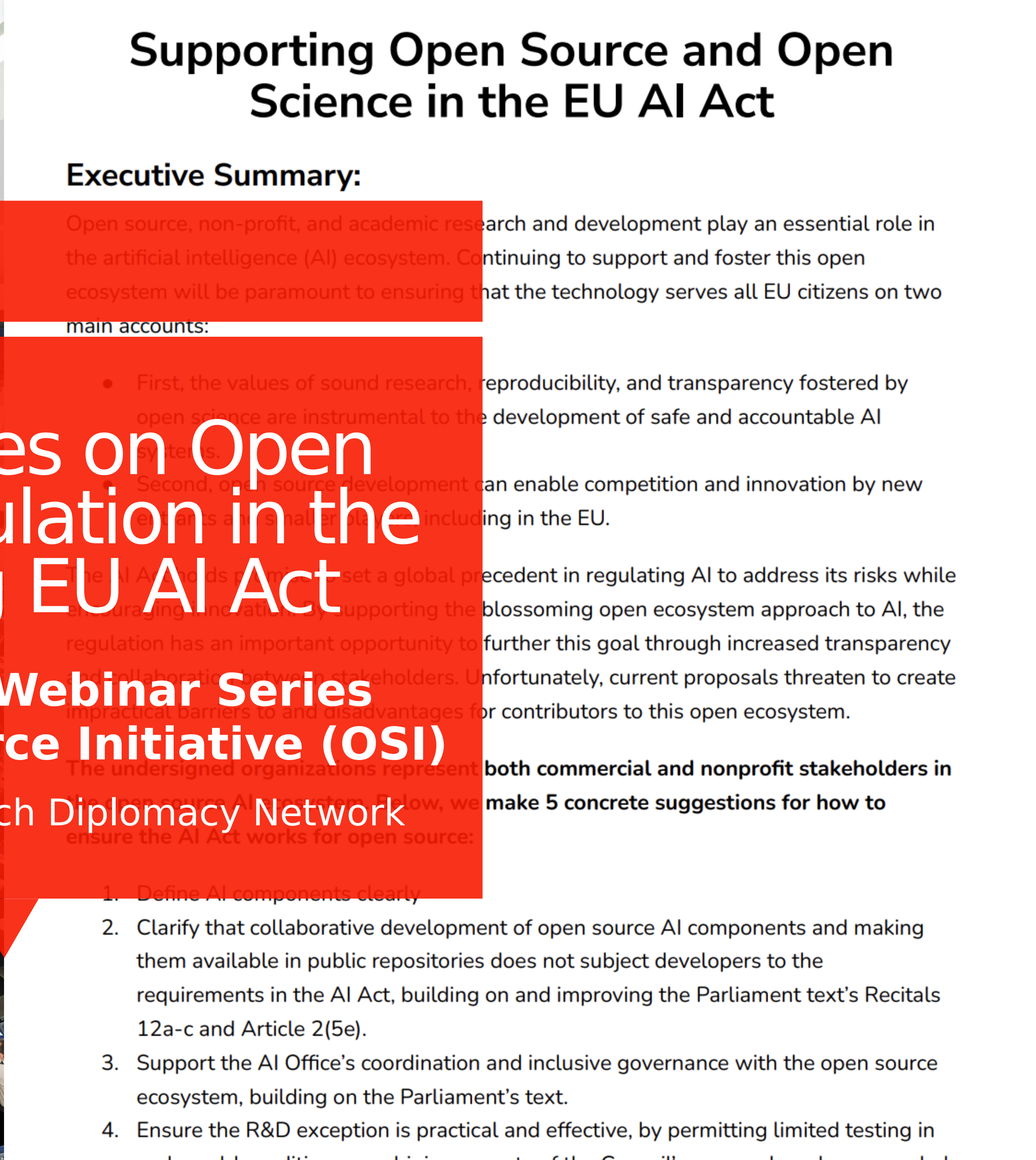
Perspectives on Open Source Regulation in the upcoming EU AI Act

Deep Dive: AI Webinar Series (2023) Open Source Initiative (OSI)

Katharina Koerner, Tech Diplomacy Network



Supporting Open Source and Open Science in the EU AI Act

Executive Summary:

Open source, non-profit, and academic research and development play an essential role in the artificial intelligence (AI) ecosystem. Continuing to support and foster this open ecosystem will be paramount to ensuring that the technology serves all EU citizens on two main accounts:

- First, the values of sound research, reproducibility, and transparency fostered by open science are instrumental to the development of safe and accountable AI systems.
- Second, open source development can enable competition and innovation by new entrants and smaller players, including in the EU.

The AI Act holds promise to set a global precedent in regulating AI to address its risks while encouraging innovation. By supporting the blossoming open ecosystem approach to AI, the regulation has an important opportunity to further this goal through increased transparency and collaboration between stakeholders. Unfortunately, current proposals threaten to create impractical barriers to and disadvantages for contributors to this open ecosystem.

The undersigned organizations represent both commercial and nonprofit stakeholders in the open source AI ecosystem. Below, we make 5 concrete suggestions for how to ensure the AI Act works for open source:

1. Define AI components clearly
2. Clarify that collaborative development of open source AI components and making them available in public repositories does not subject developers to the requirements in the AI Act, building on and improving the Parliament text's Recitals 12a-c and Article 2(5e).
3. Support the AI Office's coordination and inclusive governance with the open source ecosystem, building on the Parliament's text.
4. Ensure the R&D exception is practical and effective, by permitting limited testing in

Content

- Significance of Open Source in the EU Economy
- Policy Support for Open Source
- Overview of draft EU AI Act & Negotiations
- Scope of EU AI Act and Open-Source exceptions
- Challenges around Foundations models
- Preparing for the EU AI Act

European Commission

The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy

FINAL STUDY REPORT

Knut Blind
Mirko Böhm
Paula Grzegorzewska
Andrew Katz
Sachiko Muto
Sivan Pätsch
Torben Schubert

