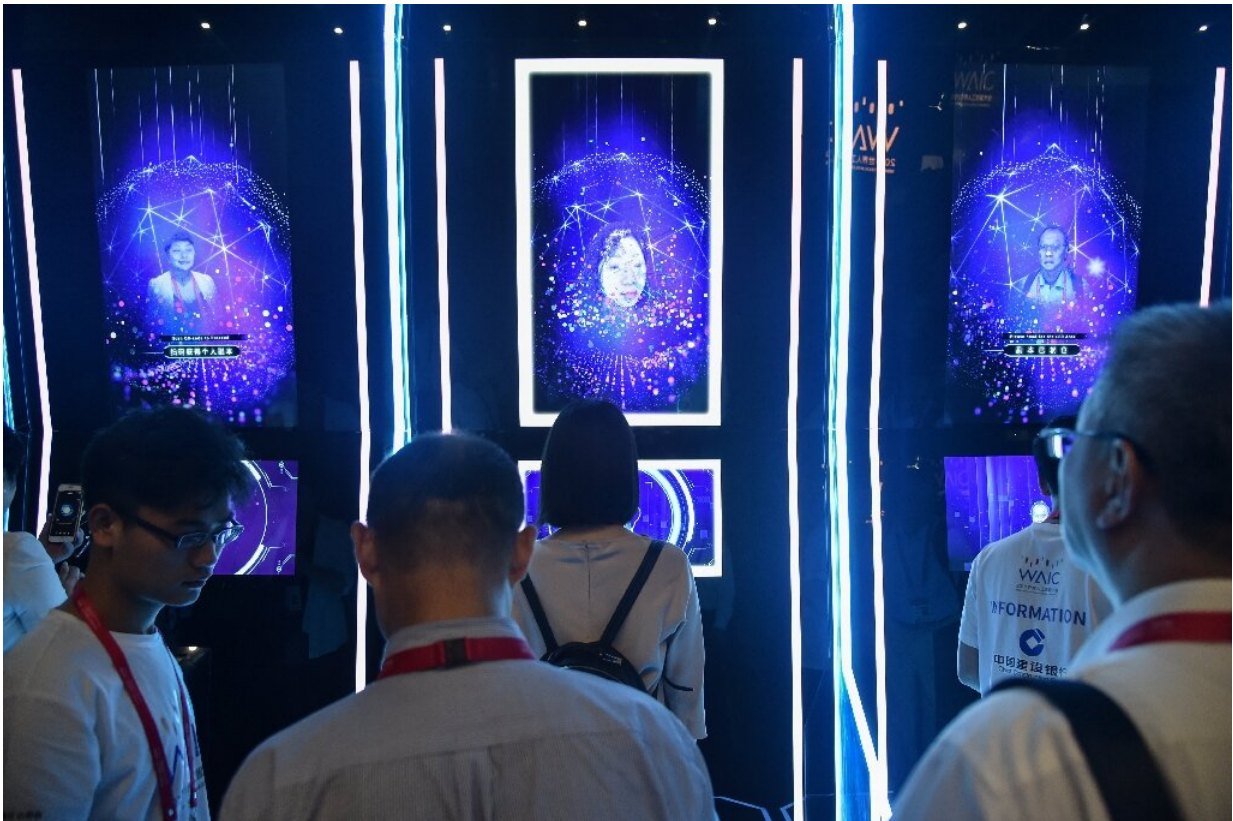# China to require 'security assessment' for new AI products

April 11 2023, by Peter CATTERALL

A flurry of Chinese companies are rushing to develop AI services following the launch of US-based OpenAI's ChatGPT.

New AI products developed in China will have to undergo a security assessment before being released and must reflect "core socialist values",

a sweeping new draft law by the country's internet regulator showed Tuesday.

The fresh regulations come as a flurry of Chinese companies rush to develop artificial intelligence services that can mimic human speech since San Francisco-based OpenAI launched ChatGPT in November, sparking a gold rush in the market.

Rapid advancements in AI have stoked global alarm over the technology's potential for disinformation and misuse, with deepfake images and people shown mouthing things they never said.

"Before providing services to the public that use generative AI products, a security assessment shall be applied for through national internet regulatory departments," the draft law, released by the Cyberspace Administration of China, reads.

The draft law—dubbed "Administrative Measures for Generative Artificial Intelligence Services"—aims to ensure "the healthy development and standardized application of generative AI technology", it read.

AI-generated content, it continued, needs to "reflect core socialist values, and must not contain content on subversion of state power".

It must also not contain, among other things, "terrorist or extremist propaganda", "ethnic hatred" or "other content that may disrupt economic and social order."

The Cyberspace Administration of China said it was seeking public input on the contents of the new regulations, which under Beijing's highly centralized political system are almost certain to become law.

