stating that "In some cases, regulation can even spur

---

[53] WIRED, *Now That ChatGPT Is Plugged In, Things Could Get Weird* (Mar. 28, 2023), https://www.wired.com/story/chatgpt-plugins-openai/

[54] Ameet Deshpande, Vishvak Murahari, Tanmay Rajpurohit, Ashwin Kalyan and Karthik Narashiman, *Toxicity in ChatGPT – Analyzing Persona-Assigned Language Models* (Apr. 11, 2023), DOI:10.48550/arXiv.2304.05335, https://www.semanticscholar.org/paper/Toxicity-in-ChatGPT%3A-Analyzing-Persona-assigned-Deshpande-Murahari/; *See also,* Ameet Deshpande, Vishvak Murahari, Tanmay Rajpurohit, Ashwin Kalyan and Karthik Narashiman, *Toxicity in ChatGPT – Analyzing Persona-Assigned Language Models,* Medium, Blog Post (Apr. 12, 2023), https://blog.allenai.org/toxicity-in-chatgpt-ccdcf9265ae4

[55] Kai Greshake, Sahar Abdelnabi, Shailesh Mishra, Christoph Endres, Thorsten Holz, Mario Fritz, *Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection* (May 5, 2023), https://arxiv.org/pdf/2302.12173.pdf

innovation"[56] Furthermore, "Countering disinformation is about to get much harder: In the near term, ChatGPT and similar chatbots powered by large language models, or LLMs, will let threat actors master a range of malicious activities, including manufacturing more believable lies at scale.

81. National Security Agency (NSA) Director of Cybersecurity Rob Joyce has said, ChatGPT will enable malicious foreign actors to craft very convincing, native-language, English text for phishing schemes, false backstories, and even malign influence operations."[57]

82. The US Department of Defense's Chief Digital and AI Officer, Craig Martell stated he is "scared to death" of the potential for generative artificial intelligence systems like ChatGPT to deceive citizens and threaten national security."[58] He further stated, "My fear is that we trust it too much without the providers of [a service] building into it the right safeguards and the ability for us to validate the information."[59]

C. Privacy and Data Breaches

83. In the original complaint, CAIDP called attention to a significant data breach concerning the use of GPT-4 by employees at Amazon.[60]

---

[56] John Sakellariadis, *Easterly plays China Card to promote AI regulation,* Politico Pro, News, (May 5, 2023), https://subscriber.politicopro.com/article/2023/05/easterly-plays-china-card-to-promote-ai-regulation-00095592

[57] Jason Robertson, *Countering Disinformation In A Post-ChatGPT World,* Booz| Allen| Hamilton, Perspectives, https://www.boozallen.com/insights/cyber/tech/how-to-counter-disinformation-in-a-post-chatgpt-world.html

[58] Jack Aldane, *Agencies 'don't have the tools ' to head off ChatGPT threat to national security, warns Pentagon's AI Chief,* Global Government Forum (May 11, 2023), https://www.globalgovernmentforum.com/agencies-dont-have-the-tools-to-head-off-chatgpt-threat-to-national-security-warns-pentagons-ai-chief/

[59] Id.

[60] CAIDP, *FTC Complaint, in the matter of Open AI, Inc.*, para. 65

84. More data breaches are now being reported. Like the Amazon "breach," these are not breaches involving the third-party theft of personal data collected by the service providers. Rather these incidents relate to the product design of the machine learning model for GPT-4.

85. ChatGPT exposes users to risk of loss of data and privacy violations through "Conversational AI leaks."[61] The incidents of data breaches arising from the use of ChatGPT are the result of the product design of the machine learning model for GPT-4.

86. OpenAI itself has disclosed that users' payment information may have been leaked during a ChatGPT outage. According to OpenAI "about 1.2% of ChatGPT Plus users may have had their payment data leaked to other ChatGPT users – which could be significant, as recent stats show Plus hosts roughly one million subscribers."[62] (*emphasis added*)

87. Samsung banned the use of ChatGPT and similar Generative AI tools following a leak of sensitive internal source code by an engineer who uploaded it to ChatGPT.[63] Samsung issued a company-wide memo banning the use of "generative AI" tools including ChatGPT.[64]

---

[61] Vilius Petkauskas, *Lessons learned from ChatGPT's Samsung Leak,* Cybernews (May 9, 2023), https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/

