Joint Statement on AI Safety and Openness

October 31, 2023

We are at a critical juncture in AI governance. To mitigate current and future harms from AI systems, we need to embrace openness, transparency, and broad access. This needs to be a global priority.

Yes, openly available models come with risks and vulnerabilities — AI models can be abused by malicious actors or deployed by ill-equipped developers. However, we have seen time and time again that the same holds true for proprietary technologies — and that increasing public access and scrutiny makes technology safer, not more dangerous. The idea that tight and proprietary control of foundational AI models is the only path to protecting us from society-scale harm is naive at best, dangerous at worst.

Further, history shows us that quickly rushing towards the wrong kind of regulation can lead to concentrations of power in ways that hurt competition and innovation. Open models can inform an open debate and improve policy making. If our objectives are safety, security and accountability, then openness and transparency are essential ingredients to get us there.

We are in the midst of a dynamic discourse about what 'open' signifies in the AI era. This important debate should not slow us down. Rather, it should speed us up, encouraging us to experiment, learn and develop new ways to leverage openness in a race to AI safety.

We need to invest in a spectrum of approaches — from open source to open science — that can serve as the bedrock for:

A. Accelerating the understanding of AI capabilities risks and harms by enabling independent research, collaboration and knowledge sharing.
B. Increasing public scrutiny and accountability by helping regulators adopt tools to monitor large scale AI systems.
C. Lowering the barriers to entry for new players focused on creating responsible AI.

As signatories to this letter, we are a diverse group — scientists, policymakers, engineers, activists, entrepreneurs, educators and journalists. We represent different, and sometimes divergent, perspectives, including different views on how open source AI should be managed and released. However, there is one thing we strongly agree on: open, responsible and transparent approaches will be critical to keeping us safe and secure in the AI era.

When it comes to AI safety and security, openness is an antidote, not a poison.

Share on Mastodon **Share on X**

Add your signature

Your full name

Email address (professional)

name@example.com

Job title

Affiliation

By submitting this form you agree to Mozilla handling your information as explained in this privacy notice.

Sign the letter

1821

signatures

Signatories

Camille François, Columbia University

Mark Surman, Mozilla

Deborah Raji, UC Berkeley

Maria Ressa Rappler, Nobel Peace Prize Laureate

Stella Biderman, EleutherAI

Alondra Nelson, Institute for Advanced Study

Arthur Mensch, MistralAI

Marietje Schaake, Stanford University

Abeba Birhane, Mozilla Fellow

Bruce Schneier, Berkman Center

Mitchell Baker, Mozilla

Bruno Sportisse, INRIA

Anne Bouverot, Ecole Normale Supérieure

Alexandra Reeve Givens, CDT

Cedric O, MistralAI

Andrew Ng, AI Fund

Yann Lecun, Meta

Jean-Noël Barrot, Minister for Digital Affairs, France

Amba Kak, AI Now

Joy Buolamwini, Algorithmic Justice League

Julien Chaumond, Hugging Face

Brian Behlendorf, Linux Foundation

Eric Von Hippel, MIT Sloan School of Business

Moez Draief, Mozilla.ai

Pelonomi Moiloa, LelapaAI

Philippe Beaudoin, Waverly

Raffi Krikorian, Technically Optimistic

Audrey Tang, Minister of Digital Affairs, Taiwan

Jimmy Wales, Wikimedia Foundation

Krishna Gade, Fiddler AI

John Borthwick, Betaworks

Karim Lakhani, Harvard Business School

Stefano Maffulli, Open Source Initiative

Arvind Narayanan, Princeton University

Aviya Skowron, EleutherAI

Catherine Stihler, Creative Commons

Nabiha Syed, The Markup

Tim O’Reilly, O'Reilly Media

Nicole Wong, Former Deputy U.S. Chief Technology Officer

Irina Rish, Mila - Quebec AI Institute

Mohamed Nanabhay, Mozilla Ventures

J. Bob Alotta, Mozilla

Imo Udom, Mozilla

Ayah Bdeir, Mozilla

Blake Richards, McGill/Mila

Andrea Renda, CEPS

Jenia Jitsev, LAION/Juelich Supercomputing Center & Helmholtz Research Center Juelich

Charles Gorintin, MistralAI

Daniel J. Beutel, Flower Labs

Nicholas Lane, Flower Labs

Taner Topal, Flower Labs

Aaron Gokaslan, Cornell University

Shayne Longpre, MIT

Luca Soldaini, Allen Institute for AI

Joelle Pineau, Meta

Michiel van de Panne, University of British Columbia

Nawar Alsafar, Bytez Inc

Holly Peck, Bytez Inc

Susan Hendrickson, Harvard University

Sharad Sharma, iSPIRT Foundation

Andy Stepanian, The Sparrow Project

Paul Keller, Open Future

Goran Marby, Ybram Consulting

Huu Nguyen, Ontocord.ai; LAION.ai

Mike Bracken, Public Digital

Elaheh Ahmadi, Themis AI

Umakant Soni, AI Foundry, ART Venture Fund

Saoud Khalifah, Mozilla

Merouane Debbah, Khalifah University

Felix Reda, Former Member of the European Parliament

Brett Solomon, Access Now

David Morar, Open Technology Institute

Frédérick Douzet, IFG - GEODE, Université Paris 8

Yacine Jernite, Hugging Face

Anjney Midha, A16z

Hessie Jones, LAION

Jeffrey McGregor, Truepic Inc

Victor Storchan, Mozilla.ai

Sri Krishnamurthy, QuantUniversity

Jorn Lyseggen, meltwater

Corynne McSherry, Electronic Frontier Foundation

Brian Granger, Project Jupyter

See all 1821 signatures

Website Privacy Notice Cookies Legal Community Participation Guidelines

Visit Mozilla Corporation’s not-for-profit parent, the Mozilla Foundation.