Fraunhofer ISI

ofe OpenForu
Europe

Significance of open source in the EU economy

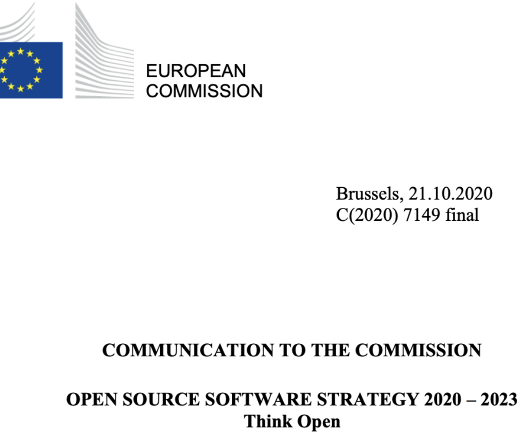
STUDY
Requested by the AIDA committee

European Parliament

Challenges and limits of an open source approach to Artificial Intelligence

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Alexandra THEBEN, Laura GUNDERSON, Laura LÓPEZ-FORÉS, Gianluca MISURACA and Francisco LUPIÁÑEZ-VILLANUEVA.
PE 662.908 - May 2021

EN

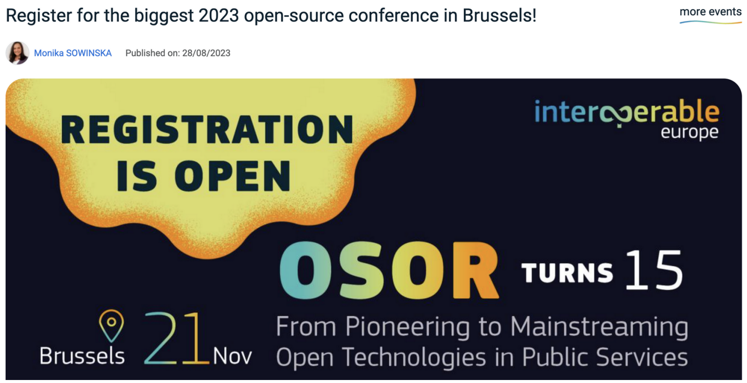


EUROPEAN COMMISSION

Brussels, 21.10.2020
C(2020) 7149 final

COMMUNICATION TO THE COMMISSION

OPEN SOURCE SOFTWARE STRATEGY 2020 – 2023
Think Open

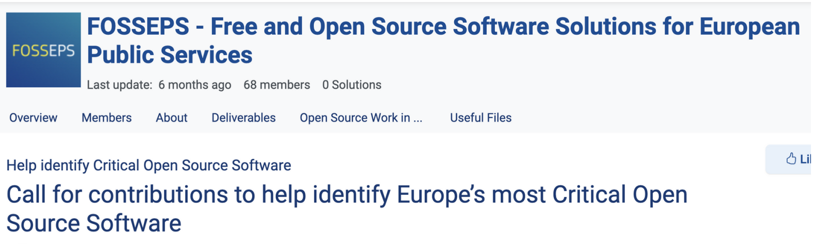


Register for the biggest 2023 open-source conference in Brussels!

more events

Monika SOWINSKA Published on: 28/08/2023

REGISTRATION IS OPEN
interoperable europe
OSOR TURNS 15
Brussels 21 Nov
From Pioneering to Mainstreaming Open Technologies in Public Services

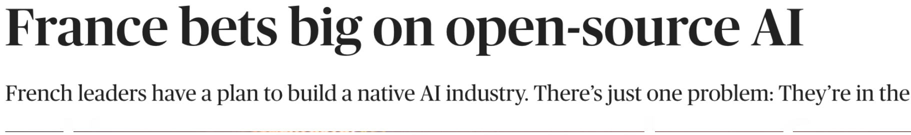


FOSSEPS - Free and Open Source Software Solutions for European Public Services

Last update: 6 months ago 68 members 0 Solutions

Help identify Critical Open Source Software

Call for contributions to help identify Europe's most Critical Open Source Software

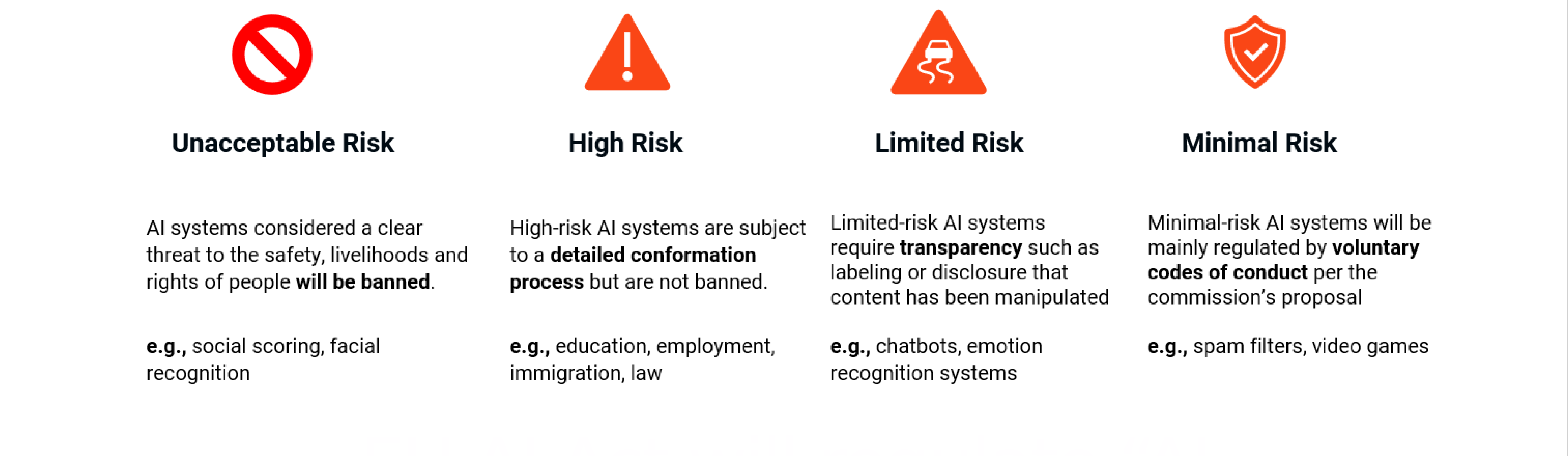


France bets big on open-source AI

French leaders have a plan to build a native AI industry. There's just one problem: They're in the EU.