[62] Stefanie Schappert, *ChatGPT leaks user credit card details,* Cybernews (Jun. 2, 2023), https://cybernews.com/news/payment-info-leaked-openai-chatgpt-outage/; *See also,* Abraham Jewett, *ChatGPT allegedly suffers outage, data breach,* Top Class Actions (Apr. 4, 2023), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/chatgpt-allegedly-suffers-outage-data-breach/; Sue Poremba, *ChatGPT Confirms Data Breach, Raising Security Concerns,* Security Intelligence (May 2, 2023), https://securityintelligence.com/articles/chatgpt-confirms-data-breach/

[63] Siladitya Ray, *Samsung bans ChatGPT Among Employees After Sensitive Code Leak,* Forbes (May 2, 2023), https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/?sh=6f59bcb96078

[64] Mark Gurman, *Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak,* Bloomberg News (May 1, 2023), https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak#xj4y7vzkg

88. By default, ChatGPT saves a user's chat history and uses the conversations to train its models further, and while the platform allows users to disable this manually, it is unclear if this option retroactively applies to older chats.[65]

89. Bank of America, Goldman Sachs, Wells Fargo, Citigroup and Deutsche Bank have also imposed restrictions on the use of ChatGPT and other generative AI tools.[66]

90. Wells Fargo has stated "We are imposing usage limits on ChatGPT, as we continue to evaluate safe and effective ways of using technologies like these."[67] JP Morgan Chase also heavily restricted the use of ChatGPT by its staffers amid concerns that it may face potential regulatory risks surrounding the sharing of sensitive financial information.[68]

91. Apple has also banned internal use of ChatGPT[69] due to OpenAI storing users' data to train the Company's AI systems.[70]

---

[65] Siladitya Ray, *Samsung bans ChatGPT Among Employees After Sensitive Code Leak,* Forbes (May 2, 2023), https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

[66] Gabriela Mello, William Shaw and Hannah Levitt, *Wall Street Banks Are Cracking Down on AI-Powered ChatGPT*, Bloomberg News (Feb. 24, 2023), https://www.bloomberg.com/news/articles/2023-02-24/citigroup-goldman-sachs-join-chatgpt-crackdown-fn-reports?sref=CSMHWBLp#xj4y7vzkg

[67] Id.

[68] Siladitya Ray, *Samsung bans ChatGPT Among Employees After Sensitive Code Leak,* Forbes (May 2, 2023), https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

[69] Aaron Tilley and Miles Kruppa, *Apple Restricts Employee Use of ChatGPT, Joining Other Companies Wary of Leaks,* Wall Street Journal (May 18, 2023), https://www.wsj.com/articles/apple-restricts-use-of-chatgpt-joining-other-companies-wary-of-leaks-d44d7d34

[70] James Vincent, *Apple restricts employees from using ChatGPT over fear of data leaks,* The Verge (May 19, 2023), https://www.theverge.com/2023/5/19/23729619/apple-bans-chatgpt-openai-fears-data-leak

92. In response to growing scrutiny of its privacy practices by European privacy authorities, OpenAI now allows users to turn off the chat history option on ChatGPT. But even with this setting enabled, OpenAI still retains conversations for 30 days with the option to review them "for abuse" before deleting them permanently.[71]

93. Google's parent company Alphabet.inc also issued a warning to engineers from using ChatGPT, it's own AI chatbot -Bard and similar generative AI tools to produce code on grounds of data leak risks.[72]

D. Risks in Education

94. There is growing concern among the research and educational community that ChatGPT will increase plagiarism and theft of copyrighted or original ideas from research communities.[73]

95. The policies established by StackOverflow highlight that ChatGPT answers are "substantially harmful to the site and to users who are asking and looking for correct answers"[74] and discourages users from posting such answers for community learning purposes.

