NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down

April 4 2024, by Jake Offenhartz

New York City Mayor Eric Adams speaks during a news conference at City Hall, Dec. 12, 2023, in New York. An artificial intelligence-powered chatbot meant to help small business owners in New York City has come under fire for dispensing bizarre advice that misstates local policies and advises companies to violate the law. But the chatbot remains online, even as Adams acknowledged Tuesday, April 2, 2024, that its answers were “wrong in some areas.” Credit: AP

Photo/Peter K. Afriyie, File

An artificial intelligence-powered chatbot created by New York City to help small business owners is under criticism for dispensing bizarre advice that misstates local policies and advises companies to violate the law.

But days after the issues were first reported last week by tech news outlet The Markup, the city has opted to leave the tool on its official government website. Mayor Eric Adams defended the decision this week even as he acknowledged the chatbot's answers were "wrong in some areas."

Launched in October as a "one-stop shop" for business owners, the chatbot offers users algorithmically generated text responses to questions about navigating the city's bureaucratic maze.

It includes a disclaimer that it may "occasionally produce incorrect, harmful or biased" information and the caveat, since-strengthened, that its answers are not legal advice.

It continues to dole out false guidance, troubling experts who say the buggy system highlights the dangers of governments embracing AI-powered systems without sufficient guardrails.

"They're rolling out software that is unproven without oversight," said Julia Stoyanovich, a computer science professor and director of the Center for Responsible AI at New York University. "It's clear they have no intention of doing what's responsible."

In responses to questions posed Wednesday, the chatbot falsely

suggested it is legal for an employer to fire a worker who complains about sexual harassment, doesn't disclose a pregnancy or refuses to cut their dreadlocks. Contradicting two of the city's signature waste initiatives, it claimed that businesses can put their trash in black garbage bags and are not required to compost.

At times, the bot's answers veered into the absurd. Asked if a restaurant could serve cheese nibbled on by a rodent, it responded: "Yes, you can still serve the cheese to customers if it has rat bites," before adding that it was important to assess the "the extent of the damage caused by the rat" and to "inform customers about the situation."

A spokesperson for Microsoft, which powers the bot through its Azure AI services, said the company was working with city employees "to improve the service and ensure the outputs are accurate and grounded on the city's official documentation."

At a press conference Tuesday, Adams, a Democrat, suggested that allowing users to find issues is just part of ironing out kinks in new technology.

"Anyone that knows technology knows this is how it's done," he said. "Only those who are fearful sit down and say, 'Oh, it is not working the way we want, now we have to run away from it all together.' I don't live that way."

Stoyanovich called that approach "reckless and irresponsible."

Scientists have long voiced concerns about the drawbacks of these kinds of large language models, which are trained on troves of text pulled from the internet and prone to spitting out answers that are inaccurate and illogical.

But as the success of ChatGPT and other chatbots have captured the public attention, private companies have rolled out their own products, with mixed results. Earlier this month, a court ordered Air Canada to refund a customer after a company chatbot misstated the airline's refund policy. Both TurboTax and H&R Block have faced recent criticism for deploying chatbots that give out bad tax-prep advice.

Jevin West, a professor at the University of Washington and co-founder of the Center for an Informed Public, said the stakes are especially high when the models are promoted by the public sector.

"There's a different level of trust that's given to government," West said. "Public officials need to consider what kind of damage they can do if someone was to follow this advice and get themselves in trouble."

Experts say other cities that use chatbots have typically confined them to a more limited set of inputs, cutting down on misinformation.

Ted Ross, the chief information officer in Los Angeles, said the city closely curated the content used by its chatbots, which do not rely on large language models.

The pitfalls of New York's chatbot should serve as a cautionary tale for other cities, said Suresh Venkatasubramanian, the director of the Center for Technological Responsibility, Reimagination, and Redesign at Brown University.

"It should make cities think about why they want to use chatbots, and what problem they are trying to solve," he wrote in an email. "If the chatbots are used to replace a person, then you lose accountability while not getting anything in return."