EU Policy support of open source (AI)

EU AI Act will regulate “AI systems”



Unacceptable Risk

AI systems considered a clear threat to the safety, livelihoods and rights of people **will be banned**.

e.g., social scoring, facial recognition

High Risk

High-risk AI systems are subject to a **detailed conformation process** but are not banned.

e.g., education, employment, immigration, law

Limited Risk

Limited-risk AI systems require **transparency** such as labeling or disclosure that content has been manipulated

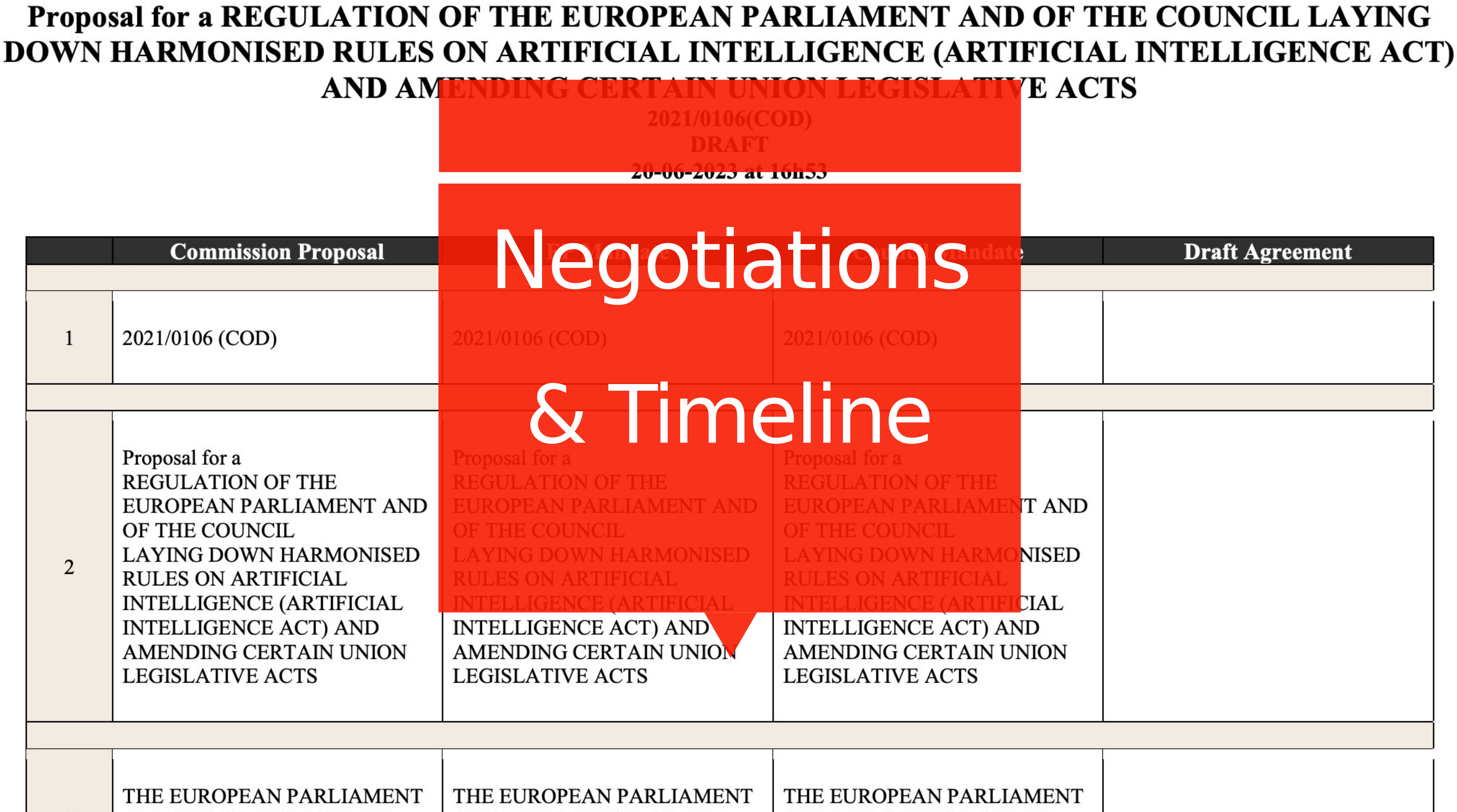
e.g., chatbots, emotion recognition systems

Minimal Risk

Minimal-risk AI systems will be mainly regulated by **voluntary codes of conduct** per the commission’s proposal

e.g., spam filters, video games

Negotiations & Timeline



Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

2021/0106(COD)
DRAFT
20-06-2023 at 16h53

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
1	2021/0106 (COD)	2021/0106 (COD)	2021/0106 (COD)	
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	
	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	

What is an AI system?

Art. 3 – Definition (EP version):

AI system is "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations or decisions that influence physical or virtual environments.”

Scope: EU AI Act applies to…

Providers (natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge):

regardless of their location, when they introduce AI systems to the EU market, international law applies, or the AI system's output is used in the EU.

- when located in the EU, also when they introduce high-risk systems outside the EU, either directly or through a distributor.

Deployers (natural or legal person, public authority, agency or other body using an AI system under its authority, except when used during a personal non-professional activity):

- regardless of their location, when international law applies or when the system's output is used in the EU.
- located within the EU.

Importers (natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union;):

- located in the EU.

Distributors (natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties):

- located in the EU.