---

[71] Benj Edwards, *ChatGPT now disabling chat history, declining training, and exporting data,* Ars Technica, (Apr. 25, 2023), https://arstechnica.com/information-technology/2023/04/chatgpt-users-can-now-opt-out-of-chat-history-and-model-training/

[72] Ana Faguy, *Google Warns Employees about chatbots- Including Its Own Bard—Out Of Privacy Concerns, Report Says,* Forbes (Jun. 15, 2023), https://www.forbes.com/sites/anafaguy/2023/06/15/google-warns-employees-about-chatbots-including-its-own-bard-out-of-privacy-concerns-report-says/

[73] Eva A.M. Van Dis, Johan Bollen, Willem Zuidema, Robert Van Rooij, & Claudi L. Bockting, *ChatGPT: Five Priorities for Research,* Nature, (Feb. 3, 2023), https://www.nature.com/articles/d41586-023-00288-7

[74] Stack Overflow, *Why Posting GTP and ChatGPT generated answers is not currently acceptable* (Feb. 2023), https://stackoverflow.com/help/gpt-policy

96. Open AI itself acknowledged that harmful and untruthful outputs, including toxic content are still present in the outputs of the model, despite their use of "reinforcement learning from human feedback (RLHF)."[75]

97. The UNESCO Report[76] on ChatGPT and Artificial Intelligence in Higher Education highlights seven areas of concern on ChatGPT in education including challenges to academic integrity, privacy concerns, and cognitive bias. The UNESCO report states:

> The extremely rapid development of ChatGPT has caused apprehension for many, leading a group of over 1,000 academics and private sector leaders to publish an open letter calling for a pause on the development of training powerful AI systems. This cessation would allow time for potential risks to be investigated and better understood and for shared protocols to be developed.[77]

E. Misrepresentation and Deception of Users

98. ChatGPT is now integrated with Microsoft's Bing search service and includes advertising.[78] Microsoft states "We are also exploring additional capabilities for publishers including our more than 7,500 Microsoft Start partner brands. We recently met with some of our partners to begin exploring ideas and to get feedback on how we can continue to distribute content in a way that is meaningful in traffic and revenue for our partners."[79]

---

[75] OpenAI, *Methods,* https://openai.com/blog/chatgpt/

[76] UNESCO, *ChatGPT and Artificial Intelligence in higher education: Quick Start Guide,* 2023, https://www.iesalc.unesco.org/wp-content/uploads/2023/04/ChatGPT-and-Artificial-Intelligence-in-higher-education-Quick-Start-guide_EN_FINAL.pdf

[77] Id at 11.

[78] Devin Coldewey, *That was fast! Microsoft slips ads into AI-powered Bing Chat,* TechCrunch (Mar. 29, 2023), https://techcrunch.com/2023/03/29/that-was-fast-microsoft-slips-ads-into-ai-powered-bing-chat/

[79] Yusuf Mehdi, *Driving more traffic and value to publishers from the new Bing,* Microsoft Bing Blogs, (Mar. 29, 2023), https://blogs.bing.com/search/march_2023/Driving-more-traffic-and-value-to-publishers-from-the-new-Bing

99. In an illustrative Tweet by a user regarding the response generated by Bing Chat to the prompt/search for the 'cheapest Honda car', the response with advertisements was clearly confusing. In relation to this Tweet and the specific advertisement placed to the User, analysts stated that it was unclear to the user what was sponsored in the response and if the user can ask for non-sponsored results.[80]

100. The Federal Trade Commission has routinely investigated and prosecuted unfair and deceptive advertising practices. In the business guidance issued on May 1, 2023 the FTC pointed towards this category of deceptive practice cautioning AI firms that:

> *[I]t should always be clear that an ad is an ad, and search results or any generative AI output should distinguish clearly between what is organic and what is paid. People should know if an AI product's response is steering them to a particular website, service provider, or product because of a commercial relationship. And, certainly, people should know if they're communicating with a real person or a machine.*[81]

101. ChatGPT plugins are currently being deployed in a numerous consumer facing applications including restaurant reservations, ordering groceries, booking trips, language tutoring, family and home management solutions, and online shopping.[82] None of these uses have any disclaimers as to possible security or privacy risks and Users are not aware that they are interacting with an AI agent while using these applications.

