BigTech’s Efforts to Derail the AI Act

VB verfassungsblog.de/bigtechs-efforts-to-derail-the-ai-act/

Jascha Bareis
05 Dezember 2023

What is happening at the regulatory finish line?

Things have been quite hectic on the European Union’s floors lately. The Artificial Intelligence Act (AI Act), the ambitious European AI regulatory proposal that was proposed by the European Commission in April 2021, is reaching the finish line.

The trilogue between Commission, Parliament and Council is supposed to finalize the AI Act by 6 December, before the European Parliament will be dissolved for next year’s parliamentary elections. But the AIA negotiations “hit the brakes” on a deadlock on 10 November in the trilogue: Germany, France and Italy, Europe’s most powerful economies and political heavyweights, refused to put so-called foundation models under tighter regulation. The EU Parliament and the Spanish presidency had proposed a tiered approach to introduce a stricter regime for “high-impact” foundation models, including risk mitigation reviews such as pre-deployment red-teaming (i.e., testing how resilient a model is to security bypasses, and manipulation of functionality) and post-deployment auditing (i.e., an external review of the model and dataset to see if there are biases or other security concerns). Under pressure from big European AI companies such as Aleph Alpha and Mistral, which develop such foundation models, Germany, France and Italy teamed up and published an agreement in which they declared that restrictive regulation shall be lowered to “mandatory self-regulation through codes of conduct”.

The proposition basically means nothing more than the declaration of some lofty ethical principles, with no external check on whether they are actually implemented, or any sanctioning mechanism if they are not. The outcry against such regulation-washing was immediate. AI experts published and sent a letter of concern to the German government on 28 November, warning that “if coverage of foundation models is dropped, a weakened or failed AI Act would be regarded as a historic failure.“

What are foundation models and why should we care?

Why all the fuss about foundation models? As the term implies, foundation refers to a process of *homogenisation* and *generalization* of AI models that serve as the main building block for more specialized AI applications. Article 3(1)(1)(c) of the most recent AI Act

proposal of the European Parliament states: “‘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.” Foundation models represent a recent paradigm shift in AI (Bommasani et al), particularly in speech and image processing, where they drive state-of-the-art models that drive popular programs such as ChatGPT, Bard, or DALL-E. The following characteristics (ibid: pp.4) pinpoint what makes them foundational:

Transfer learning: Foundation models allow to take the ““knowledge” learned from one task (e.g., object recognition in images) and apply it to another task (e.g., activity recognition in videos)” (see illustration).

Performance: Recent improvements in hardware performance and model architecture enable unprecedented powerful data processing capabilities (“GPU throughput and memory have increased 10x over the last four years”).

Scale: Access to an immense amount of data has made it possible to train models for greater statistical accuracy and robustness.