Exemption for open source AI components

EU AI Act - Version of the European Parliament:

Recital 12a - Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. **Users are allowed to run, copy, distribute, study, change, and improve software and data, including models by way of free and open-source licenses.** Research by the Commission also shows that free and open-source software can contribute between EUR 65 billion to EUR 95 billion to the European Union’s GDP and that it can provide significant growth opportunities for the European economy. To foster the development and deployment of AI, especially by SMEs, start-ups, academic research, but also by individuals, **this Regulation should not apply to such free and open-source AI components except to the extent that they are placed on the market or put into service by a provider as part of a high-risk AI system or of an AI system that falls under Title II or IV of this Regulation."**

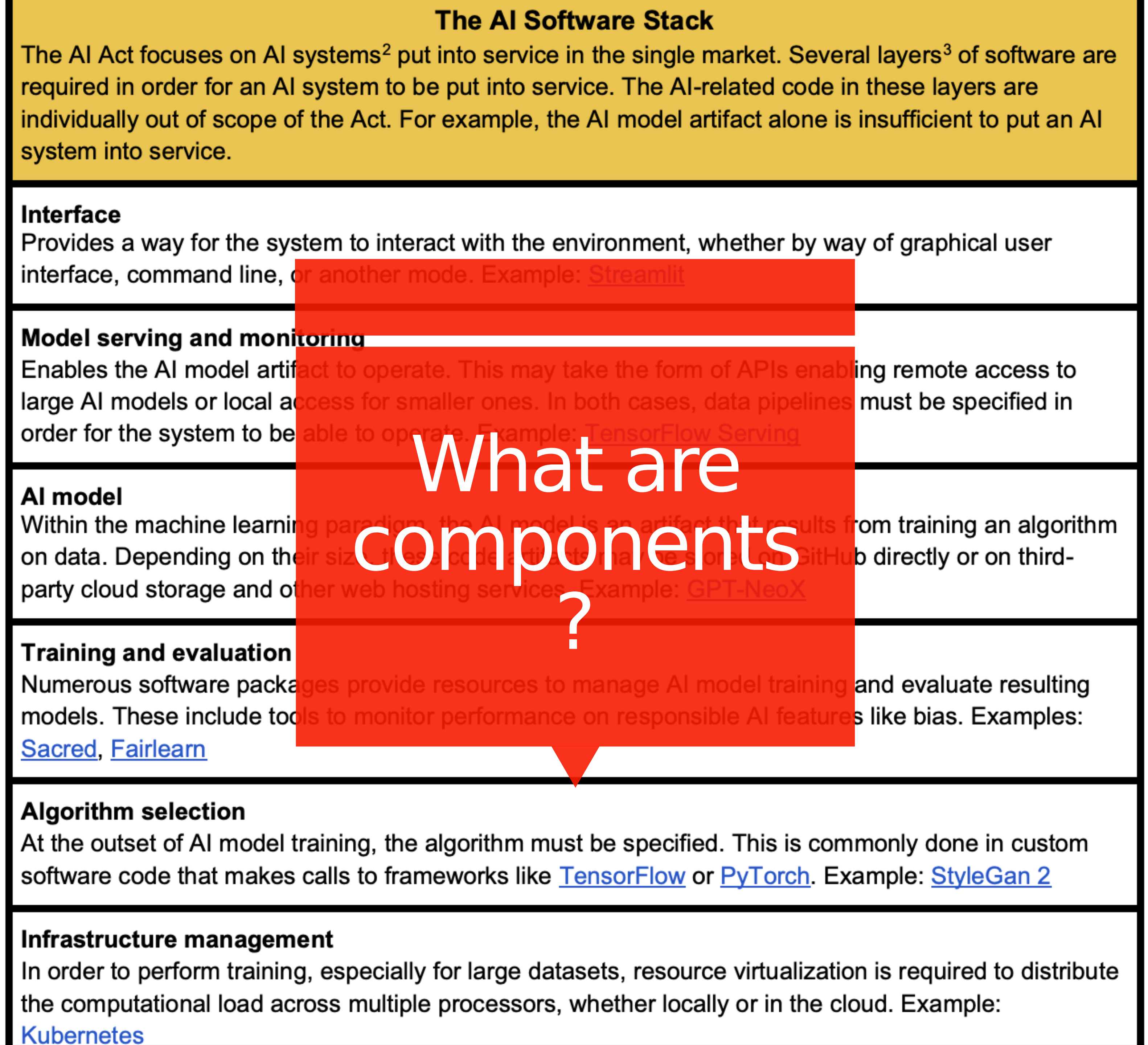
Exemption for open source AI components

Article 5e – “This Regulation shall not apply to AI components provided under free and open-source licences

except to the extent

they are placed on the market or put into service by a provider as part of a high-risk AI system or of an AI system that falls under Title II or IV.

This exemption shall not apply to foundation models as defined in Art 3.”



The AI Software Stack

The AI Act focuses on AI systems[2] put into service in the single market. Several layers[3] of software are required in order for an AI system to be put into service. The AI-related code in these layers are individually out of scope of the Act. For example, the AI model artifact alone is insufficient to put an AI system into service.

Interface
Provides a way for the system to interact with the environment, whether by way of graphical user interface, command line, or another mode. Example: Streamlit

Model serving and monitoring
Enables the AI model artifact to operate. This may take the form of APIs enabling remote access to large AI models or local access for smaller ones. In both cases, data pipelines must be specified in order for the system to be able to operate. Example: TensorFlow Serving

AI model
Within the machine learning paradigm, the AI model is an artifact that results from training an algorithm on data. Depending on their size, these code artifacts may be stored on GitHub directly or on third-party cloud storage and other web hosting services. Example: GPT-NeoX

Training and evaluation
Numerous software packages provide resources to manage AI model training and evaluate resulting models. These include tools to monitor performance on responsible AI features like bias. Examples: Sacred, Fairlearn

Algorithm selection
At the outset of AI model training, the algorithm must be specified. This is commonly done in custom software code that makes calls to frameworks like TensorFlow or PyTorch. Example: StyleGan 2

Infrastructure management
In order to perform training, especially for large datasets, resource virtualization is required to distribute the computational load across multiple processors, whether locally or in the cloud. Example: Kubernetes

What are components ?

Components of AI systems:

1. **Model**
2. **Deployment Software**
3. **Training Dataset**
4. **Training Algorithm**
5. **Code Used for Training**
6. **Evaluation Datasets**

This complexity of AI systems distinguishes them from traditional software systems which typically refers to access to source code.