102. A report published in the MIT Technology Review stated:

> Tech companies are racing to embed these models into tons of products to help people do everything from book trips to organize their calendars to take notes in meetings. But the way these products work—receiving

[80] Devin Coldewey, *That was fast! Microsoft slips ads into AI-powered Bing Chat,* TechCrunch, (Mar. 29, 2023), https://techcrunch.com/2023/03/29/that-was-fast-microsoft-slips-ads-into-ai-powered-bing-chat/

[81] Michael Atleson, *The Luring Test: AI and the engineering of consumer trust,* FTC, Business Blog (May 1, 2023) (emphasis in original), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust

[82] OpenAI, *ChatGPT Plugins, https://openai.com/blog/chatgpt-plugins*

> instructions from users and then scouring the internet for answers—creates a ton of new risks. With AI, they could be used for all sorts of malicious tasks, including leaking people's private information and helping criminals phish, spam, and scam people. Experts warn we are heading toward a security and privacy disaster.[83]

103. While OpenAI represents that it is CCPA, GDPR, SOC 2, SOC 3 compliant in its Trust Portal, users are unable to view the substantiation of these compliance certifications or data privacy measures or details of any other 'trust measure' without first signing up and providing personal data.[84] This is a manipulative and deceptive representation of privacy and security assurances to Users.

104. OpenAI collects 'user data' to train ChatGPT by default unless Users 'opt-out' of the 'training' by disabling 'chat histories' in the user interface. This also disables the 'chat history' feature and users lose all their previous prompts. The usage conditions and product design of ChatGPT are inherently deceptive as to user data and FTC has stated that such interface designs and buried in conditions tricking or forcing users to give up their data or privacy are digital dark patterns.[85]

105. In April 2023, ChatGPT was integrated with Snapchat – used by many children. There is no opt-out from the chatbot in the standard, free version of the app. The information

[83] Melissa Heikkilä, *Three ways AI chatbots are a security disaster,* MIT Technology Review (Apr. 3, 2023), https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/

[84] OpenAI, *Security Portal,* https://trust.openai.com

[85] FTC, *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers - Tactics Include Disguised Ads, Difficult-to-Cancel Subscriptions, Buried Terms, and Tricks to Obtain Data,* Press Release (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers

page on Snapchat states "My AI "may include biased, incorrect, harmful or misleading content" and suggests that users should independently verify any advice it gives before acting on it."[86]

106. Integration of ChatGPT with applications widely used by children will enable further collection of children's personal data as kids may not be aware of the nature of the information they are disclosing to the chatbot.

107. ChatGPT has demonstrated negative effects of providing misinformation,[87] incorrect advice, creation of bullying content.[88] The inclusion of a conversational feature in social media apps used predominantly by children is likely to result in higher amounts of data scraped from children, increased screen-time[89] and endanger online child safety.

108. The Federal Trade Commission has routinely investigated business practices that impact childrens' safety and privacy.

F. European Consumer Organization (BEUC) Complaint about ChatGPT

109. On April 21, 2023 the European Consumer Organization (BEUC) petitioned the Consumer Protection Cooperation Network of the European Commission to open inquiries into

[86] Bernard Marr, *Snapchat Debuts ChatGPT – Powered Snap AI: But is it safe for kids?*, Forbes (Apr. 26, 2023), https://www.forbes.com/sites/bernardmarr/2023/04/26/snapchat-debuts-chatgpt-powered-snap-ai--but-is-it-safe-for-kids

[87] Open AI, *The GPT-4 System Card* (Mar.15 2023)**.** https://cdn.openai.com/papers/gpt-4-system-card.pdf

[88] Senator Michael Bennett*, Bennett Calls on Tech Companies to Protect Kids as They Deploy AI Chatbots: Following Early Reports of Potentially Harmful Content from AI Chatbots, Bennet Urges Tech CEOs to Prioritize Young Americans' Safety* (Mar. 21, 2023), https://www.bennet.senate.gov/public/index.cfm/2023/3/bennet-calls-on- tech-companies-to-protect-kids-as-they-deploy-ai-chatbots; The Lancet, *ChatGPT: Friend or Foe,* Editorial(Feb. 6, 2023), https://www.thelancet.com/action/showPdf

[89] Gaia Bernstein, *ChatGPT Is the Wake-Up Call Schools Need to Limit Tech in Classrooms,* Time (Mar. 28, 2023), https://time.com/6266311/chatgpt-tech-schools/

ChatGPT and similar AI-text generators.[90] Among the key concerns presented by the BEUC were:

a) Deceptive commercial statements and advertising in consumer-facing services and applications for example the use of a language model for giving investment or debt management advice, wrong purchasing advice on e-commerce platforms,

b) Misleading practices due to omission of information and lack of information. The OpenAI website offers substantial amounts of marketing claims, praising the 'reasoning' capabilities of the GPT model. However, given the present risks, for example, producing advice on terrorist attacks or hate speech, the website is misleading by not providing an accurate description of the main characteristics of the product in a clear and comprehensible manner, and

c) Exacerbate risks to vulnerable users/consumers like children and teenagers, including deceptive advertising, aggressive commercial practices, and manipulation.

