1 - NTIA should define the ''open'' model as a model that has the entirety of its weights, training data, and the exact methods that it was created with, open, and replicable by the wider community.

a. There have been multiple occurrences of models close to closed AI systems becoming widely available, for example, LLAMA 1 has been leaked online in its entirety, as has the Mistral Medium model, called Miqu. Such occurrences have occurred times in the past, and will surely occur many times in the future. It is a fact that when a single file finds its way on the internet, there is no way to delete it. And all it takes for a model to leak, is one person in a chain of hundreds of thousands of employees making either an honest mistake, or having some interest in leaking it. Or getting hacked. It's simply impossible to stop such from happening.

b. Based upon my favorite benchmark, yes, it is possible to do such. The benchmark tests performance of LLM's in a very niche logical puzzle category, and as such allows to compare 'intelligence' between them. As it stands right now, Google Bard, Chat GPT 3.5, and Claude-Instant has been beaten in under a year by Mixtral-8x7b. However, to refer to a much more well known and respected benchmark, I'll allow myself to refer to LMSYS Chatbot Arena Leaderboard. According to it, GPT 3.5, Gemini Pro, Claude Instant, Claude 2.1 and Claude 2.0, and other closed AI models from last year all were defeated by Qwen 1.5-72B the reason for this is important but also simple, but, just to note. All of these models took years to get where they ended up. And then, all in less then a year, Alibaba Cloud team managed to get performance far better then all these models, and all in far smaller scale. (It is not public information how large GPT 3.5 is, or other closed models are, but all of the credible speculation I've observed had these models measuring over 120B, which means that Qwen team managed to cut the size of model in half, make it better, and then done such in under a year compared to closed models. Now, to the reason itself, this was possible because the community that gathered around open source LLM's have put in a tremendous amount of work in researching and improving Open Source LLM's, and by leveraging closed-source LLM's to speed certain processes up. And all of this is achievable with current level of technology that we possess right now, and as the technology gets better, and more people use consumer GPU's like RTX 3000 or 4000 series, the amount of potential compute that open source community can spend on novel and often incredibly innovative processes that a hierarchical slow moving organization would take years to develop, will only increase, and with such, Development of open source LLM's will only accelerate.

c. Wide availability of model weights should be defined as a company itself releasing the model with accompanying documentation and information on what data, how exactly, with how much compute, and in what ways the model was trained and made. Otherwise, in my opinion, the model is not widely available or open source.

d. In my opinion, closed source models are more risky for one reason. In the case of all models, as soon as the model is available in any way, shape, or form, it can be used in any number of ways. And it will be attempted to be used in such, so, at that point, all such deployments are of similar risk. However, I would like to point to the incredibly simple process of prompt-injecting, or other ways of bypassing any form of alignment on closed-source models as a simple reality of the situation, which also means that slow internal process of bug fixing in large companies means that closed-source models will have vulnerabilities of many sorts, that will be unpatched for however long it takes, whereas in open source community, bug fixing is constant, as everyone can simply patch whatever flaw that comes up, but with closed source models being closed and less accessible, only few people can, and the entire process takes much longer. Therefore, closed source AI is more dangerous.

i. The best way to guarantee as much safety and benefit over risk when it comes to AI is a full open source release all documentation and development information being open would make it possible to counter-train an AI by anyone with enough of (constantly de facto becoming more affordable, thanks to technological advancement) compute resources to deal with any form of malicious use of the original AI, as well as to train it to counter any such use. Which is far safer than any other option.