In scope: Commercial use of open source AI components

Circumstances for open source turning commercial

Recital 12b - **Neither the collaborative development of free and open-source AI components nor making them available on open repositories should constitute a placing on the market or putting into service. A commercial activity, within the understanding of making available on the market, might, however, be characterized by <u>charging a price</u>**, with the exception of transactions between micro-enterprises,

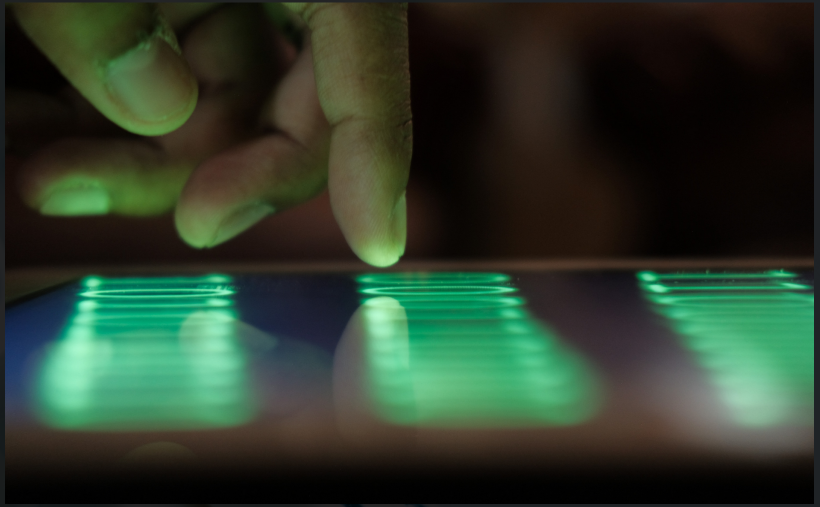
- **for a free and open-source AI component but also**
- by charging a price for **technical support services,**
- **by providing a software platform through which the provider monetizes other services,** or
- **by the use of personal data for reasons other** than exclusively for **improving the security, compatibility, or interoperability** of the software."

Exception for open source developers

No obligations for developers

Recital 12c - **The developers of free and open-source AI components should not be mandated under this Regulation to comply with requirements targeting the AI value chain and, in particular, not towards the provider that has used that free and open-source AI component.** Developers of free and open-source AI components should, however, be encouraged to implement widely adopted documentation practices, such as model and data cards, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union.

Examples of other EU-open source exceptions



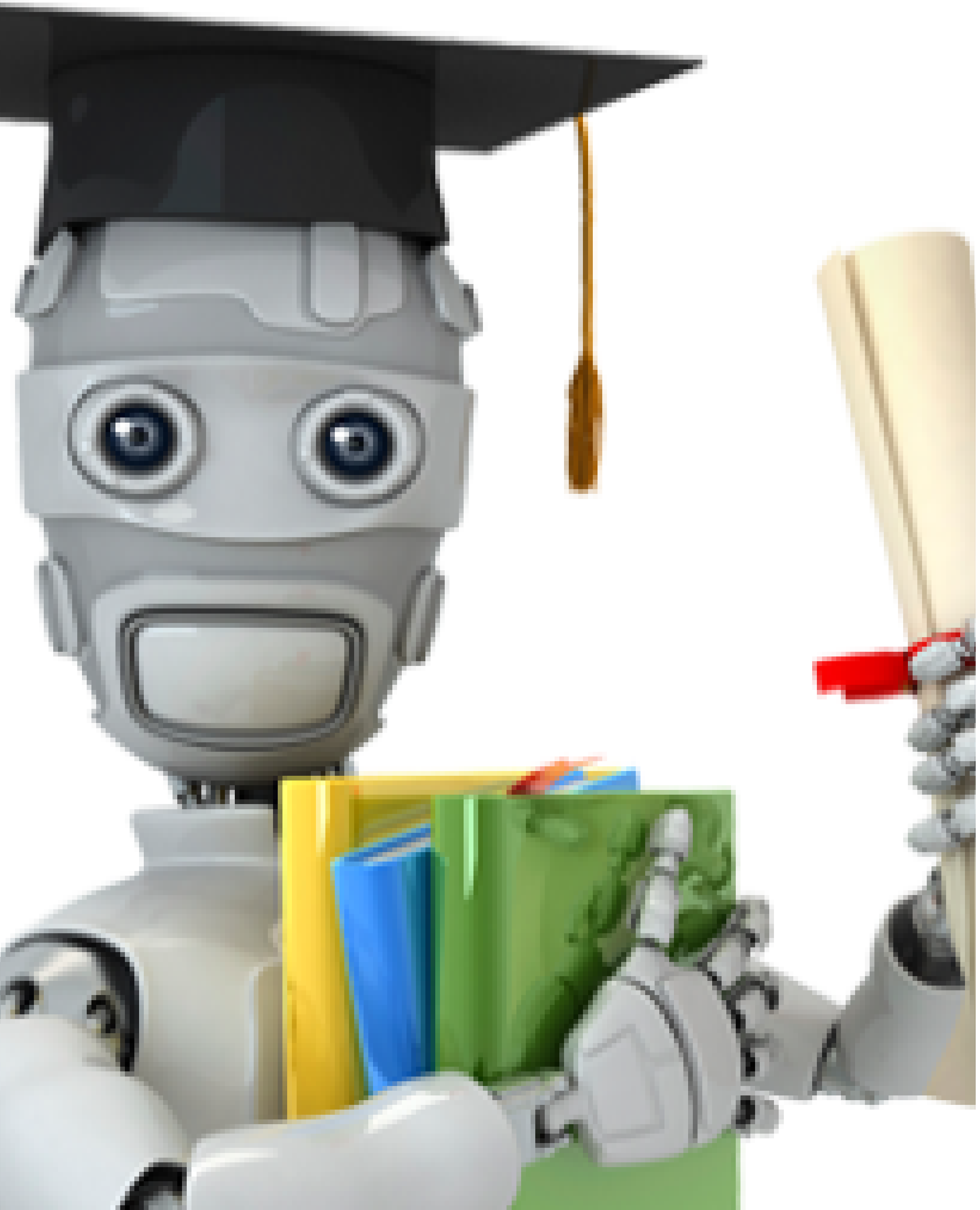
2019 Copyright Directive:

- Acknowledged the importance of protecting open source platforms, with provisions addressing content filtering considerations.

