Regulating AI will put companies and governments at loggerheads

AI developers and lawmakers would benefit from a deeper understanding of each other

yesterday

AI developer Geoffrey Hinton has announced his resignation from Google, saying he regretted his work © Masahiro Sugimoto/The Yomiuri Shimbun/Reuters

The writer is international policy director at Stanford University's Cyber Policy Center and serves as special adviser to Margrethe Vestager

The rapid release of generative AI tools has been a moment of reckoning. Just this week Geoffrey Hinton, a celebrated developer of AI, announced his resignation from Google, saying he regretted his work and wants to speak freely about the dangers and risks of the technology he created.

Elon Musk, in typical contrarian fashion, has both warned that AI can destroy civilisation and created an AI company. He previously invested in OpenAI, the company behind generative AI tools such as GPT-4.

Musk joined AI experts and some industry leaders calling for a six-month pause in the development of generative AI, while urging policymakers to get rules in place, presumably within that timeframe. Clearly they have never experienced a democratic legislative process. Getting an AI law adopted and implemented, let alone setting up a new regulatory body, will take years.

Others suggest questioning AI executives under oath to compile a record of security issues they have encountered. But previous hearings with Meta's Mark Zuckerberg or Google's Sundar Pichai left no mark on the social media and search giants' business models, and no laws to restrict their powers were imposed.

Suddenly, everyone wants to regulate AI. Open letters have been written and legislative proposals discussed. Unfortunately, the mismatches between the characteristics of AI and the solutions offered betray a deep misunderstanding between the people developing and selling AI and those making policy and voting on new laws.

Politicians the world over have grasped that they must do something fast. They are now racing to set new rules. In a rare moment of political alignment, Republicans and Democrats, the Chinese and European governments are all hoping to curb the threats from AI (albeit for their own political reasons). The EU has advanced furthest in outlining what the guardrails should look like. The EU's AI Act mostly looks at how AI, once deployed, might create risks in access to employment, education or human rights. Yet EU officials concede this focus on the applications of AI omits generative AI, or AI as a technology. The next set of breakthroughs will make today's synthetic media look primitive. We may not know what is coming next, but we do know that new technologies will keep emerging. Regulations adopted today will also have to address future iterations.

That is a challenge that needs to be solved and will require the

innovation of policy itself. (It would be great if AI developers updated their understanding of the rule of law, but I have learnt to lower my expectations there.) What excites engineers worries regulators. The risks of AI systems lie not only in their specific applications, but also in the question of who has agency over them at all. At the moment, companies run the show and that is a danger to democracy.

Any successful AI regulation must tackle three areas. First, the power dynamics between AI developers and the rest of society need rebalancing. This asymmetry is already so significant that only the biggest tech companies can develop AI, both because of access to data sets and the ability to train and process them. Even a wealthy university such as Stanford, which trains top AI engineers, does not have the data or computing power of its neighbouring Silicon Valley companies. As a result, the secrets of AI's inner workings — which have enormous societal impact — remain locked in corporate systems.

The second problem is access to information. There must be public interest safeguards to allow lawmakers to see the inner workings of AI. There is no public understanding of the algorithms governing apps which affect society. That in turn hinders fact-based discussion, focused public policy and necessary accountability mechanisms.

And third, we cannot ignore the ever-changing nature of AI. Regulation needs to be flexible and firmly enforceable. This could include keeping logs so that when settings are adjusted, the impacts can be recorded.

While there is political will to regulate AI, the path forward is difficult. Both AI experts and lawmakers would benefit from a deeper understanding of the other: computer scientists should understand their impact on democracy and regulators should dive deeper into how AI works. The gap between them will further hinder the development of regulations that match the power of AI — and that mismatch creates risks all of its own.