2 - The risk is much smaller with open-weighted models, as we can look inside the 'black box', and find any malicious or negative outcome that it can create, and counteract it, instead of risking that a random employee at one of one of hundreds companies that will be using LLM's steals some part of it, and sells it to a hacking group, or a foreign advisory, and we don't learn about it fast enough, and as such, we cannot counteract it fast enough. Whereas transparency that open source provides makes this outcome impossible. Compare the amount of Malware on Windows compared to Linux operating system. This is simply because the open source community is far faster, and often far superior at finding any flaws, and then patching them. Compared to a goliathan hierarchical organization such as Microsoft. As such, open source is far safer.

a. The more actual information and power the open source community possesses, the lower the risk is. Compared to a centralized untransparent organization that very often would face incentives of cover ups, and hiding data, I'd like to point out how many companies are often very reluctant to announce they had been hacked, as they fear investor reaction. Which can often harm many people whose data has leaked in the hack, or have been otherwise compromised by it. Compare this to an open source community, in which there are no incentives to hide vulnerabilities, or any flaws. Instead there is incentive to actually get the work done and get credited for such.

b. No, the open models would not lead to such an outcome, as any group that would be potentially impacted negatively by an open source model, could review it, and find if it's in any way detrimental to their rights or status. Whereas closed source models are a black box that cannot be ever reviewed by anyone. I'd like to point out the recent Google Gemini fiasco, where it generated PoC as Nazis. Because some random employee at Google decided that such would be for the best. Whereas I had never seen Stable Diffusion maliciously changing user prompts, unlike Google Gemini which did such, changing said prompts into something else, just because Google thinks users should be shown that instead. Which ended up being quite hurtful for the PoC community, and lead Google to an extreme move of shelving the product, as they didn't knew how to solve it, as the Big Tech organizations are so large, any change takes ages to occur, which couldn't at all be said of open source community.

c. I do not see any risk to privacy that would exist because of open models existing, as all the data these models would be trained would be publicly available, as such, I do not see any risk to privacy arising from such, unless model would be trained on data that was illegally harvested, which is a crime, and should be handled as such.

d. No, there are no novel ways that would work in such a way, as any such possibility could be easily detected, and then rectified long before any such action could take place. However, in an event of a novel closed source model being stolen, such not being known, as it was hushed up by the company, and then being used to do some harm like such, could absolutely however take place, as companies have far lower incentive to care about safety, compared to any members of public. The incentive of a company isn't safety, but monetary gain, whereas the public at large clearly cares far more about not being impacted by any sort of such attack.

I. I will allow myself to point to my comment in point 2.d

ii. In my opinion, these risks are exactly the same as ones with closed and open operating systems, where open source operating systems such as Linux are far safer, and are by far preferred by biggest companies because of safety. Safety is the main reason why companies like Amazon with its Web Services are running Linux on its servers and not Windows. It's simply because open source is far safer and far faster to patch any flaws, as compared to a sluggish closed source. And even where open source fails, one can switch the component that fails and make a new one themselves, instead of waiting eons on a large company to finally send out a patch.

e. In my opinion, the main risk of open source models being available in one jurisdiction and not the other would be far greater power in information and economy spheres of such jurisdictions in hands of a few big tech companies instead of the public. Meanwhile, in open source jurisdictions, small businesses and researchers could fully customize and use models that fit them best, without having to pay rent to few big tech companies that control everything, and without having to worry about few of these big companies using closed source models to eliminate any sort of competition.

f. The most severe risk in my opinion is concentration of power in hands of a few gigantic companies that would be only ones allowed to possess novel technology, with everyone else forced to rely on them, by undue regulation and de facto monopolization of the sector in hands of a few all-powerful incumbents, achieving the dream of every rent-seeker, and creating a perfect condition for unlimited abuse of power by one of the big tech corporations.