[90] BEUC, The European Consumer Organization, *Call for action to open an inquiry on generative AI systems to address risks and harms for consumers,* submitted to DG JUST, European Commission CPC Network (Apr. 21, 2023), https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-045_Call_for_action_CPC_authorities_Generative_AI_systems.pdf

G. Norwegian Consumer Council (BEUC) Report about ChatGPT

110. In June 2023, the Norwegian Consumer Council (NCC) published *Ghost in the Machine,* a report addressing the consumer harms of generative AI.[91] The NCC report presents several critical findings:

a) "Generative AI models are dependent on large amounts of data that is taken from a multitude of sources, usually without the knowledge or consent of the originator of the data, be it a piece of art, a news article, or a selfie. Information is siphoned and gathered to be used in different ways, with an end goal of enriching a small number of companies. This raises questions of value distribution, usage permission, privacy, account- ability, intellectual property, and human rights.[92]

b) The question of who controls the development and training of generative AI models and how they are used is of fundamental importance. Those who control the technology have significant potential to create de-pendencies, set the terms of use, and decide who has access. This entrenchment of power creates overarching concerns about leading tech companies becoming gatekeepers that can exclude rivals and otherwise abuse their increasingly dominant market positions.[93]

c) The promise of generative AI models has also reached the advertising industry. The technology is already being used to generate ad copy, creating synthetic stock photos and models, and as part of marketing stunts. These use cases may reduce labour in the advertising sector but can also have adverse effects on consumers, particularly by

[91] Norwegian Consumer Council, *Ghost in the machine – Addressing the consumer harms of generative AI* (Jun. 2023), https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf

[92] Id at 15.

[93] Id at 17.

making it easier and more efficient to manipulate people through creating personalized and/or conversational advertising.[94]

d) There are rising concerns about generative AI in chat- bots and their ability to trick consumers into sharing personal data, which may be repurposed to serve targeted advertising or to manipulate consumers into purchasing products or services. This is especially relevant in the case of vulnerable groups such as children or lonely people, who may be more likely to share sensitive information about themselves in conversation with the generative AI.[95]

e) Image generators are usually trained on huge datasets that include images of real people. These images can, for example, be taken from social media and search engines, without a lawful legal basis or knowledge by the people in the pictures. Similarly, text generators are trained data-imasets that could include personal data about individuals, or conversations between individuals."[96]

H. Public Opinion Favors Regulation of ChatGPT

111. Recent polling data conducted by the Pew Research Center indicates that the American public can readily distinguish between AI applications that may be beneficial and AI applications that may be harmful.[97]

[94] Id at 28.
[95] Id at 28.
[96] Id at 30.
[97] Brian Kennedy, Alec Tyson and Emily Saks, *Public Awareness of Artificial Intelligence in Everyday Activities,* Pew Research Center (Feb. 15, 2023), https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

112. According to Pew Research Center, Americans are generally not impressed by Chatbots to support mental health or for writing news articles. Americans are rather impressed by the use of AI to predict extreme weather, advance medical science, and improve crop production.[98]

113. Solid evidence drawn from public opinion indicates that "the public remains cautious about the impact of artificial intelligence is having on American life."[99]

114. As a general matter, Americans are more concerned about AI than excited. According to a March 2022 Pew poll, 37% of Americans are "more concerned than excited," 18% are more excited than concerned, and 45% are equally concerned and excited.[100]

115. This finding continued in a February 2023 poll. Pew found that 38% of Americans are more concerned about AI than excited, 15% are more excited than concerned, and 46% are equally concerned and excited.[101]

116. A poll conducted by YouGovAmerica, asked 20,810 adults "Would you support or oppose a six-month pause on some kinds of AI development?" 41% answered that they would

[98] Marc Rotenberg, *Recent Polling data from Pew Research Center,* (Apr. 7, 2023), https://www.linkedin.com/posts/marc-rotenberg_ai-data-tech-activity-7048101703635644416-Vgne

[99] Id.