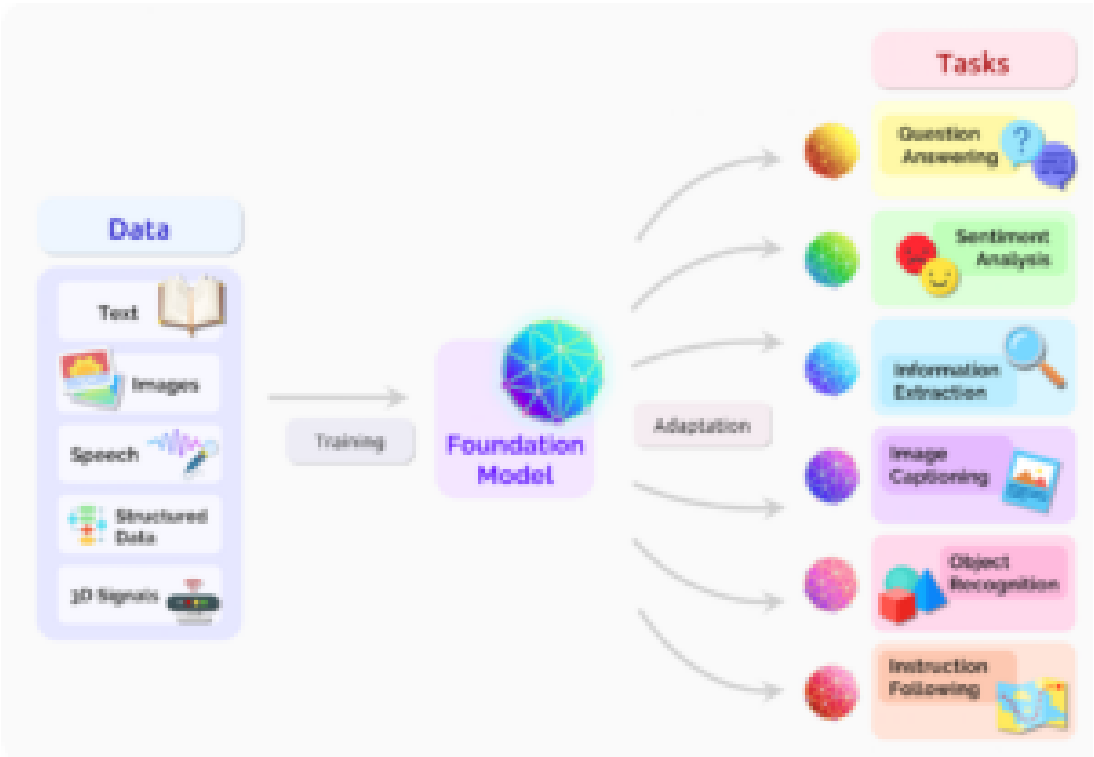

Diagram from https://arxiv.org/abs/2108.07258

In the current data and AI economy, very few powerful companies own the infrastructure necessary to develop foundation models. Only deep-pocketed tech companies can build so many server farms and high-performance CPUs, attract the best computer scientists around

the world and, above all, access the massive amounts of data needed to train such models. Hence, AI development worldwide is increasingly reliant on highly centralized and resource-intensive infrastructure controlled by private tech giants.

Especially BigTech companies from the US, such as Meta and Alphabet, and from Europe, such as Aleph Alpha and Mistral – companies that hold the necessary infrastructure – are so determined to water down the current paragraph on foundation models in the AI Act. It is precisely the transferability and adaptability of these models to perform tasks in all social domains – ranging from healthcare (visual cancer detection), education (large-language-model writing tools) to social scoring (risk assessment for credit or social aid) – that makes their strict regulation so pivotal. Without thorough assessment, potential security gaps, performance issues or discriminatory biases can be disseminated and scaled widely into other AI applications. The German, French and Italian proposal shifts all compliance and liability costs from the shoulders of the biggest AI companies to the thousands of downstream users, public agencies and small-and-medium enterprises that adapt and deploy them.

BigTech's systematic deregulatory narratives

The show-down regarding foundation models in Brussels is one more chapter in the unprecedented lobbying efforts of the private sector on EU AI regulation. Reports by the 'Corporate Europe Observatory' (CEO) and 'Transparency International' show how BigTech, corporate think tanks, and trade and business associations are active in blocking and watering down AI regulation in Brussels. BigTech, largely dominated by US firms, have "spen[t] over € 97 million annually lobbying the EU institutions […] ahead of pharma, fossil fuels, finance, or chemicals" (CEO, 2021: 6). This goes hand in hand with great access to the top European floors. Industry lobbyists had by far the most meetings with the EU Commission for the Digital Service Act and Digital Markets Act negotiations (192 out of 271 meetings) and are most active in agenda and standard setting. Since the beginning of the negotiations around the AI Act, "tech companies have reduced safety obligations, sidelined human rights and anti-discrimination concerns" (CEO, 2023: 3).

The fact that final EU policy decisions are now taken in the trilogue behind closed doors, without any public transparency, favors the powerful BigTech lobbies, "as secrecy means that only the well-resourced well-connected lobbying actors can follow and intervene in trilogues, and excludes citizens from crucial discussions that will have an impact on their lives." Most politicians and Big Tech lobbyists greet each other through revolving doors anyway, as "three quarters [!] of all Google and Meta's EU lobbyists have formerly worked for a governmental body at the EU or member state level" (CEO, 2023: 7).

Money and access allow BigTech lobbyists and company leaders to stage key *narratives* that attempt to push policy makers towards a deregulatory agenda. What do they tell ministers at dinners and canapés floor meetings? Revealed documents by lobby control initiatives allow

to deduce a pattern.