Draft Cyber Resilience Act (2022) &

Draft Product Liability Directive (2022):

- Propose exemptions for open source.

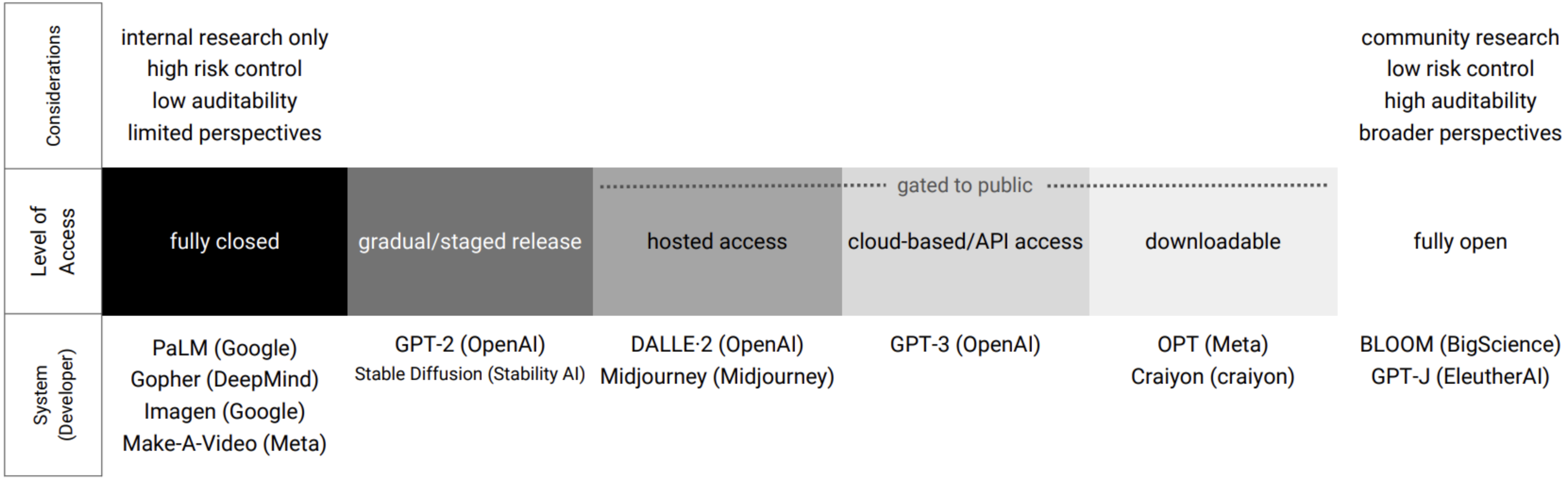


Many open foundation models

Pre-trained models can reduce costs, environmental impact, and data needs.

There are hundreds of open pre-trained models, many of which align with the AI Act's definition of foundation models.

They vary in language, training data, capabilities, and adaptability to different applications.



Considerations	internal research only high risk control low auditability limited perspectives					community research low risk control high auditability broader perspectives
			gated to public			
Level of Access	fully closed	gradual/staged release	hosted access	cloud-based/API access	downloadable	fully open
System (Developer)	PaLM (Google) Gopher (DeepMind) Imagen (Google) Make-A-Video (Meta)	GPT-2 (OpenAI) Stable Diffusion (Stability AI)	DALLE·2 (OpenAI) Midjourney (Midjourney)	GPT-3 (OpenAI)	OPT (Meta) Craiyon (craiyon)	BLOOM (BigScience) GPT-J (EleutherAI)

The Gradient of Generative AI Release: Methods and Considerations Irene Solaiman, Hugging Face, Feb. 2023, arXiv:2302.04844v1 [cs.CY])

Categorization of (open source) foundation models

Foundation models in the EU AI Act

Art. 2(5e) excludes foundation models from the open source exemption:

“This exemption shall not apply to foundation models as defined in Art 3”

Art. 3 (1c) ‘foundation model’ means an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;

Requirements for Foundation Models

Art. 28b: Obligations of Foundation Model Providers

1. **Providers of foundation models must ensure compliance with the requirements** outlined in this article before making them available on the market or putting them into service. **This applies** whether the foundation model is provided as a standalone model, embedded in an AI system or product, **distributed under free and open source licenses**, offered as a service, or through other distribution channels.

Requirements for Foundation Models

Obligations on foundation models in Article 28b(2) include:

- Ensure identification, reduction, and **mitigation of foreseeable risks** through **design, testing, and analysis**.
- Apply **data governance** to assess data sources, biases, and mitigation.
- Engage **independent experts, document analysis, and test** for performance, safety, and more.
- Include **energy/resource measurement** and environmental impact in design.
- Create comprehensive **technical documentation** for downstream compliance.
- Implement a **quality management system** to ensure Article 28 compliance.
- **Register** the model in the EU high-risk AI

Foundation Models: compliant?

