# The EU is leading the way on AI laws. The US is still playing catch-up

Publication Date: 2023-06-13

Author: Johana Bhuiyan

Section: Technology

Tags: Artificial intelligence (AI), US Senate, US Congress, Computing, features

Article URL: https://www.theguardian.com/technology/2023/jun/13/artificial-intelligence-us-regulation

Last month, Sam Altman, the CEO of OpenAI and face of the artificial intelligence boom, sat in front of members of Congress urging them to regulate artificial intelligence (AI). As lawmakers on the Senate judiciary subcommittee asked the 38-year-old tech mogul about the nature of his business, Altman argued that the AI industry could be dangerous and that the government needs to step in. “I think if this technology goes wrong, it can go quite wrong,” Altman said. “We want to be vocal about that.” How governments should regulate artificial intelligence is a topic of increasing urgency in countries around the world, as advancements reach the general public and threaten to upend entire industries. The European Union has been working on regulation around the issue for a while. But in the US, the regulatory process is just getting started. American lawmakers’ initial moves, several digital rights experts said, did not inspire much confidence. Many of the senators appeared to accept the AI industry’s ambitious predictions as fact and trust its leaders to act in good faith. “This is your chance, folks, to tell us how to get this right,” Senator John Kennedy said. “Talk in plain English and tell us what rules to implement.” And much of the discussion about artificial intelligence has revolved around futuristic concerns about the technology becoming sentient and turning against humanity, rather than the impact AI is already having: increasing surveillance, intensifying discrimination, weakening labor rights and creating mass misinformation. If lawmakers and government agencies repeat the same mistakes they did while attempting to regulate social media platforms, experts warn, the AI industry will become similarly entrenched in society with potentially even more disastrous consequences. “The companies that are leading the charge in the rapid development of [AI] systems are the same tech companies that have been called before Congress for antitrust violations, for violations of existing law or informational harms over the past decade,” said Sarah Myers West, the managing director of the AI Now Institute, a research organization studying the societal impacts of the technology. “They’re essentially being given a path to experiment in the wild with systems that we already know are capable of causing widespread harm to the public.” AI fervor and attempts to regulate it In response to mass public excitement about various AI tools including ChatGPT and DALL-E, tech companies have rapidly ramped up the development or, at least, plans to develop AI tools to incorporate into their products. AI is the buzzword of the quarter, with industry executives hoping investors take notice of the mentions of AI they’ve weaved throughout their most recent quarterly earnings reports. The players who have long worked in AI-adjacent spaces are reaping the benefits of the boom: chipmaker Nvidia, for instance, is now a trillion-dollar company. The White House and the federal government have announced various measures to address the fervor, hoping to make the most of it while avoiding the free-for-all that led to the last decade of social media reckoning. It has issued executive orders asking agencies to implement artificial intelligence in their systems “in a manner that advances equity", invested $140m into AI research institutes, released a blueprint for an AI bill of rights, and is seeking public comment about how best to regulate the ways in which AI is used. Federal efforts to address AI have so far largely resulted in additional funding to develop "ethical" AI, according to Ben Winters, a senior counsel at the Electronic Privacy Information Center, a privacy research nonprofit. The only "regulation-adjacent" guidelines have come through executive orders which Winters says "aren't even really meaningful". "We don't even have a clear picture that any of the 'regulation' of AI is going to be actual regulation rather than just support [of the technology]," he said. In Congress, lawmakers appear at times to be just learning what it is they're hoping to regulate. In a letter sent on 6 June, Senator Chuck Schumer and several other lawmakers invited their colleagues to three meetings to discuss the "extraordinary potential, and risks, AI presents". The first session focuses on the question "What is AI?" Another is on how to maintain American leadership in AI. The final, classified session will discuss how US national security agencies and the US's "adversaries" use the technology. The lack of leadership on the issue in Washington is leaving the sector room to govern itself. Altman suggests creating licensing and testing requirements for the development and release of AI tools, establishing safety standards, and bringing in independent auditors to assess the models before they are released. He and many of his contemporaries also envision an international regulator akin to the International Atomic Agency to help impose and coordinate these standards at a global scale. Those suggestions for regulation, which senators applauded him for during the hearing, would amount to little more than self-regulation, said West of the AI Now Institute. The system as Altman proposes it, she said, would allow players who check off certain boxes and are deemed "responsible" to "move forward without any further levels of scrutiny or accountability". It's self-serving, she argued, and deflects from "the enforcement of the laws that we already have and the upgrading of those laws to reach even basic levels of accountability". OpenAI did not respond to a request for comment by the time of publication. Altman's and other AI leaders' proposals also focus on reining in "hypothetical, future" systems that are able to take on certain human capabilities, according to West. Under that scheme, the regulations would not apply to AI systems as they're being rolled out today, she said. And yet the harms AI tools can cause are already being felt. Algorithms power the social feeds that have been found to funnel misinformation to wide swaths of people; it's been used to power systems that have perpetuated discrimination in housing and mortgage lending. In policing, AI-enabled surveillance technology has been found to disproportionately target and in some cases misidentify Black