[100] Lee Rainie, Cary Funk, Monica Anderson, Alec Tyson, *How Americans think about artificial intelligence,* Pew research Center (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/how-americans-think-about-artificial-intelligence/

[101] Brian Kennedy, Alec Tyson, and Emily Saks, *Public Awareness of Artificial Intelligence in Everyday Activities: Limited enthusiasm in U.S. over AI's growing influence in daily life,* Pew Research Center (Feb. 15, 2023), https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

"strongly support" the pause, 28% somewhat support the Pause, 9% somewhat oppose, 4% strongly oppose, and 18% were not sure.[102]

117. There appeared to be little disparity in the YouGovAmerica poll results by region, gender, politics, age, or race.

I. Safety Concerns

118. Roy Friedmann, senior director analyst in the Gartner Legal & Compliance Practice has noted that "ChatGPT is also prone to 'hallucinations,' including fabricated answers that are wrong, and nonexistent legal or scientific citations."[103]

119. Oded Vanunu, head of products vulnerability research at Check Point Software, has said "ChatGPT-4 can empower bad actors, even non-technical ones, with the tools to speed up and validate their activity."[104]

120. Anjana Susarla, Professor of Information Systems, Michigan State University, has written that "Experts on AI fairness contend that issues of bias and fairness in AI cannot be addressed by technical methods alone but require more comprehensive risk mitigation practices such as adoption institutional review board for AI."[105]

---

[102] YouGovAmnerica, More than 1,000 technology leaders recently signed an open letter calling on researchers to pause development of certain large-scale AI systems for at least six months world-wide, citing fears of the "profound risks to society and humanity." Would you support or oppose a six-month pause on some kinds of AI development? (Apr. 3, 2023), https://today.yougov.com/topics/technology/survey-results/daily/2023/04/03/ad825/2

[103] Gartner, *Gartner Identifies Six ChatGPT Risks Legal and Compliance Leaders Must Evaluate* (May 18, 2023), https://www.gartner.com/en/newsroom/press-releases/2023-05-18-gartner-identifies-six-chatgpt-risks-legal-and-compliance-must-evaluate

[104] Verdict, *GPT-4 Risks Accelerating Cybercrime, Expert Warns* (Mar. 17, 2023), https://www.verdict.co.uk/gpt-4-risks-accelerating-cybercrime-expert-warns/

[105] The Conversation, *How can Congress regulate AI? Erect guardrails, ensure accountability, and address monopolistic power* (May 30, 2023), https://theconversation.com/how-can-congress-regulate-ai-erect-guardrails-ensure-accountability-and-address-monopolistic-power-205900

121. Sam Altman, CEO of OpenAI, himself has voiced concerns with the systems that OpenAI is creating. In a blog post, he writes that, "The systems we are concerned about will have power beyond any technology yet created, and we should be careful not to water down the focus on them by applying similar standards to technology far below this bar."[106]

122. Christiano Giardina, an AI researcher, has found multiple instances of "prompt injection," manipulating LLMs to become unconstrained. He notes, "the danger for this would come from large documents where you can hide a prompt injection where it's much harder to spot."[107]

123. Researchers have also "proved that for any behavior that an A.I. model could exhibit, no matter how unlikely, there exists a prompt that will elicit that behavior, with less likely behaviors simply requiring longer prompts."[108]

124. Ali Alkhatib, acting director of the Center for Applied Data Ethics at the University of San Francisco has voiced concerns that "Things are moving fast enough to be not just dangerous, but actually harmful to a lot of people."[109]

125. The World Health Organization has said that "The data used to train AI may be biased, generating misleading or inaccurate information that could pose risks to health, equity and inclusiveness.

