EU votes to ban AI in biometric surveillance, require disclosure from AI systems

Enlarge / The EU flag in front of an AI-generated background.
EU / Stable Diffusion

reader comments

47 with

On Wednesday, European Union officials voted to implement stricter proposed regulations concerning AI, according to Reuters. The updated draft of the "AI Act" law includes a ban on the use of AI in biometric surveillance and requires systems like OpenAI's ChatGPT to reveal when content has been generated by AI. While the draft is still non-binding, it gives a strong indication of how EU regulators are thinking about AI.

The new changes to the European Commission's proposed law—which have not yet been finalized—intend to shield EU citizens from potential threats linked to machine learning technology.

The changes come amid the proliferation of generative AI systems that imitate human conversational abilities, such as OpenAI's ChatGPT and GPT-4, which have triggered controversial calls for action among AI scientists and industry executives regarding potential societal risks. However, the EU's proposed AI Act is over 2 years old, so it isn't just a knee-jerk

response to AI hype. It includes provisions that guard against other types of AI harm that are more grounded in the here and now than a hypothetical AI takeover.

“While Big Tech companies are sounding the alarm over their own creations, Europe has gone ahead and proposed a concrete response to the risks AI is starting to pose,” said Brando Benifei, who is co-rapporteur of the bill. (A co-rapporteur is similar to a co-sponsor of a bill in the US Congress, sharing responsibility with another person for drafting and guiding proposed legislation through the legislative process.)

The new draft of the AI Act includes a provision that would ban companies from scraping biometric data (such as user photos) from social media for facial recognition training purposes. News of firms like Clearview AI using this practice to create facial recognition systems drew severe criticism from privacy advocates in 2020. However, Reuters reports that this rule might be a source of contention with some EU countries who oppose a blanket ban on AI in biometric surveillance.

Advertisement

The new EU draft also imposes disclosure and transparency measures on generative AI. Image synthesis services like Midjourney would be required to disclose AI-generated content to help people identify synthesized images. The bill would also require that generative AI companies provide summaries of copyrighted material scraped and utilized in the training of each system. While the publishing industry backs this proposal, according to The New York Times, tech developers argue against its technical feasibility.

Additionally, creators of generative AI systems would be required to implement safeguards to prevent the generation of illegal content, and companies working on “high-risk applications” must assess their potential impact on fundamental rights and the environment. The current draft of

the EU law designates AI systems that could influence voters and elections as “high-risk.” It also classifies systems used by social media platforms with over 45 million users under the same category, thus encompassing platforms like Meta and Twitter.

According to Reuters, Microsoft and IBM applaud the new rules proposed by EU lawmakers, though they hope for further refinement of the proposed legislation. “We believe that AI requires legislative guardrails, alignment efforts at an international level, and meaningful voluntary actions by companies that develop and deploy AI,” a spokesperson for Microsoft told the news service.

However, despite growing calls for AI regulation, some companies like Meta have downplayed the potential threats of machine learning systems. At a conference in Paris on Wednesday, Meta Chief AI Scientist Yann LeCun said, “AI is intrinsically good because the effect of AI is to make people smarter.”

Also, some critics think the alarm over the existential risk from AI systems is overblown and only serves to aid companies like Microsoft and OpenAI achieve regulatory capture—using their clout and influence to shape regulations to their advantage. Especially concerning potential US-based AI regulation, critics argue that allowing tech giants to write the rules could harm smaller firms and stifle competition.

The European Commission first introduced the AI Act draft rules in April 2021, and some have criticized the slow pace of regulations on the global stage, but with the technology changing so quickly, it’s difficult to keep up. EU industry chief Thierry Breton emphasized the need for swift action rather than delaying progress. “AI raises a lot of questions—socially, ethically, economically,” he said. “But now is not the time to hit any ‘pause button.’ On the contrary, it is about acting fast and taking responsibility.”

Experts say that after considerable debate over the new rules among EU member nations, a final version of the AI Act isn’t expected until later this year.

https://arstechnica.com/?p=1948103