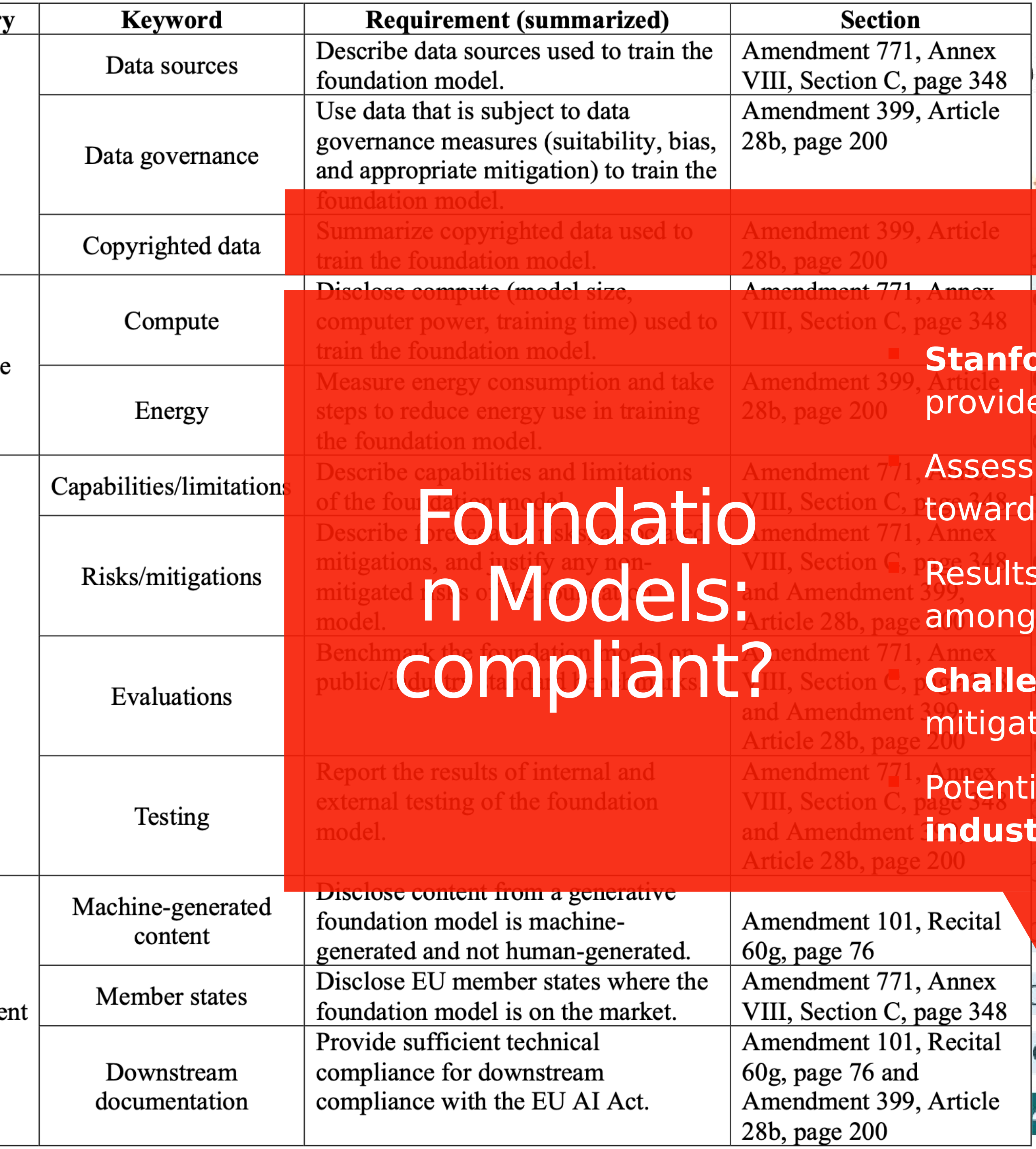
Stanford Study: Evaluation of foundation model providers' compliance with EU AI Act (EP draft).

Assessment of 12 critical requirements directed towards foundation model providers.

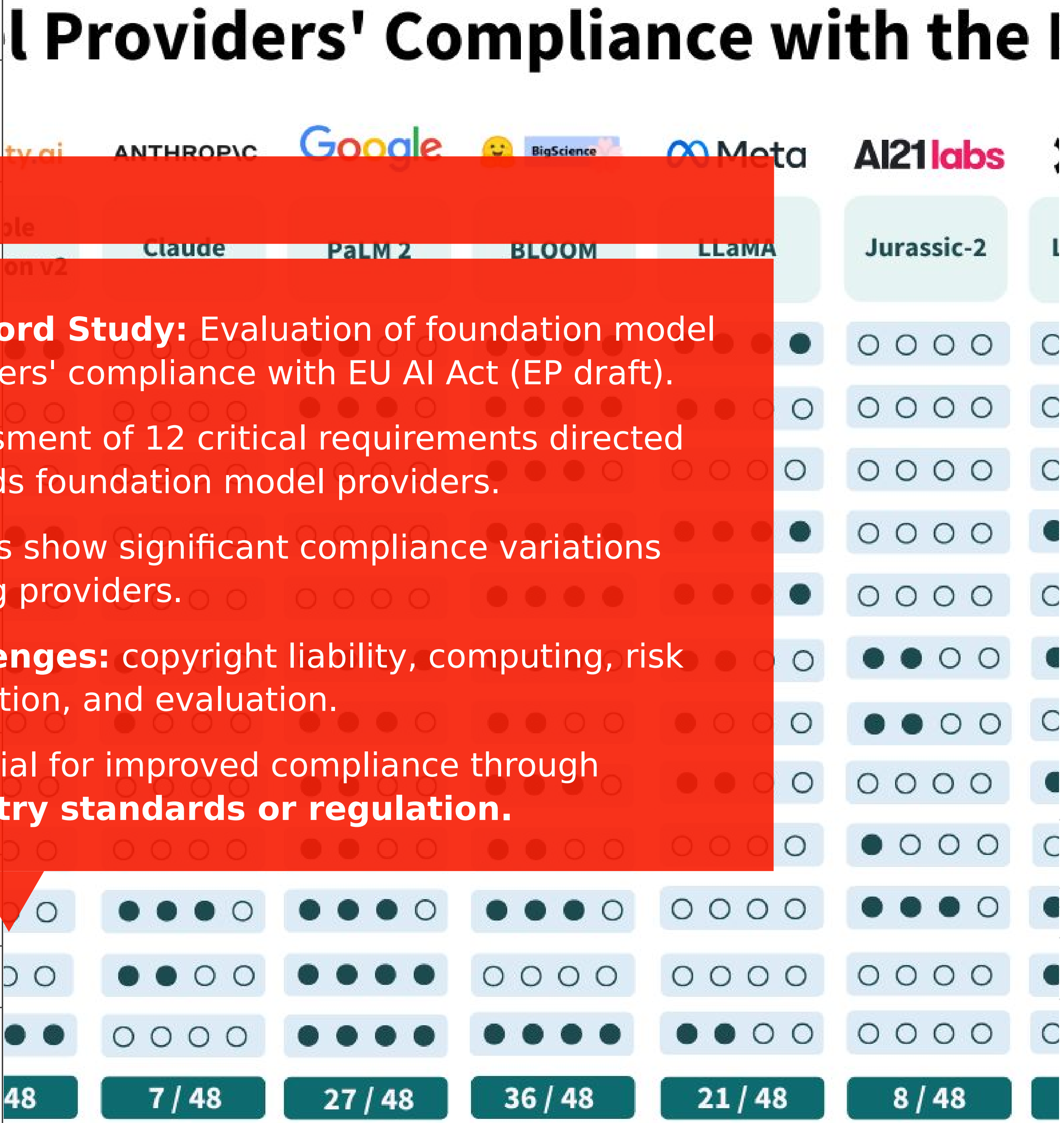
Results show significant compliance variations among providers.