---

[106] OpenAI, *Governance of Superintelligence* (May 22, 2023), https://openai.com/blog/governance-of-superintelligence#SamAltman
[107] WIRED, *The Security Hole at the Heart of ChatGPT and Bing* (May 25, 2023), https://www.wired.com/story/chatgpt-prompt-injection-attack-security/
[108] Fortune, *Why OpenAI's latest breakthrough to make ChatGPT safer is actually a step away from the AI we want* (Jun. 6, 2023), https://www.fortune.com/2023/06/06/openai-chatgpt-llm-training-rlhf-process-supervision-alphago-move37-eye-on-a-i/
[109] WIRED, *Now That ChatGPT Is Plugged In, Things Could Get Weird* (Mar. 28, 2023), https://www.wired.com/story/chatgpt-plugins-openai/

J. AI Now Institute Report on General Purpose AI

126. A recent paper on General Purpose AI (GPAI), prepared by the AI Now Institute for consideration in the context of the current negotiation of the EU AI Act, also identifies several issues of relevance to the FTC consideration of the CAIDP complaint.[110]

127. The AI Now Expert paper notes that GPAI is an ”expansive category” and should include “many methods (tasks) up which other AI systems can be built.”[111]

128. The AI Now paper states that “GPAI must be regulated throughout the product cycle, not just at the application layer, in order to account for the range of stakeholders involved.”

129. The AI Now Institute paper emphasizes that “potential harms are wide-ranging, including effects on privacy, representation, and access to social services that are dependent on protected traits such as race and gender.”

K. Risks to Democracy

130. The Public Broadcasting Service has reported that “The implications for the 2024 campaigns and elections are as large as they are troubling: Generative AI can not only rapidly produce targeted campaign emails, texts or videos, it also could be used to mislead voters, impersonate candidates and undermine elections on a scale and at a speed not yet seen.”[112]

131. In the article "How ChatGPT Hijacks Democracy," a computer security expert and a data scientist at Harvard University explain how effective content moderation will become

---

[110] AI Now Institute, *Five considerations to guide the regulation of “General Purpose AI” in the EU’s AI Act* (Apr 2023), https://ainowinstitute.org/wp-content/uploads/2023/04/GPAI-Policy-Brief.pdf

[111] Id at 1.

[112] PBS, *AI-generated disinformation poses threat of misleading voters in 2024 election,* (May 14, 2023), https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election

even more complicated, especially when elected officials are the targets."[113] ChatGPT could also "mimic the work that the Russian Internet Research Agency did in its attempt to influence our 2016 elections, but without the agency's reported multimillion-dollar budget and hundreds of employees."

132. A Brookings Commentary on the impact of generative AI on the 2024 election states that "Generative AI can develop messages aimed at those upset with immigration the economy, abortion policy, critical race theory ,transgender issues or the Ukraine War. It can also create messages that take advantage or social and political discontent, and use AI as a major engagement and persuasion tool." [114]

133. The Brennan Center for Justice has warned that "malign actors could deploy generative AI with the intent to suppress votes or circumvent defenses that secure elections." [115] The analysis also highlights how "Influence campaigns could deploy tailored chatbots to customize interactions based on voter characteristics, adapting manipulation tactics in real time to increase their persuasive effect."

134. Chatbots and deepfake audio could also exacerbate threats to election systems "through phishing efforts that are personalized, convincing, and likely more effective than what we've seen in the past."[116]

135. Recent headlines reveal the range of concerns about AI and the upcoming elections:

---

[113] Nathan E. Sanders and Bruce Schneier, *How ChatGPT Hijacks Democracy* (Jan. 15, 2023), https://www.nytimes.com/2023/01/15/opinion/ai-chatgpt-lobbying-democracy.html
[114] Darrell M West, *How AI will transform the 2024 elections,* Brookings Commentary (May 3, 2023), https://www.brookings.edu/articles/how-ai-will-transform-the-2024-elections/
[115] Mekela Panditharatne, *How AI Puts Elections at Risk and the Needed Safeguards,* Brennan Center for Justice, Analysis (Jun. 13, 2023), https://www.brennancenter.org/our-work/analysis-opinion/how-ai-puts-elections-risk-and-needed-safeguards
[116] Id.

- Reuters, *Deepfaking it: America's 2024 election collides with AI boom,* May 30, 2023

- AP, *AI presents political peril for 2024 with threat to mislead voters*, May 14, 2023

- US News and World Report*, Artificial Intelligence Brings 'Nightmare' Scenario to 2024 Presidential Campaign: Analysts - With the 2024 presidential election fast approaching and zero federal regulations in place to combat false AI-generated political stunts, voters likely will be left questioning not only what they know but what they see. than scared of deepfakes,* July 7, 2023

- New York Post, *AI 'deepfakes' poised to wreak havoc on 2024 presidential election: experts,* June 14, 2023

136. OpenAI itself has warned that large language models will enable disinformation campaigns. The report notes that "Generative models could be trained specifically for capabilities that are useful for influence operations."[117]

137. The Business and Human Rights Resource Center invited Microsoft and OpenAI to respond to concerns from researchers about ChatGPT's impact on democratic processes, the Companies did not respond.[118]

138. The Federal Trade Commission may be the only federal agency with the opportunity and authority at this time to regulate ChatGPT so as to diminish threats to the 2024 election.

