ACLU CENTER FOR DEMOCRACY & TECHNOLOGY ELECTRONIC FRONTIER FOUNDATION OPEN TECHNOLOGY INSTITUTE

May 21, 2024

Hon. Michael McCaul
2300 Rayburn House Office Building
50 Independence Ave. SW
Washington, D.C. 20515-4310

Hon. Gregory Meeks
2310 Rayburn House Office Building
50 Independence Ave. SW
Washington, D.C. 20515-3205

Dear Chair McCaul, Ranking Member Meeks, and Members of the House Foreign Affairs Committee:

The below-signed civil rights, civil liberties, and open technology advocates write to express concerns with H.R. 8315, the ENFORCE Act. The bill would allow the Department of Commerce to effectively ban online publication of artificial intelligence (AI) systems in order to prevent them from being available in foreign countries — consequently hampering ongoing civil rights efforts to promote transparency in AI systems, impeding academic and scientific research, and raising First Amendment concerns. To help mitigate these concerns, we recommend including language in the statute or perhaps in a committee report instructing the Bureau of Industry and Security (BIS) to ensure that existing provisions for "published" software accommodate AI systems.

First, we are concerned the bill would hamper algorithmic transparency, as publication or release of key components of AI models (especially online) would make them available abroad — and thus constitute an export. Although the Export Administration Regulations (EAR) has special provisions for the publication of software, they may not be applicable here. The EAR exempts "published" software, meaning the software is "made available to the public without restrictions upon its further dissemination."[1] However, different conceptions of "openness" are emerging in the AI community, which may not meet the requirement that there not be restrictions on further dissemination.[2] For example, the components of a model might be released with limitations on uses, such as for research or prohibiting harmful uses, or be supplied through an API. Regardless of the degree of openness, it can often help further goals around algorithmic transparency.

Some of the signatories of this letter recently filed comments with a coalition of civil rights organizations on a similar issue before the National Telecommunications and Information

[1] 15 C.F.R. § 734.7(a).
[2] David Gray Widder, Sarah West & Meredith Whittaker, *Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI*, SSRN at 4 (2023), here.

Administration.[3] In those comments, the civil rights coalition urged NTIA to recognize that restrictions on the publication of model weights — a component of foundational AI models — would hamper efforts around algorithmic transparency, which are key to protecting civil rights in algorithmic decision-making. Similarly, other signatories observed in separate comments to NTIA that "open models" increase "transparency, education, testing, and trust around the use of AI, enabling researchers and journalists to audit and write about AI systems' impact on different demographic groups."[4]

Second, many of AI's most promising applications have already been fueled by widely available, "open" AI models. For example, key model architectures like AlexNet, frameworks like PyTorch and TensorFlow, and research on topics like attention mechanisms were all made widely available, fueling significant advances in AI research and development.[5] Open models also help accelerate scientific research because they can be less expensive, easier to fine-tune, and supportive of reproducible research.

Finally, the bill may also raise First Amendment concerns. In *Junger v. Daley*, the Court of Appeals agreed that source code is protected speech.[6] It said, "Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."[7] Although there is robust debate on whether the publication of some parts of AI models is protected speech,[8] the ENFORCE Act would cover the entire AI model, including any underlying source code. Consequently, the ENFORCE Act may trigger heightened judicial scrutiny, which would require evidence that the risks that the bill seeks to mitigate are not speculative[9] and that it is narrowly tailored to those risks.[10]

The bill may have difficulty clearing that standard. For example, its definition of "covered artificial intelligence system" is *not* limited to any specific national security harms. Instead, it reaches any AI system that "exhibits . . . capabilities . . . that pose a serious risk to the national security." The listed harms — chemical, biological, radiological, or nuclear (CBRN)

[3] Comments of ACLU et al., NTIA Dual Use Foundation Artificial Intelligence Models With Widely Available Model Weights, Docket No. 240216-0052 (Mar. 27, 2024), here.

[4] Comments of the Center for Democracy & Technology, Mozilla, et al. at 2, NTIA Dual Use Foundation Artificial Intelligence Models With Widely Available Model Weights, Docket No. 240216-0052 (Mar. 25, 2024), here (citing Stephen Casper et al., *Black-Box Access is Insufficient for Rigorous AI Audits*, arXiv (2024), here).

[5] Mark Surman et al., Mozilla, Accelerating Progress Toward Trustworthy AI at 6 (2024), here.

[6] Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

[7] *Id.* at 485; *accord* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001).

[8] Alan Z. Rozenshtein, *There Is No General First Amendment Right to Distribute Machine-Learning Model Weights*, Lawfare (Apr. 4, 2024), here ("Unlike source code, which humans use to express ideas to each other, model weights function solely as machine-readable instructions.").

[9] Erie v. Pap's A.M., 529 U.S. 277, 313-14 (2000) (Souter, J., concurring in part and dissenting in part) ("The upshot of these cases is that intermediate scrutiny requires a regulating government to make some demonstration of an evidentiary basis for the harm it claims to flow from the expressive activity . . . . What is clear is that the evidence of reliance must be a matter of demonstrated fact, not speculative supposition.")

[10] United States v. Chi Mak, 683 F.3d 1126, 1134–35 (9th Cir. 2012).

weapons, offensive cyber operations, and evasion of human control — are merely examples, as indicated by the "such as by" text introducing them.

Other export regulations are more narrowly tailored. For example, restrictions on the export of "technical data" regarding munitions have been upheld.[11] "Technical data," however, is limited information "which is *required* for the design, development, production," or operation of munitions[12] — a much narrower scope than the definition of "covered artificial intelligence system" in the ENFORCE Act. Further, to our knowledge, there is no evidence beyond "speculative supposition"[13] that the use of AI systems appreciably increases the risks posed by CBRNs, cyber offensives, or evasion of human control beyond the status quo.[14]

To preserve efforts around transparency, either the bill or a committee report should instruct BIS to ensure that the existing exception for "published" software includes "open" AI systems. As noted above, the concept of "openness" is still evolving regarding AI systems, and BIS should ensure that the EAR accommodates that evolution. Although some concerns may continue to exist, the ability to publish models or their components will help advance transparency, civil rights, and research.

Thank you for your consideration, and please do not hesitate to contact us at cvenzke@aclu.org with any questions.

Sincerely,

American Civil Liberties Union
Center for Democracy & Technology
Electronic Frontier Foundation
New America's Open Technology Institute

[11] Def. Distributed v. United States Dep't of State, 838 F.3d 451, 459 (5th Cir. 2016); United States v. Chi Mak, 683 F.3d 1126, 1134 (9th Cir. 2012).
[12] 22 C.F.R. § 120.33(a)(1).
[13] *Pap's A.M.*, 529 U.S. at 14 (2000) (Souter, J., concurring in part and dissenting in part).
[14] Rishi Bommasani et al., *Considerations for Governing Open Foundation Models*, HAI Policy & Society Issue Brief (Dec. 2023), here ("Correctly characterizing these distinct risks requires centering the marginal risk: To what extent do open foundation models increase risk relative to (a) closed foundation models or (b) pre-existing technologies like search engines?").