Challenges: copyright liability, computing, risk mitigation, and evaluation.

Potential for improved compliance through **industry standards or regulation.**



ry	Keyword	Requirement (summarized)	Section
	Data sources	Describe data sources used to train the foundation model.	Amendment 771, Annex VIII, Section C, page 348
	Data governance	Use data that is subject to data governance measures (suitability, bias, and appropriate mitigation) to train the foundation model.	Amendment 399, Article 28b, page 200
	Copyrighted data	Summarize copyrighted data used to train the foundation model.	Amendment 399, Article 28b, page 200
e	Compute	Disclose compute (model size, computer power, training time) used to train the foundation model.	Amendment 771, Annex VIII, Section C, page 348
	Energy	Measure energy consumption and take steps to reduce energy use in training the foundation model.	Amendment 399, Article 28b, page 200
	Capabilities/limitations	Describe capabilities and limitations of the foundation model.	Amendment 771, Annex VIII, Section C, page 348
	Risks/mitigations	Describe foreseeable risks, associated mitigations, and justify any non-mitigated risks of the foundation model.	Amendment 771, Annex VIII, Section C, page 348 and Amendment 399, Article 28b, page 200
	Evaluations	Benchmark the foundation model on public/industry standard benchmarks.	Amendment 771, Annex VIII, Section C, page 348 and Amendment 399, Article 28b, page 200
	Testing	Report the results of internal and external testing of the foundation model.	Amendment 771, Annex VIII, Section C, page 348 and Amendment 399, Article 28b, page 200
	Machine-generated content	Disclose content from a generative foundation model is machine-generated and not human-generated.	Amendment 101, Recital 60g, page 76
ent	Member states	Disclose EU member states where the foundation model is on the market.	Amendment 771, Annex VIII, Section C, page 348
	Downstream documentation	Provide sufficient technical compliance for downstream compliance with the EU AI Act.	Amendment 101, Recital 60g, page 76 and Amendment 399, Article 28b, page 200



Concerns with AI Act Article 28b

Broad Scope Critique: Article 28b criticized as overly broad.

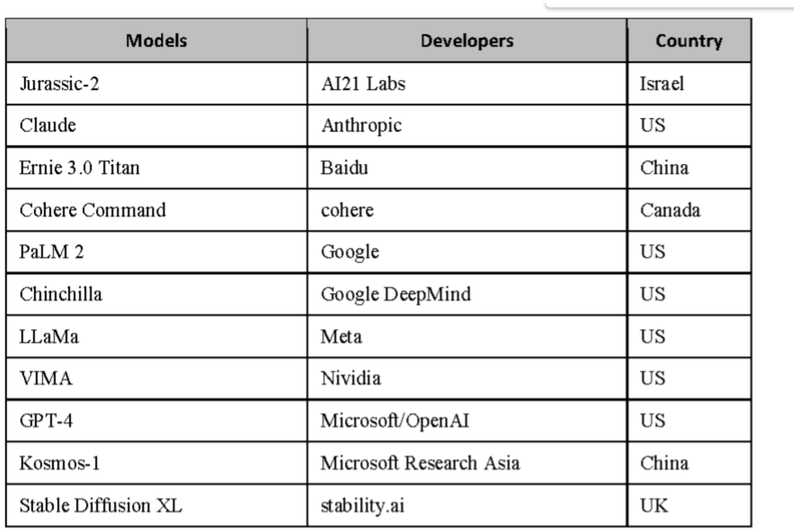
Market Dominance: Uniform obligations may favor major companies.

Supporting Innovation: Emphasize preserving innovation for smaller entities.

Lack of Clarity: Article 28b lacks detail, relying on standards and guidelines.

DSA Inspiration: Consider modeling after Digital Services Act (DSA) Article 33(4).

Balancing Innovation: Criteria can assess model importance while fostering innovation.



Models	Developers	Country
Jurassic-2	AI21 Labs	Israel
Claude	Anthropic	US
Ernie 3.0 Titan	Baidu	China
Cohere Command	cohere	Canada
PaLM 2	Google	US
Chinchilla	Google DeepMind	US
LLaMa	Meta	US
VIMA	Nividia	US
GPT-4	Microsoft/OpenAI	US
Kosmos-1	Microsoft Research Asia	China
Stable Diffusion XL	stability.ai	UK

Table 2: Foundation models

The non-exhaustive Table 2 indicates what a list of systemic foundation models could be if the European Commission, in close cooperation with the AI Office, would have assessed the status quo in June 2023.

Preparing for Upcoming AI Regulations

- **Anticipate Regulation**: Prepare for forthcoming AI regulations affecting the entire ecosystem.
- **Shift Left Approach**: Implement privacy, security, ethics, and responsibility by design.
- **Strengthen Documentation**: Enhance transparency and accountability through comprehensive documentation.
- **Model Cards**: Utilize Model Cards to communicate AI model details and ethical considerations.

Preparing for regulations and emphasizing responsible AI practices supports compliance and trust in open source AI projects.

Thank you!

Home

About

Resources

Services

Contact / Calendar

Katharina Koerner

Privacy and Responsible AI.
Connecting people and ideas.

Visit My Website & Follow Me:

katharinakoerner.us

https://www.linkedin.com/in/katharina-koerner-privacyengineering

@KatharinaKoern1