OpenAI chief faces tough audience of privacy regulators in vowing responsible development

By Mike Swift

Brief

The top lawyer at OpenAI sat shoulder to shoulder today with the privacy regulators of Canada and Italy who represent two data-protection agencies that have been most aggressive in publicly probing the maker of ChatGPT. There was no hostility, but neither was there acceptance. Privacy regulators from Canada, Norway and Italy today said that as attractive as the technology is, its development can't move forward at the sacrifice of human values such as protecting privacy as a fundamental right.

Full Text

The top lawyer at OpenAI sat shoulder to shoulder today with the privacy regulators of Canada and Italy who represent two data-protection agencies that have been most aggressive in publicly probing the maker of ChatGPT. There was no hostility, but neither was there acceptance.

Last spring, the Office of the Privacy Commissioner of Canada and the Garante Italia, respectively, announced probes of the maker of ChatGPT, and temporarily banned its use. Speaking at the annual global gathering of privacy regulators,* neither was willing to say today that their concerns about the technology have been satisfied, despite the Italian DPA ending its ban.

Philippe Dufresne, Canada's privacy commissioner, acknowledged there are significant benefits to society from generative AI from applications such as combating climate change and finding new drugs. But he suggested it might be necessary to slow the deployment of AI systems if they can't be shown to be safe.

"I agree that it's up to society and up to democracies to say this is what we stand for as a society, including privacy as a fundamental right," Dufresne said. "We wouldn't think of building a super-fast plane by neglecting safety, by neglecting pre-departure checks. And we wouldn't say, 'well, it's so innovative and it's so efficient, it's such a game-changer, that, you know, we're prepared to sacrifice it'."

Guido Scorza of the Italian regulator said the best way for generative AI to fully benefit society is for regulators to perform their watchdog roles, so the technology won't be developed in a way that promotes profits over human values. The Garante Italia has ordered OpenAI to add an age-verification process to its generative AI tool ChatGPT for Italian users by December (see here).

To maximize the benefit of AI to society, the goal of regulators, Scorza said, should be "simply to do our duty, promoting and protecting our privacy right, assuring that the industry . . . in the field of artificial intelligence avoid any kind of sacrifice, of needing any kind of sacrifice of humanity, any kind of sacrifice although it arrives in the name of business and money. Nothing more. Nothing less."

A third regulator speaking today, Tobias Judin of the Norwegian Data Protection Authority, said it would be "a drastic step" but not unthinkable for a privacy regulator to order an AI company to delete its entire algorithm, if it was built with scraped personal data that could be personally tied to individuals and if the company is unable to segregate out or anonymize illegally scaped personal data.

That is a possible outcome because of the danger of what is known to programmers as a Model Inversion, or "MI" attack, in which attackers try to extract personal information from a working AI model, Judin said.

If the personal data couldn't be isolated because of the model's design choices, "whereby, well, you can't do that without completely scrapping the model, I don't think it could be ruled out that someone could be asked to completely scrap their model," Judin said. "And obviously, yes, there would be repercussions to this, but I think that right now, a lot of companies are just trying to be first — just trying to get their model out there, trying to get people addicted to the technology."

Dufresne took the step of publicly announcing the OPC's probe of OpenAI in April (see here), he said, because he

believed it was important to show the public that regulators have their eyes on artificial intelligence and its risks. In addition to the Canadian and Italian probes, MLex has independently confirmed that the US Federal Trade Commission is investigating OpenAI's scraping of data from the Internet to train its algorithms (see here).

Che Chang, the general counsel for OpenAI, said the company was founded with the intention of benefitting humanity, not making money. The company was initially a nonprofit, although it has taken large investments from for-profit backers such as Microsoft. Chang said it has put limits in how much money can be earned by investors and employees to make sure OpenAI stays true to those values.

Chang said OpenAI has been careful to reach out to regulators and other governmental organizations to say, "hey, in order to do this right, we have to all work together. It's not just industry rushing forward to try to maximize profits," he said. OpenAI is among 15 AI companies that have committed to a voluntary code of conduct with the US Biden Administration and is participating in the UK Safety Summit next month (see here).

"We think, in discussions with policy makers, [generative AI] is extremely valuable. And that's being borne out by the fact that people are using these tools to increase productivity and connect with people and do all these things they're capable of," Chang said.

**45th Global Privacy Assembly 2023, Bermuda; Oct. 15-20, 2023.*

Please e-mail editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.