Addressing Open Source Software (OSS) in the EU’s AI Act

OSS provides critical benefits to society. While it can be used in ways that contribute to risks covered by the AI Act, the creation of OSS itself should be treated distinctly from the offering of ongoing services, including commercial services. Otherwise, the AI Act risks stalling development of OSS in ways that will harm European innovation, competition as well as fairness and safety.

Open Source Software (OSS) provides critical benefits to Europe.

OSS is critical to software development – one study in 2022 found that up to 98% of codebases contain at least some OSS, and provide fundamental, if often less visible, functions. OSS thrives because users can not only run the software but also copy, study, modify, improve, and redistribute it. As such, it can be rapidly improved and built upon, driving innovation forward and releasing creativity.

Because Europe has been a leader in this area, it has gained significant economic benefits. The European Commission has previously conducted research demonstrating OSS contributes between €65 billion to €95 billion to the European Union’s GDP and that it provides significant growth opportunities for the European economy. Similarly, a study of France’s procurement policies point to an increase in tech start-ups and jobs.

In the context of AI, OSS can help ensure that the marketplace is more competitive, fairer, and safer.

Across its digital strategy, the Commission has rightly focused on market concentration and barriers to competition in the tech sector (such as through the Digital Markets Act), as well as legislating to stop ways in which online services may enable illegal activity or other harms to society including violation of fundamental rights (such as through the Digital Services Act).

As AI becomes ever more important to online services, the development of OSS tools is crucial to meeting the objectives of increased competition, fairness and safety. OSS ensures that the power to deploy AI is not merely concentrated in a few large, commercial actors but decentralized and interoperable for the benefit of all users large or small, commercial or not-for-profit, and ultimately society at large. Moreover, openness can facilitate safety through transparency – allowing people to understand on what basis AI models were trained and how they operate and contribute to shedding light on AI’s “black box.”

Developers who simply create and collaborate on open source projects are distinct from entities that make software available as part of an ongoing service, including commercial operations, and the AI Act should recognize these distinctions.

The OSS ecosystem is diverse. Projects may be maintained by individual developers, communities, nonprofits, companies, or other entities, and regardless of the project structure, many different types of entities may contribute to the code’s evolution.
In many cases, OSS is not offered as part of an ongoing service, let alone as part of a commercial proposition. Instead, it is uploaded to a code repository, like Github or Hugging Face, and then made available for others to collaborate on. Code that is merely uploaded is not in and of itself high-risk, as it has not been deployed for any particular use or purpose. Moreover, the developers do not have an (ongoing) relationship with downstream users, so they are not positioned to manage and control how their code is used across the “supply” or “value chain.”

For instance, EleutherAI is a nonprofit research institute that grew from a chat discussion into developing cutting-edge AI tools. It grew out of and continues to operate from a single Discord chat group, driving collaboration among employees, volunteers, and other institutions. Its tools are geared to enhance the interpretability and alignment of these tools with positive, public-interest objectives.

Similarly, Hugging Face is a platform that hosts many different open source models and datasets for AI. The site is committed to supporting open, ethical AI usage through open tools. While it is a commercial service developed by three French entrepreneurs, its many users run the gamut from companies to individual developers and hobbyists, and they are used by all sorts of entities.

Such examples demonstrate the power of OSS to challenge software and other tech industry gatekeepers to achieve a fairer, healthier, and more competitive innovation market.

To the extent people who merely upload OSS to an open repository or collaborate on its development may be implicated by the AI Act, their responsibilities should be proportionate and limited to sharing information with downstream users, who may further deploy AI for regulated purposes, including in areas such as high risk uses.

OSS providers should not be covered by the Act, unless their software is made available as part of an ongoing commercial service or when a provider puts it into service as part of a high-risk or banned use under the Act, as well as uses facing enhanced transparency requirements under Title IV. In other words, the obligations under the AI Act should not apply to entities that merely develop and upload OSS packages.

To the extent they are covered, the Act should take a proportionate approach, ensuring developers make information available to downstream users in support of their compliance, but otherwise not regulating open-source software or creating the expectation that open-source developers can control or be responsible/liable for downstream use. Chilling effects on OSS development would far outweigh any benefits of restricting such development.

While some have expressed concern that this approach will allow companies to evade the requirements of the AI Act, we do not share this assessment. After all, if a company puts an open source package into a service they are offering to users that is regulated by the Act, then that company would still come under the AI Act’s scope. We should not conflate OSS with the services, uses or purposes to which OSS is put. By overregulating OSS as currently proposed in the AI Act, we risk dealing a severe blow to an essential engine of public-interest technology development with myriad positive social benefits for EU citizens.