Uber Technologies, Inc.
1515 3rd Street
San Francisco, CA 94158

Uber

March 27, 2024

Stephanie Weiner
Chief Counsel
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4898
Washington, D.C. 20230

RE: Dual Use Foundation Artificial Intelligence Models with Widely Available Model Weights; Request for Comments, NTIA–2023–0009

Dear Chief Counsel Weiner:

Thank you for the opportunity to provide input on the National Telecommunications and Information Administration's (NTIA) Request for Comments regarding the potential risks, benefits, other implications, and appropriate policy and regulatory approaches to dual-use foundation models for which the model weights are widely available. Uber Technologies, Inc. ("Uber") respectfully submits these comments in response to the Request for Comments.

The potential of artificial intelligence (AI) and algorithms and their promise to solve societal problems is immense. At Uber, we are proud of the ways we have been able to leverage technology to help facilitate billions of trips and deliveries around the world. The introduction of these new services has expanded access to transportation and economic opportunity, helping individuals overcome gaps in transportation systems and creating value for workers, customers, and small business restaurants. At the same time, we recognize that the use of AI can raise questions and concerns about safety and the risk to individuals.

Both the risks and the potential benefits of AI are present when we consider the recent developments in generative AI. At Uber, we believe that technological progress and the use of AI can be accomplished both safely and collaboratively. Historically, open-source technology has been critical to safe, technological progress. In order for deployers of AI to build on these AI systems, they need access to and confidence in the data and the models they are using.

As a technology company that is involved in the early development and application of AI technology that benefits consumers in their daily activities and transactions, we appreciate the opportunity to share our perspective. We are deeply involved both in the development and deployment of AI models and make use of both "open" and "closed" models. As an entity in the ecosystem that is not developing the large, dual-use foundational models that the government is

concerned about but may use these models to enhance our existing products and services, we have a unique perspective.

At a high level, Uber believes that widely available model weights, and the source code and data of these models, are extremely important for:

- **Innovation: Widely available model weights spur innovation in the field of AI. By democratizing access to foundational AI models, innovators from diverse backgrounds can build upon existing frameworks, accelerating the pace of technological advancement and increasing competition in the space.**
- **Safety and security: Widely available model weights, source code, and data are necessary to foster accountability, facilitate collaboration in risk mitigation, and promote ethical and responsible AI development.**

Fostering Innovation and Democratizing Access to Model Weights

Open-source frameworks play a crucial role in driving innovation in AI. They enable the creation of benchmarks, tools, and methodologies to ensure the quality and safety of AI systems.

Foundation models with widely available model weights offer several benefits. Firstly, by making model weights openly available, we can accelerate innovation across many fields, including but not limited to, education, training, medicine, and computer science. This is particularly evident as open-source software enhances accessibility and fosters a culture of knowledge-sharing. For example, this can create a positive separation between AI developers and deployers, facilitating the development of better tools and scientific advancement. This division allows AI developers to focus on innovating and refining models, while deployers can dedicate their efforts to using the technology to advance their respective industries.

Moreover, in the financial sector, open-source AI systems are employed to analyze data, improve security systems, and provide banking forecasts. Within healthcare, AI is increasingly applied as a tool for diagnostics and tasks such as medical image analysis, owing to its accuracy comparable to that of expert clinicians.

Secondly, this inclusive approach increases competition and diversifies access to generative AI models. This fosters collaboration and a diverse technological landscape that not only benefits corporate entities like Uber but also the broader tech sector and society at large.

Thirdly, open-source models create a more level playing field and lower barriers to entry for AI use, ensuring that more individuals and organizations can access and improve upon existing technology. This allows AI innovations to flourish at an accelerated rate.

Finally, the increased accessibility facilitated by open-source frameworks fuels economic growth by enabling companies to leverage existing source code and data to increase productivity. This also paves the way for novel AI-based solutions to address societal challenges in various sectors.

Moreover, when open-source data is made public, it enables models to be trained on high-quality, diverse data that ensures that AI systems are more inclusive and representative of different populations.

Safety and Dependability

Ensuring that AI technology is safe is dependent on the availability of weight models, source code, and training data. As large language models (LLMs) continue to evolve, access to the underlying models and the data used to train them allows developers and deployers to ensure the data is free of intellectual property violations, biases, and sensitive or private information. Without such access, it becomes challenging to conduct thorough assessments of the data quality and mitigate associated risks effectively.

Currently, several governments are considering how to assign liability to companies and individuals deploying AI systems. If a deployer is forced to assume liability for a model that it cannot assess or evaluate, it will hamper innovation, as this may be a risk they are unwilling to take.

Open-source models can improve oversight in the evaluation of models for biases, limitations, and societal impacts, thereby enhancing transparency and accountability of the technology. This enables stakeholders to scrutinize models more effectively and identify potential issues or bad actors. Moreover, requiring parties to make their training data and code available can help build societal trust and prevent risks associated with the misuse of open model weights.

Having data and source code simultaneously available is especially beneficial during the development stage of new and emerging technologies, as it allows for rapid identification and resolution of potential security issues. By leveraging the collective intelligence and expertise of the open-source community, developers can identify and address software flaws and vulnerabilities. Addressing these issues early on will further fuel AI research globally and enhance AI safety efforts.

Navigating Risks: Balancing Openness with Security and Regulation

While there are many benefits and opportunities associated with widely available model weights, training data, and source code, we realize that open source can also present challenges for AI technology.

The risks associated with widely available model weights are multifaceted and are grounded in transparency. Firstly, the broad accessibility of model weights enables broader access for people to use the technology. While developers can leverage these LLMs for various applications, including educational and innovative purposes, there is also the risk of the potential misuse of the technology. For example, bad actors have used LLMs to develop and spread misinformation by using the technology to create deep fakes.

Widely available model weights can also increase cybersecurity risks—if individuals or businesses fail to effectively secure or manage their open-source systems, it can increase the likelihood of a security breach.

It is important to note that the misuse of generative AI by bad actors will emerge regardless of whether only model weights or both training data and source code are simultaneously made widely available. Nevertheless, we will be better able to tackle the challenges posed by the misuse of AI if training data and source code are made widely available. This approach would not only expedite and democratize AI research but it would also foster a larger community of LLM users and experts equipped to counteract bad actors. For companies like Uber that will utilize these systems, it is critical to correct issues with training data and address cybersecurity risks.

Applying restrictions on widely available model weights may also inadvertently incentivize the development of closed, proprietary models that operate outside of transparent and accountable frameworks. This could further exacerbate risks associated with AI technology, so it is important to keep model weights widely available to maintain a dynamic and inclusive system for managing AI risks.

While we have outlined some of the risks associated with making model weights—and their training data and source code—widely available, these risks must be weighed against the benefits of fostering open innovation and transparency in AI development. By promoting responsible AI practices and ensuring access to data and source code, policymakers can support the advancement and democratization of AI technology while mitigating potential risks associated with its misuse.

We hope that this response will provide valuable insight for the report on the potential benefits, risks, and implications of dual-use foundations. Thank you for considering our input on this important matter. We look forward to continuing to collaborate with NTIA and other stakeholders to promote the responsible development and adoption of AI technology.

Sincerely,

CR Wooters
Head of Federal Affairs
Uber Technologies, Inc.