3. The benefits are that anyone, any group, any individual, any researcher, and individual, if they possess any sort of even somewhat new computer, would be able to create and use what they precisely want. This would lead researchers, small businesses and any individual to be able to access whatever they want, without having to deal with seeking of rent by a few big tech companies that would then be able to sway the entire economy with few changes in code. For example, Imagine what if Google is the only company allowed to have an LLM-search, and some dissatisfied employee decides to make it so that the LLM-search is creating pure falsehoods about a certain company, what if the company in question is a single-parent owned small businesses, and the negative false opinions that the model creates, make it go bankrupt, and because Google is a monolithic gigantic company, it might be months or years before such is found, and question there is, would Google have any incentive to come clean about such incident? Whereas, anyone could find such a flaw in an Open-Source model, and would have incentive to note everyone about such. The risk here remains in monopolization and few companies having complete control over information that the public is using, and zero transparency these companies provide, which is a total contrast to the open source community. Where transparency is a prerequisite, and incentives align into making the product best it could be.

a. Instead of using hypotheticals, I will allow myself to use an example that actually occurred. Recently, a few researchers namely: Yang-Hui He, from London Institute for Mathematical Sciences, Thomas Oliver, mathematician at the University of Westminster, and Kyu-Hwan Lee, mathematician at the University of Connecticut, started working on their own machine learning model. Then by December of the last year, their model was able to predict the ranks of elliptic curves with high accuracy. Something that would take an incredible amount of hard and long work if done by humans. This is already a net-benefit to humanity, but what if to create any machine-learning model, they'd have to pass a few years long certification process? What if they'd have to pay Google or Microsoft 500 dollars to be allowed to use their AI, to do what they'd be instead perfectly able to do on their own? In how many cases, we'd be forced to slow down progress of science itself because of most likely overloaded and underfunded bureaucratic process on one side, and on the other side, we'd be forcing any scientist or researcher to pay a defacto tax to a private company, to do something that they would be perfectly able to do on their own.

b. We have already multiple times seen many 'hacks' being done on ChatGPT, this is possible, because it takes a company like OpenAI a far longer amount of time to apply a fix or a change to their program compared to open source community. But, I'd like to also use an another example, Llama-Guard published by Meta is an open source AI that allows the user to create any guardrail in the model they are using at the time, as such allowing safe deployment of LLM in any circumstance, Llama-guard is an open source product as well, which has lead to numerous documented improvements. It is a far better safety model compared to any closed source product, as the swift iteration and bug-patching allows software like it to be made far better then its closed source alternative. It also should be mentioned that in case of Open-Source AI, one can take the product that is being used by any nefarious actor, and then find a way how to make it obsolete, and patch any vulnerability far faster then in case of Closed-Source products. As far as many more eyes and brains have access to it then would happen otherwise.

c. I had already mentioned this before, but yes, by allowing models to be changed, and allowing any member of the public access to them, one can find any flaw, or any inherent bias much faster then with tiny groups of often very insular individuals who otherwise get to make any choice about it. This would make it far easier for members of society from any impacted group to step up, find any flaw, and then be able to correct it, as opposed to the closed source models.

d. I will return to the Qwen model, it is not a secret that China is an adversary of the United States, and the Chinese Communist Party would very much be glad to see the United States hurt in any possible way. And it is fully within my belief that if the Chinese manage to outpace the United States in AI technology development, the Chinese Communist Party will use the technology against the people of America. As such, the biggest danger in national security space would be if the United States would out of its own volition kneecap the technology development by allowing only few big companies to pursue it. Compared to very swiftly iterating Chinese Open Source Models such as Qwen. The reason Chinese Companies that are controlled by the Chinese Communist Party publish Open Source AI is not because they are benevolent, but because they see that the Open Source AI advances much faster compared to the closed source AI. And as such want to exploit that in order to take lead in the technological race. In my opinion, this is one of the main reasons why the United States shouldn't restrict the Open Source community, as it would simply be an action that hurts the United States, whilst bringing benefit only to a few CEO’s of a few big tech companies.

e. In my opinion, as I already mentioned multiple times, the benefits increase as more power is given to the open source community, which is why the more training data and more source code is available, the greater the benefits, as the community is able to take these, and apply them in innovative and often very out-of-the-box ways, helping to progress the technology along.