“Being irreplaceable and indispensable”

Notions of ‘break-through’ and ‘revolution’ are well-used metaphors in order to create a sense of urgency and menacing opportunity costs around AI development. The outcry and hype around Chat-GPT earlier this year was a prime example of how key figures in BigTech adopted an alarmist and messianic narrative of social disruption to pressure regulators. The lobbying narrative of BigTech’s “irreplaceability” when it comes to problem solving narrows down societal perceptions and alternative pathways. It represents a techno-solutionist (Morozov) dogma that tries to reframe social problems as technical ones. Then the question discussed is only *how* to implement or *fix* AI systems, hence, narrowing down tech as the only problem solving repertoire. This strategy relinquishes democratic zones of contestation (Powles and Nissenbaum), namely, the vast problem-solving possibilities that do not rely on AI at all. It is well studied in political communication (Bareis&Katzenbach) how governments around the world have embraced these tech-narratives instead of acting as sober watchdogs.

This dependency, so far, is a myth, because at the moment none of BigTech’s inventions deserves the naming of a social ‘revolution’. Chat-GPT and social media are tools and platforms which, indeed, do influence our everyday lives, but society is definitely not dependent on them. But with more public administrations letting BigTech build central infrastructure and adopt their models, this dependency grows. “[T]hese companies control the tooling, development environments, languages, and software that define the AI research process – they make the water in which AI research swims“ (Whittaker). From this perspective it is imperative to regulate foundational models and not let them off public control.

“Fear international competition”

The narrative of being indispensable for societal well-being is amplified by situating European economies in a fierce arena of international competition. The greatest threat staged by US tech figures aligned with the American government is a technology race against China, harnessed within a positioning of capitalist and geopolitical striving. The motive here is to create a powerful rhetorical triangle, staging “an interdependent connection between technology advancement, economic performance, and the resilience capabilities of a society”.

However, it remains questionable why the EU would want to compete with a Chinese business model that embodies exactly what the EU’s fundamental rights approach and risk-based AI regulatory framework is supposedly designed to prevent. Why would the EU want to compete with an authoritarian regime that uses data and the latest AI models to surveil and control its society, with social media companies like TikTok engaging in shadow banning

to filter out ‚critical' content? Even the US government has reversed its previous deregulatory stance on AI and just issued (30 October) an executive order on AI regulation that explicitly targets foundation models with mandatory federal notification of "all red-team safety tests".

"Self-regulation through mandatory codes of conduct"

The mandatory self-regulatory proposal by Germany, France and Italy caters to the public accountability narrative BigTech has been trying to install in public. For years stakeholders in the field have been outdoing each other with claims to ethical AI and codes of conduct to ensure a socially desirable implementation of AI (Jobin et al). The publication of ethical guidelines in the private and public realm has become so plentiful (and repetitive) that it has reached a scale that is hard to keep track of. Self-declared corporate ethical principles attempt to install a corporate image of public responsibility and care. Essentially, though, it has proven to be a strategy for escaping legal regulation (Wagner). How shall a rule be mandatory, after all, if there is no enforcement or sanction mechanism?

Will the EU exempt BigTech from accountability and liability?

Watering down the AI Act in its final stages of negotiation would be detrimental to the public image of the AI Act as well as its EU regulatory bodies. Certainly, the AI Act already has its caveats (Guijarro), but to exclude foundation models from regulation would be the fundamental blow.

Foundation AI models are high-risk models and need to be regulated before they enter society. Given that in the past years, BigTech only took responsibility for hate speech after being regulated, there is little hope that it will be any different with foundation models. So far BigTech has been caring little about societal polarization, disinformation on its platforms, about the ecological footprint or dual use of its inventions – or paying their fair share of taxes.

It is again unacceptable that citizens are treated as a public laboratory while the wealthiest and biggest tech players are exempted from accountability and liability. The AIA must include foundation models to be a regulation worthy of its name.

SUGGESTED CITATION Bareis, Jascha: *BigTech's Efforts to Derail the AI Act, VerfBlog,* 2023/12/05, https://verfassungsblog.de/bigtechs-efforts-to-derail-the-ai-act/, DOI: 10.59704/265f1afff8b3d2df.
LICENSED UNDER CC BY SA