AI perceptions: trust and understanding

Percent of people polled who express trust in the use of Aritifical Intelligence, plus proportion saying they have a "good understanding" of AI
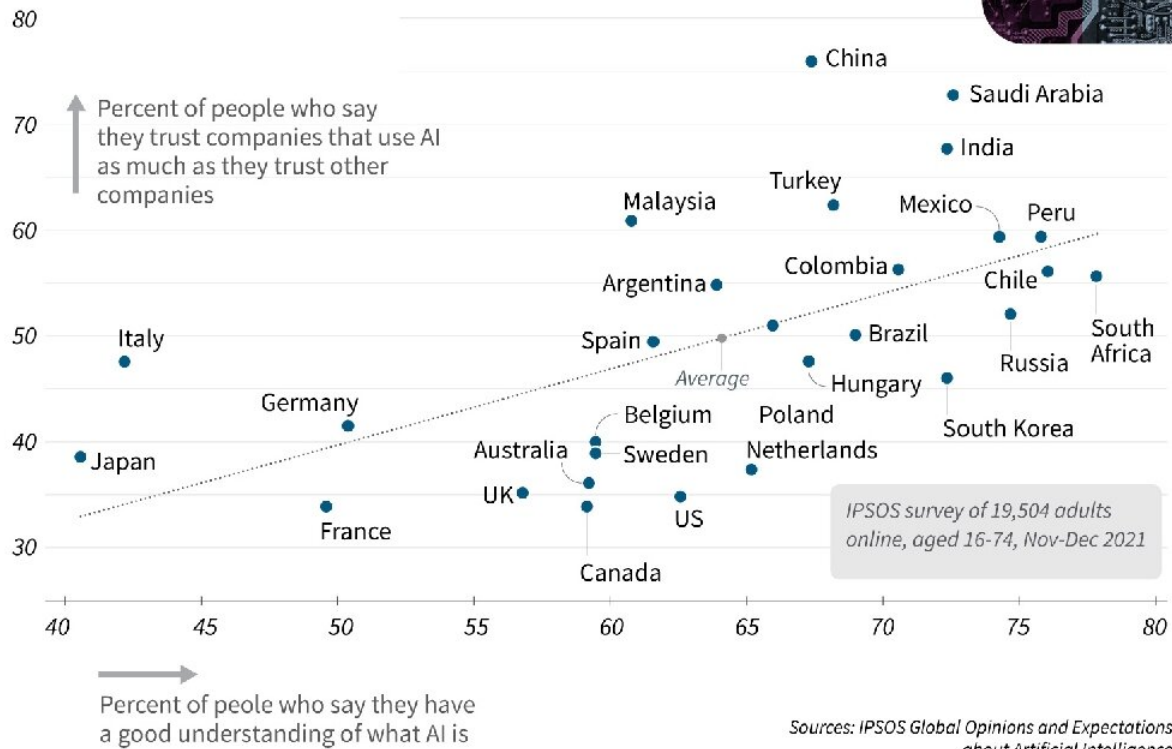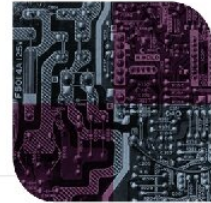

Chart showing percent of people expressing trust in Artificial Intelligence, and people saying they have a good understanding of AI in selected countries according to an IPSOS poll released in 2022.

'Strictest so far'

"The new CAC draft document is one of the strictest measures for generative AI so far," Andy Chun, adjunct professor at City University of Hong Kong, told AFP.

Companies submitting security assessments will need to "be very careful to ensure each data source used for AI learning must be within guidelines, accurate, unbiased, and not infringe on IP rights of others," he said.

"Ensuring accuracy is hard. No generative AI system to date can do that," said Chun.

The regulatory crackdown comes as China's tech giants ramp up their efforts in the closely-watched sector.

Alibaba's cloud computing unit on Tuesday unveiled its own product called Tongyi Qianwen, which is expected to be rolled out across the tech giant's office workplace communications software and household appliances.

CEO Daniel Zhang said in a statement that the software came in a "technological watershed moment driven by generative AI and cloud computing".

Beijing has announced ambitious plans to become a global leader in the field of AI by 2030.

And Baidu—which operates the country's leading search engine—released its own "Ernie Bot" AI chat product last month.

But investors were unimpressed by the bot's display of linguistic and math skills at an unveiling, sending shares falling by as much as 10 percent.

ChatGPT is unavailable in China, but the American software is also gaining a base of Chinese users who use virtual private networks to get around the ban, deploying it to write essays and cram for exams.

And a 24-year-old Shanghai blogger caused a stir this month when he used AI technology to "resurrect" his dead grandmother, producing lifelike imagery of his interactions with the deceased relative.

Beijing has announced ambitious plans to become a global leader in the field of AI by 2030, and consultancy group McKinsey estimates the sector could add about $600 billion every year to China's gross domestic product by then.

But it has also warned that deepfakes present a "danger to national security and social stability".

Beijing in January enforced new rules that would require businesses offering deepfake services to obtain the real identities of their users. They also require deepfake content to be appropriately tagged to avoid "any confusion".

© 2023 AFP

Citation: China to require 'security assessment' for new AI products (2023, April 11) retrieved 28 April 2024 from https://techxplore.com/news/2023-04-china-law-require-ai-products.html