Chatbots, AI and the future of privacy

Mar 31, 2023 Save This ()

Ali Jessani
IAPP Member Contributor (/about/person/0011P000011CwwWQAS)

Chatbots are now all the rage. They have been the subject of numerous investigative news pieces (https://www.nytimes.com/2023/02/16/technology/chatbots-explained.html) and countless Twitter posts (https://twitter.com/MovingToTheSun/status/1625156575202537474), and multiple companies are investing billions of dollars to further develop the technology. We have only reached the tip of the iceberg, but chatbots and other generative artificial intelligence tools are here to stay, and they will inevitably revolutionize how we interact with technology and with each other.

Though AI and machine learning are nothing new, generative AI is different because it is already embedded into consumer culture. Instead of companies using AI and ML to improve their products and services behind the scenes, chatbots and other generative AI tools are being used by consumers for everyday use. This is already leading to unanticipated consequences. For example, some school districts (https://www.cnn.com/2023/01/05/tech/chatgpt-nyc-school-ban/index.html#:~:text=check%20back%20later.-,New%20York%20City%20public%20schools%20ban%20access%20to,tl banned chatbots because they believe using them will lead to negative learning outcomes for students. Meanwhile, in an employment context, chatbots are playing an active role (https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/28/dont-let-chatbots-throw-off-your-job-search-game/?sh=3c19b31a6a2c) in the hiring process, which impacts both job applicants and HR employees that could potentially be replaced by these systems. The unresolved societal issues relating to the prevalence of AI are evolving as quickly as the technology itself.

The growth of chatbots and related AI tools may have unintended consequences for consumer privacy. Harvesting data is critical for AI tools to develop. Chatbots in particular scrape billions of data points (https://www.sciencefocus.com/future-technology/gpt-3/) from across the internet to train and update their predictive language models. In fact, if you ask ChatGPT what information it uses, it will tell you it was "trained on a large dataset of text data, consisting of billions of words, phrases, and sentences," which included "a diverse range of text sources, including books, articles, websites, and other digital content." In terms of sources, ChatGPT's latest update, GPT-4, (https://openai.com/research/gpt-4) claims it was trained using publicly available data (including internet data), as well as data licensed by the developers.

When asked, ChatGPT insists it does not have any personal information about users. But the reality is more complicated, partly because the rules governing personal information are evolving almost as rapidly as AI technology itself. New privacy laws going into effect – such as the California Privacy Rights Act – are implementing an expansive definition of personal information, one that includes inferences a business can make about a privacy concerns.

For example, the more I use a particular chatbot, the more it will learn about me. That is the nature of AI. It will, of course, process the information I directly provide, but it could also theoretically make certain, well-informed assumptions about me. These assumptions may be based on my age, gender, profession, interests and billions of additional data points it has processed about other, potentially similar users. This information is valuable as it is exactly the type of deterministic data advertisers rely on for targeting purposes. If chatbots and related AI tools truly go mainstream, they could provide advertisers a whole host of new information for serving tailored ads that is likely more accurate than the types of data they currently use. This creates some potential benefits for consumers but also further exacerbates the concerns we may have with the targeted advertising model in general, an area that has already been the subject of heavy scrutiny from privacy regulators.

There are also potential privacy concerns related to what a generative AI tool could tell a user about other individuals. Right now, at least theoretically, a chatbot will not provide nonpublic information about someone else if asked for it. But one can easily imagine a scenario where a company develops a chatbot not bound by the same limitations. Similar to how a chatbot could make profiling inferences about its own users, it could also develop the same assumptions about any individual on the internet using their likes, Tweets, comments and other publicly available data points. And then there is the "I, Robot" scenario, where a potentially malicious actor could use a chatbot to steal passwords and other sensitive data for illicit purposes. These are only a few of the potential data protection concerns posed by the rise of generative AI.

To be clear, privacy law already has some rules that apply to these issues. There are standards for what is and what is not personal information, i.e., the specific definitions of deidentified, aggregated and publicly available information must be accounted for. When personal information is being processed, notice, consent, contracting and a whole host of other requirements potentially apply. There are additional regulations for specific use cases, such as targeted advertising and automated decision making. There are also data security obligations for personal information and laws that apply when certain categories of information are breached.

Though existing data privacy laws provide at least some form of protection for consumers in relation to this emerging technology, there is an opportunity for us to proactively address the unique privacy ramifications of generative AI before it becomes even further ingrained in our everyday lives. Instead of regulating from behind, like we have attempted to do with targeted advertising, we can set the rules about data use and purposes for generative AI from the very beginning. This approach can mitigate some of the unanticipated concerns we may have with this technology, at least from a privacy perspective.

However, even if we agree proactively addressing privacy concerns in generative AI is the right approach, there are still questions around implementation. For example, who should take the lead on regulating on this issue? Should the rules come from U.S. Congress, or should states lead, as they have with comprehensive privacy proposals? Is this an area the U.S. Federal Trade Commission should address through its future rulemaking, or should we rely on industry self-regulation as we have in the targeted advertising space? There are also scoping issues. Should privacy issues related to AI be addressed as part of regulating privacy more generally, such as through laws like the CPRA, or should we have separate rules for AI to specifically address a whole host of potential issues related to this technology, as have been proposed in Europe and Canada?

These are only a few of the many issues that will shape the debate around regulating generative AI. If these conversations happen sooner rather than later and lead to the development of an appropriate regulatory framework, we will be able to integrate this evolving technology into our daily lives while also being comfortable with the relevant risks, including those related to consumer privacy.

iapp CPE credits approved Approved CDPO, CDPO/BR, CDPO/FR, CIPM, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPT, LGPD

SUBMIT FOR CPES (/CERTIFY/CPE-SUBMIT/)

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200