4. There are really three main components when it comes to making a working machine-learning model. First of them is the basic technique, which is by now already widely diffused through the world, be it transformers like LLm that GPT4 is, or be it diffusion-based models like Stable Diffusion. Should there be any secret not currently widely known technique, I do not believe I have to explain how such would revolutionize the field if released. Second of the components is data, which, obviously, is crucial to creating a good machine learning model, should the data list as well as what data was used be disclosed and released, it could be used in other models and fields, and as such, bring all of the field to another standard. One should mention here that even without data behind models such as GPT4 not being even disclosed, the output based on that data is widely used in the Open Source AI model space, and as such, it is slowly being diffused throughout it as well, even when undisclosed and unreleased, the process is however slower, and creates doubts based on legality of data the companies have used as it has not been disclosed. Finally, then there is ‘secret sauce’ part of what makes a model work, be it RAG, or be it the default instruction-tune prompt, which Open Source community also is working on implementing, just like with data, the process is slower, as it is somewhat of a reverse engineering process, but even with it, the advancements it brings to other model is immense, and only growing over time. Should all of this be released at once, it would only accelerate technological progress.

5. The main risks involved are opaque structure and lack of transparency, as when we don’t know why something is doing a thing, we cannot address it. Imagine you have a dog running around your house making highly irregular and concerning noises, you are however not allowed to inspect the dog, nor even take a glance at the animal. Because of this, you can’t really take any steps to address whatever is causing the behavior of the animal. So, in the case of AI, whatever is causing it to act the way it does. With it being closed source, you would have to trust that a few people will be smart enough, and fast enough to deal with whatever problem pops up, and also worry about their incentive being perfectly aligned to whatever the best result for public is, which in private companies have been not always a case, even when under heavy scrutiny of government, I don’t believe I need to name any names, but just to make my point clear, I’d like to point out to the fact that despite Boeing being the biggest company in the U.S. that is a manufacturer of planes, as of right now, millions of Americans are in heavy doubt over safety of using planes manufactured by the company, because company opaque structure has lead to culture of a lack of safety, transparency, and profit-chasing over all else. The main risk with AI isn’t tied with any technical aspect of it, it is tied with humans acting like humans have acted since the start of written history, and the best way to mitigate such is by forcing as much transparency as possible, and making it easy to inspect and patch any flaw, and the more the eyes and brains are working on such, the higher the chance of such occurring.

a. I believe that unless we are talking of technology that is being developed specially for government, such as malware or spyware that is used to fight terrorist organizations or other hostile entities, it is by far the safest option to release all models as open and transparent, as such makes it possible to address any security concern fast and mitigate it. As such, evaluation like this is not needed.

b. Unless one would forbid all human access to a model, there is not a safeguard that would stop its weights or data from eventually leaking, either through someone hacking a worker, worker being compromised individually themselves, or an user of a model finding a bug. When all that is needed is achieving one success, eventually, even a monkey will be able to write complete works of Shakespeare on a typewriter.

c. It would require the ability to read minds of everyone who accesses the model without a failure at all times, and the ability to stop any hacking attempt from ever being successful, which would require time travel. As such, I remain skeptical of the possibility of either of such being developed any time soon.

d. The only way that I can think of for erasing of such information would be literal destruction of all of the internet, and even then, the model would probably already had spread to hard drives, so these would have to be found and confiscated, and that all would need to be done before someone managed to copy the model weighs onto anything else. The only possible way for this to be achieved would be a global EMP wave that would fly all the electronics, and even then, if any of the hard drives would be shielded, even that would fail. As such, I will say that it seems quite impossible for me.

e. Again, it would require screening of every single employee more than U.S government screens their most sensitive employees, and it would also require absolute inability to be hacked, something literally impossible for any consumer-facing hardware. I do not wish to sound unreasonable here, but I’d like to bring up case of Edward Snowden who was NSA contractor who stole NSA information and published it, or Ana Montes who was a senior analyst at Defense Intelligence Agency who had spied for Cuba for 17 years, or even Jack Teixeira from 102nd Intelligence Wing, who had lead to one of worst leaks of U.S. intelligence in recent memory. In short, if United States, with all power that our country has, is unable to stop various opportunists, ideological zealots, or just plainly unwise people from accessing and then sharing it’s most classified material with foreign adversaries, I do not believe a private company will be able to guarantee such, even if supported by the government.

f. I believe the more eyeballs, and the more brains are working on a model, the more likely it is that a model will be safe, which is why releasing it open-source before deploying it commercially I believe would make it far safer then such model would be otherwise.

g. Yes, such technology already exists, one can just validate it using a checksum.

