

ChatGPT data leak has Italian lawmakers scrambling to regulate data collection

reader comments

49 with

Share this story

Today an Italian regulator, the Guarantor for the Protection of Personal Data (referred to by its Italian acronym, GPDP), announced a temporary ban on ChatGPT in Italy. The ban is effective immediately and will remain in place while the regulator investigates its concerns that OpenAI—the developer of ChatGPT—is unlawfully collecting Italian Internet users' personal data to train the conversational AI software and has no age verification system in place to prevent kids from accessing the tool.

The Italian ban comes after a ChatGPT data breach on March 20, exposing "user conversations and information relating to the payment of subscribers to the paid service," GPDP said in its press release. OpenAI notified users impacted by the breach and said it was "committed to protecting our users' privacy and keeping their data safe," apologizing for falling "short of that commitment, and of our users' expectations."

Ars could not immediately reach OpenAI to comment. The company has 20 days to respond with proposed measures that could address GPDP's concerns or face fines of up to 20 million euro or 4 percent of OpenAI's gross revenue.

Potential mitigation efforts to lift the ban could include notifying users about how OpenAI collects their data and implementing an age verification system to stop young kids from using ChatGPT.

Advertisement

GPDP is also concerned that ChatGPT's answers to text prompts can manipulate data and potentially mislead users by inaccurately processing data and ultimately sharing misinformation.

Currently, GPDP said there is no legal basis for OpenAI to collect and store personal data to train its AI model, which ChatGPT uses to simulate and process convincingly real conversations. There is also no age verification system to prevent minors from being exposed to answers to text prompts that are "absolutely unsuitable" to younger users' "degree of development and self-awareness."

Ars could not immediately reach GPDP to comment on the next steps in its investigation.

Because OpenAI is not currently based in the European Union, the company has up to 60 days to appeal the ban, according to a GPDP document.

Should governments be restricting AI tools?

ChatGPT is just one of many AI tools spurring a lively ethics debate, with some critics urging regulators to slow down AI technology development until the risks of mass adoption are fully understood. However, according to Reuters, ChatGPT is the fastest-growing consumer application in history—reaching 100 monthly active users within a couple of months of its launch—which is likely why it has become one of the first popular AI tools to face a government ban.

The heightened scrutiny of OpenAI's products in particular has seemingly just begun. Earlier this week, a nonprofit AI research group submitted a complaint to the US Federal Trade Commission about OpenAI's product GPT-4, claiming it was "biased, deceptive," and poses "a risk to privacy and public safety." GPT-4 is trained on a massive amount of online data and is already available to ChatGPT Plus subscribers and powers Microsoft's Bing.

<https://arstechnica.com/?p=1928298>