---

[117] OpenAI, *Forecasting potential misuses of language models for disinformation campaigns and how to reduce risks,* (Jan. 11, 2023), https://openai.com/research/forecasting-misuse; Josh A. Goldstein1, Girish Sastry, Micah Musser, Renée DiResta, Matthew Gentzel, and Katerina Sedova, *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations,* (Jan. 10, 2023), https://arxiv.org/abs/2301.04246

[118] Global: *Researchers raise concerns about ChatGPT's impact on democracy* (Mar. 17, 2023), https://www.business-humanrights.org/en/latest-news/researchers-raise-concerns-about-chatgpts-impact-on-democracy/

IV. Further Points Regarding Statements of the FTC on Generative AI

139. On April 18, 2023, FTC Commissioners testified before the House Energy and Commerce Committee.[119] During the course of the hearing, Commissioner Bedoya asserted that the FTC has the authority to enforce consumer protection measures arising out of risks from AI technologies.

140. In an editorial for the New York Times, FTC Chair Lina Kahn described the earlier failure to develop necessary regulations for the Internet.[120] She observed that "What began as a revolutionary set of technologies ended up concentrating enormous private power over key services and locking in business models that come at extraordinary cost to our privacy and security." She concluded, "As the use of A.I. becomes more widespread, public officials have a responsibility to ensure this hard-learned history doesn't repeat itself." She further stated, "Enforcers and regulators must be vigilant."

141. The FTC's recent business guidance on AI deception makes clear the risk of cyber-crime, financial fraud using generative AI tools, and states "The FTC Act's prohibition on deceptive or unfair conduct can apply if you make, sell, or use a tool that is effectively designed to deceive – even if that's not its intended or sole purpose."[121] The guidance also sets out risks that developers should consider, primarily, "whether there are reasonably foreseeable risks of fraud or harm" and whether "developers are taking measures to effectively mitigate those risks" or whether "developers are over-relying on post-release detection".

---

[119] House Energy and Commerce Committee, Innovation, Data, and Commerce Sub-Committee Hearing, *Fiscal Year 2024 Federal Trade Commission Budget* (Apr. 18, 2023), https://energycommerce.house.gov/calendars?start=2023-04-01&end=2023-04-30

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

[121] Michael Atleson, *Chatbots, deepfakes, and voice clones: AI deception for sale,* FTC, Business Blog (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

142. In the May 2023 business guidance on consumer trust and generative AI tools, the FTC states that, "Design or use of a product can also violate the FTC Act if it is unfair."[122] The guidance also states that:

> FTC staff is focusing intensely on how companies may choose to use AI technology, including new generative AI tools, in ways that can have actual and substantial impact on consumers.

V. Conclusion

143. Consumer protection agencies around the world have launched investigations of OpenAI. Leading experts and consumer organizations have identified numerous risks with ChatGPT. The President of the United States has repeatedly said that companies should not release AI products that are not safe. The company itself has acknowledged numerous risks to public safety. The Federal Trade Commission has assured the public that AI is subject to legal rules and that the Commission has authority. Yet, the FTC has not even stated whether it has opened an investigation of the most rapidly adopted consumer product in history.

144. The FTC must act now. The longer the FTC delays, the more difficult it will be to establish necessary safeguards for generative AI products in the future. And the FTC knows this.

Respectfully submitted,

Marc Rotenberg, CAIDP General Counsel
D.C. Bar # 422825
rotenberg@caidp.org

Merve Hickok, CAIDP Research Director
hickok@caidp.org

Grace Thomson

[122] Michael Atleson, *The Luring Test: AI and the engineering of consumer trust,* FTC, Business Blog (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust

CAIDP Research Fellow

Christabel Randolph
CAIDP Law Fellow

Sunny Gandhi
CAIDP Research Assistant

Desmon Israel
CAIDP Research Assistant

Washington, DC
July 10, 2023