6. The biggest issue would be lack of transparency and the fact that big tech companies such as Microsoft or Google are using data from we don’t know where, creating models that they themselves don’t fully know how exactly function, and then they attempt to use them often with insufficient input from the community. All of these problems would be solved with increased transparency and a more open stance.

a. Yes, there are many examples of platforms that ended up better when it comes to security compared to more closed platforms. One example would actually be Linux as I already had mentioned in past, however, I would also like to bring attention to Cryptography Wars, which are a description of numerous attempts made by, chief among them, NSA at attempting to limit consumer availability of strongest encryption models, because of fear that NSA will not be able to crack such. In the end, these attempts have failed, as technology has developed past them. (Back in the days of Netscape Navigator, it led to a perverse situation where security was directly impacted, as the public was de facto forced to use 40-bit encryption, because 128 bits was deemed too ‘risky’. Which meant even at the time it took a few days to decrypt it, using an off the shelf average computer.). Currently, the average SSL encryption uses 256 bits, as in the end, the public resistance combined with technological advances made it obvious that one cannot just keep technological progress locked away, whist at same time, U.S. government has managed to end up in position where the public is able to be safe from terrorist threats, as well as other undue harm, but the technological progress isn’t constrained to widely unrealistic and backwards looking ides.

b. Cheap availability of very customizable machine learning would be a great equalizer for many small businesses and organizations, allowing them to buy a few GPU’s for less then $10.000 USD and be able to run software that before only the biggest companies could afford. Which I believe would allow for greater degree of competition both healthier and more free of a market.

c. I believe the safest license would be one that allows free and absolute access to the community, whilst at same time, requiring a small percentage of royalties paid to a company that released the model, making for an open, healthy, safe, and realistic economic ecosystem.

d. I do not believe such, as many models have been released under all more or less all available licenses in existence, and they seem to be working quite well for both developers and users.

7. Voluntary mechanisms do not work, as many times it has been shown that companies don’t keep to them, I do not wish to bring up Boeing case, but in that case it has been given allowance to certify their planes on their own, the end result is well, I do not believe I need to repeat what I already said. At the same time, the domestic regulatory system already in place I believe works just the way it should, and is more than appropriate. Meanwhile, when it comes to international systems, I’d like to point out the Comprehensive Nuclear-Test-Ban Treaty, or the Intermediate-Range Nuclear Forces Treaty. If we are unable to have a discussion with our adversaries about banning technology that risks annihilating the human race with nuclear apocalypse, I do not believe we can approach countries like China and Russia and believe that they are going to be working in a good faith. The most likely end result of such a treaty would be the United States being forced to keep to its unreasonable bad faith terms, meanwhile Russia and China would do whatever it would take to gain any advantage over the United States, as such, any such treaty, in my opinion, is foolishness. And, to bring my point closer home, I would point out how Ukraine feels about the Budapest Memorandum, in which they gave up their nuclear weaponry that was passed to Ukraine from the Soviet Union, in return for Russia being one of guarantees of Ukraine independence and territorial integrity. I believe that now in hind-sight we can say that the treaty was nothing else than a mistake on the Ukrainian part.

a. Once again, I do not believe any reasonable measures can be used to achieve a 100% rate of success when it comes to preventing such access. When it comes to legal, I’d like to point out countless leaks that occur in software space such as Video Games, when it comes to security, I’d like to point out intelligence leaks. Neither works to fully guarantee security, and when cat is out of the bag, nothing reasonable works to undo the process.

