

POLITICO

OPEN SEASON: Debate about open-source AI has been bubbling at least since that infamous Google memo leaked in May. Arguments over whether open-source is dangerous, or simply dangerous to Big Tech's profit margins, raged on at both the AI summit and the AI Fringe this week.

Two camps: The likes of OpenAI and Anthropic, which have built huge proprietary models, are inclined to champion closed models. In the other corner are those developing open-source AI like Eleuther, Stability AI, and Meta. Existential risk types are in the first camp – because how could something so risky be let loose into the general populace?

What went down at the summit: Summit participants we spoke to said the open-source question was heavily discussed – it's mentioned a total of seven times in the government summary, including a reference to the need to “discuss open and closed release but not too heatedly” (emphasis ours).

No consensus: Computer scientist Wendy Hall said at the roundtables she attended, there was “no real consensus on this.” She said the arguments for open-source are “a bit like saying anyone can have a gun.” But at the same time, “these dilemmas are not easy to solve, because if you ban open-source, then all the power goes to the big companies.”

Yesterday at the AI Fringe: OpenUK CEO Amanda Brock argued that open-source models reduce the risk of systemic failures arising from over-dependence on one company's AI model and that open models are far more transparent.

What the hell is open source anyway? A moral panic in the mold of the encryption battle might just be brewing. At recent political party conferences, Brock says people were telling her “we need to regulate open-source,” but if she probed them on what open-source was, “they could not answer that question.” “Everybody has an opinion and a very small group of people seem to have an understanding,” she said.

What are the politicians saying? The ones we spoke to yesterday seemed more inclined to fly the banner for open-source. “I see tiny startups that are already billion-dollar-plus companies within a matter of literally months off the back of open source,” deputy PM Oliver Dowden told us. “So I think there was a very high bar to restrict open source in any way.”

Also at the AI Fringe: Github senior policy manager Peter Cihon said the questions he always asks about potential AI misuse are, “What is the counterfactual risk for this activity from AI?”

(for example, how bad is the problem of misinformation if we add in AI?) and “What is the marginal risk of making a model openly available?” I’m sorry Peter, that sounds far too rational for the frenzied policy debates surely set to unfold.

Open-source’s asks: Cihon argued that “regulation is needed today” but that its primary criterion shouldn’t be whether a model is open or closed, but high risk use cases – like the approach taken by the EU’s AI Act. “Those [high risk models] should be closely scrutinized and regulated – open source or proprietary,” he said.

<https://www.politico.com/>