and brown people. AI is also increasingly used to automate error-prone weaponry such as drones. Generative AI is only expected to intensify those risks. Already ChatGPT and other large language models like Google's Bard have given responses rife with misinformation and plagiarism, threatening to dilute the quality of online information and spread factual inaccuracies. In one incident last week, a New York lawyer cited six cases in a legal brief which all turned out to be nonexistent fabrications that ChatGPT created. "The propensity for large language models to just add in totally incorrect things – some less-charitable people have just called them bullshit engines – that's a real slow-burner danger," said Daniel Leufer, senior policy analyst at the digital rights organization Access Now. During the congressional hearing, Senator Richard Blumenthal mentioned his deep concern about generative AI's impact on labor – a concern that West, of the AI Now Institute, said is already being realized: "If you look to the WGA strikes, you see the use of AI as a justification to devalue labor, to pay people less and to pay fewer people. The content moderators who are involved in training ChatGPT also recently unionized because they want to improve their labor conditions as well as their pay." The current focus on a hypothetical doomsday scenario where the servant class, composed of AI-powered bots, will become sentient enough to take over, is an expression of current inequalities, some experts have argued. A group of 16 women and non-binary tech experts, including Timnit Gebru, the former co-lead of Google's ethical AI team, released an open letter last month criticizing how the AI industry and its public relations departments have defined what risks their technology poses while ignoring the marginalized communities that are most affected. "We reject the premise that only wealthy white men get to decide what constitutes an existential threat to society," the letter said. The limits of self-regulation The budding relationship between lawmakers and the AI industry echoes the way big tech companies like Meta and Twitter have previously worked with federal and local US governments to craft regulation, a dynamic that rights groups said waters down legislation to the benefit of these companies. In 2020, Washington state, for example, passed the country's first bill regulating facial recognition – but it was written by a state senator who was also a Microsoft employee and drew criticism from civil rights groups for lacking key protections. "They end up with rules that give them a lot of room to basically create self-regulation mechanisms that don't hamper their business interests," said Mehtab Khan, an associate research scholar at the Yale Information Society Project. Conversations in the European Union about AI are far more advanced. The EU is in the midst of negotiating the AI Act, proposed legislation that would seek to limit some uses of the technology and would be the first law on AI by a major regulator. While many civil society groups point to some weaknesses of the draft legislation, including a limited approach to banning biometric data collection, they agree it's a much more cohesive starting point than what is being currently discussed in the US. Included in the draft legislation are prohibitions on "high-risk" AI applications like predictive policing and facial recognition, a development advocates attribute to the years-long conversations leading up to the proposal. "We were quite lucky that we put a lot of these things on the agenda before this AI hype and generative AI, ChatGPT boom happened," said Sarah Chander, a senior policy adviser at the international advocacy organization European Digital Rights. The European parliament is expected to vote on the proposal on 14 June. Although the center-right European People's party has pushed back aggressively against the total bans of tools like facial recognition, Chander feels optimistic about prohibitions on predictive policing, emotion recognition and biometric categorization. The battle over the final details will continue for the better part of the next year – after the parliamentary vote, EU member governments will become involved in the negotiations. But even in the EU, the recent generative AI hype cycle and the concerns about a dystopian future have been drawing lawmakers' attention away from the harms affecting people today, Chander said. "I think ChatGPT muddies the water very much in terms of the types of harms we're actually talking about here. What are the most present harms and for whom do we care about?" Despite that lack of wide-reaching regulations in the AI Act, the proposals were far-reaching enough to make Altman tell reporters that the company would cease operating if it couldn't comply with the regulations. Altman slightly walked that statement back the next day, tweeting that OpenAI had no plans to leave, but his opposition to the AI Act signaled to rights advocates his eagerness to push back against any laws that would constrain business. "He only asks for the regulation that he likes, and not for the regulation that is good for society," said Matthias Spielkamp, the executive director of Algorithm Watch, a European digital rights group. Amid the lack of urgency from US lawmakers and the administration, digital rights experts are looking at existing law and efforts at the state level to put guardrails on AI. New York, for example, will require companies to conduct annual audits for bias in their automated hiring systems, as well as notify candidates when these systems are being used and give applicants the option to request the data collected on them. There are also several existing laws that may prove useful, researchers said. The Federal Trade Commission's algorithmic disgorgement enforcement tool, for instance, allows the agency to order companies to destroy datasets or algorithms they've built that are found to have been created using illicitly acquired data. The FTC also has regulations around deception that allow the agency to police overstated marketing claims about what a system is capable of. Antitrust laws, too, may be an effective intervention if the firms building and controlling the training of these large language models begin to engage in anticompetitive behavior. Privacy legislation on the state level could serve to provide reasonable protections against companies scraping the internet for data to train AI systems, said Winters. "I can't in good conscience predict that the federal legislature is going to come up with something good in the near future."