b. I believe that wide availability of AI models makes it easier to show government what it actually available and what these models can do, instead of either the hyper-optimistic claims made by people who have a very large stake in people buy-in when it comes to believing that their own product can achieve Sci-fi results and in a year they will have a model that is equal to a human, or people who believe that models are already aware and scheming to kill us.

c. I believe that should always be disclaimed, ideally together with what data has been used with that model, and other technical details.

d. I believe the government should incentivize releasing models as open source with transparent data and details, but nothing more than that, as I believe that strikes the best balance between risk and benefit.

i. I do not believe any additional bodies are needed.

e. I believe the role of model hosting services is guaranteeing that users are not downloading malware, alongside the same responsibility as any other ordinary website, as such, I don’t see any need for additional regulation.

f. I believe that the government should follow the same standards as every other group that would be using models.

g. Technological progress should be the main goal of the United States, as well as making sure we aren’t lagging in AI space compared to our adversaries. The most important partners would be the EU alongside countries such as South Korea, Japan and Taiwan. However, cooperation with any opponent such as China and Russia shouldn’t really be put into action, as these countries wouldn’t approach any agreement in good faith.

h. I believe the most important insight would be the Japanese government's positive relationship to technological development, and allowing the space to flourish.

i. I do not believe any objective and actually proven mechanism or procedure exists, or, in fact, could exist, as inherent biases would lead to unfortunate incidents such as Google Gemini image generation fiasco.

j. Realistically, open weight foundation models will be widely accessible, as such we shouldn’t think about stopping access to them, but instead about how we can change other areas and procedures to be safer from any possible interference from any adversary.

8. I believe the smartest approach is allowing things more or less as they are, but making them more transparent, and making sure no monopolistic practices are taking place. If there should be a rapid change to space, and we suddenly wake up tomorrow and OpenAI announces that they actually have a fully synthetic being that can think, talk, feel, and act, obviously, there should be greater changes to the current systems and mechanisms put in place, but as of right now, other then incentivizing greater transparency, I do not see a reason for greater government involvement.

a. Security through obscurity never worked before, and never can work, as such, I believe any action in regulatory space should keep such in mind, and seek to strike right balance between competition, innovation, and making sure that our government and country is ready for whatever challenge lies ahead, whilst we reap benefits of economic growth that automation always brings.

b I would simply like to point out that such would be unwise, as available computation power scales far faster then any regulation would. For example, Nvidia mainline spec consumer GPU from 2016. The GTX 1080 Ti could achieve 11.3 Tflops, today, the Nvidia mainline spec consumer GPU, RTX 4090, which was released two years ago, can achieve 1321.2 Tensorflop thanks to their new tensor cores. This means that in six years, Nvidia managed to make their mainline consumer GPU 120 times stronger in operations that would be used for AI. All that in six years in a consumer market, when one looks at a more professional focused market, the change grows even greater. This would lead into an absurd situation where in a few years, it may be that a Video Game AI would be defined as a frontier model, and be regulated by it, which would obviously be a mistake.

c. I do not believe any current available risk metric is in any form accurate to actual risk as it exists, and I’d recommend anyone who thinks otherwise to try playing around with models that are currently released, both open and closed source. Llama 70B chat when combined with Llama guard is far safer than GPT4 as it currently exists.

9. I believe by far the most important issue and topic here is preventing monopolization of AI space under a few big tech players. I can mention this again and again, but I cannot put enough weight on how dangerous and risky monopolization in such a case would be. Social media, when monopolized under a few companies, ended up horrible. Air travel in the United States currently has issues because Boeing exists in a de facto duopoly with Airbus and Boeing being only sane choices that many carriers are faced with. Whenever monopolization occurs, everyone but the company behind it suffers, and regulatory capture where regulations are created so that only few big companies can pass them, and all others are deterred from entering the field because it’s too resource intensive to be compliant with regulation ends up only benefiting the companies. Not the country, not the people, not the technological progress. That’s by far my biggest concern in the AI space.