PRYON

March 27, 2024

National Telecommunications and Information Administration
1401 Constitution Ave. NW
Washington, D.C. 20230

Re: NTIA Docket No. – "Dual Use Foundation Artificial Intelligence Models With Widely Available Model Weights"

Thank you for providing the Pryon Inc. ("Pryon"), with the opportunity to comment in response to the National Telecommunications and Information Administration's (NTIA) "**Dual Use Foundation Artificial Intelligence Models With Widely Available Model Weights**" (*Request for Comment)* proceeding.

About Pryon

Pryon was created by the Artificial Intelligence Pioneers instrumental in developing Alexa, Siri, and Watson, and is used by federal agencies, state governments, and leading enterprises. Our team has worked in artificial intelligence for decades, and have been behind more than one-hundred patents in the space. We have deep technical, policy, and product experience in the space, and were very encouraged by NTIA's focus on these critical areas.

A word about Pryon before we provide our comments. Pryon's mission is to reduce the distance between knowledge and people. Pryon turns vast quantities of critical, fragmented, and rapidly changing content into accurate, timely, and verifiable answers via the world's first enterprise-grade Knowledge AI Platform. Using best-in-class retrieval technology, Pryon securely extracts answers from all forms of content, including audio, images, text, and video, stored in a myriad of sources. Pryon's Knowledge AI platform is intuitive to use, is accessible via API from any system, and can be deployed in a matter of weeks in the cloud or on-premises. By reducing the distance between workers and content, Pryon builds high-performing, resilient, and responsive organizations.

Comment

In what follows below, we present our comment in terms of risks organized in 5 tables:

- "Social Harms"
- "Privacy & Copyright"
- "Business"
- "Evaluation/Technical/Algorithm," and

PRYON

- "Evolving Viruses and General Harms"

Each row of these tables identifies an actual risk item that is caused by one or more entities, such as Institutional (private, public, for profit, non-profit, etc.) or Individual End Users. In addition, each row compares the severity of the risk based on model being Open or Closed. Finally, each row compares the difficulty of enforcing a remedy for the risk and suggests a method for addressing the risk.

This is not intended to be a complete analysis. Rather, in the spirit of the Request for Comments, we are providing a tabular overview, and we would be pleased to provide more details if helpful. We also do not include other broader risks that are broadly discussed in the press, including an AI becoming "intentful "or "sentient." We also believe this analysis is part of an evolving journey that must deal with the unseen progress of technology in coming years.

Social Harm Risks

Risks	Entity Creating Risk	Risk Level	OAI v CAI Remedy Enforcement	Method
Creating information that incites division and spreads false information.	Individual or Institutional End Users	OAI = CAI	Easier for CAI as # of CAI systems is finite & better known	Filtering/Blocking the input request
Allowing for more convincing "deep fake" videos	Individual or Institutional End Users	OAI = CAI	Easier for CAI as # of CAI systems is finite & better known	Deep Fakes detectors finite & enforceable
Models can contain racial and sexual bias based on the data in the model	Credible Vendors or Developer Groups	OAI is riskier	Easier for CAI as # of CAI systems is finite & better known	Hard to control Data for OAI
Models may be used to replace workers.	Known Enterprises or Unknown Enterprises	OAI = CAI	Easier for CAI as # of CAI systems is finite & better known	Law enforcement on Known or Unknown

Privacy & Copyright Risks

Risks	Entity Creating Risk	Risk Level	OAI v CAI Remedy Enforcement	Method
If PII gets into the model it can be widely distributed	Credible Vendors or Developer Groups	OAI is riskier	Easier for CAI as # of CAI systems is finite & better known	Vendors will comply for business reasons
Company private information could be released to competitors	Individual or Institutional End Users	OAI = CAI	OAI = CAI	Algorithmic prevention technique
Use of Copyrighted material	Credible Vendors or Developer Groups	OAI is riskier	Easier for CAI as # of CAI systems is finite & better known	Law enforcement

PRYON

PRYON

Business Risks

Risks	Entity Creating Risk	Risk Level	OAI v CAI Remedy Enforcement	Method
Change Management & New Release	Individual or Institutional End Users	OAI is riskier	CAI is part of business practice	OAI needs an API layer
Competitive Advantage	Individual or Institutional End Users	Harder with OAI	OAI creates a common playing field	OAI needs a closed innovation layer

Evaluation/Technical/Algorithm Risks

Risks	Entity Creating Risk	Risk Level	OAI v CAI Remedy Enforcement	Method
Huge models are very hard to evaluate	Credible Vendors or Developer Groups	OAI is riskier	CAI vendors are disciplined for Quality Control	OAI needs a closed innovation layer
Impossible to create tests to evaluate all possible negative outcomes.	Credible Vendors or Developer Groups	OAI is riskier	OAI vendors are more disciplined	OAI needs a closed innovation layer

Evolving Viruses & General Harm Risks

Risks	Entity Creating Risk	Risk Level	OAI v CAI Remedy Enforcement	Method
AI created viruses could infect infrastructure and data	Credible Vendors or Developer Groups	OAI is riskier	New kind of threat. CAI vendors more credible	OAI needs a closed innovation layer
Unpredictable / not fully tested could damage infrastructure and data	Credible Vendors or Developer Groups	OAI is riskier	OAI vendors are more disciplined	OAI needs a closed innovation layer

PRYON

Conclusion

Thank you again for offering this opportunity to comment. We believe this is a very important topic, and your attention to this subject only reinforces that the Administration is focusing the appropriate attention on the right subjects at this critical time in the development of artificial intelligence technology.

Respectfully submitted,

Justin S. Antonipillai
Global Head of Government Affairs and
Chief Trust and Legal Officer
Pryon Inc.