

GENERATIVE AI PRESENTS OPPORTUNITIES FOR CROSS-BORDER COORDINATION OF REGULATION

As I touched upon in my introduction to generative AI ([posted](#) last week), the roll-out, followed by the unprecedented surge in use, of ChatGPT and other similar platforms based on generative AI has forced the hand of regulators to address the need for transparency and guardrails. While development of the underlying large language models has been concentrated in a few countries, policymakers and regulators in a growing number of jurisdictions are facing calls to act to protect users in their jurisdictions from the threats posed by the technology. That number will likely quickly increase.

The emerging consensus among regulators and policymakers that generative AI urgently needs to be regulated presents at least two opportunities. First, policymakers and regulators could adopt harmonized approaches to generative AI and, second, broader efforts around in adjacent spaces of data protection and privacy could likewise be harmonized across jurisdictions. A patchwork of regulations and enforcement actions would not only represent a missed opportunity but would be highly counter-productive.

As the world emerged from the pandemic, there was renewed talk of global responses to global threats – after all, the pandemic responses had largely degenerated to every country for itself. Public health, climate change, and the technology that would sometime in the future be unleashed by artificial intelligence and quantum computing were the most often cited examples of issues that lent themselves to comprehensive, coordinated responses. GDPR was a reminder of the impact of the extraterritorial effect of EU rules (ditto for EU climate change disclosure) as well as a reminder that while Europe had led the way on data protection and privacy, the United States had largely dropped the ball.

After barely five months, ChatGPT has accelerated the urgency of coordinated responses.

Regulatory Efforts

To recap, on April 13, Senate Majority Schumer [announced](#) a legislative initiative to both advance and manage AI, in light, in his words, of its “consequential and fast moving impact on society, national security and the global economy.” This initiative incidentally is presented as a national (*i.e.*, American) priority, and in fact calls out the release by China of draft Measures for the Management of Generative Artificial Intelligence Services¹. The announcement speaks of balancing innovation and leadership against security, accountability and transparency. Presumably conversations with industry, government, academics and advocacy groups will follow the playbook used for the CHIPS and Science Act.

The Schumer initiative has two key elements: (i) mandated review and testing of AI technologies by independent experts ahead of release or update and (ii) the output of the review and testing forming the foundation for four guardrails:

- **Who** trained the algorithms?
- **What** is the source of the data?
- **How** do the underlying models generate outputs?

¹ For a useful analysis of the Chinese draft measures, see the [post](#) by Stanford’s DigiChina Project, entitled “How will China’s Generative AI Regulations Shape the Future? A DigiChina Forum.”

- How to **Protect** users and the broader society?

The ultimate goal of the guardrails is to reduce the potential for misuse, disinformation and bias.

This legislative response is likely to be a significant undertaking given the need to educate members of Congress and their staffs, and the need to coordinate among multiple committees that arguably have jurisdiction over a technology whose impact is so pervasive across society. In the meantime, there are at least two other legislative initiatives that occupy adjacent spaces:

- the proposed [American Data Privacy and Protection Act](#) (H.R. 8152), which would require most companies to limit the collection, processing and transfer of personal data to that which is reasonably necessary to provide a requested product or service and to other specified circumstances; generally would prohibit companies from transferring individuals' personal data without their affirmative express consent; would establish consumer data protection, including the right to access, correct and delete personal data and require companies to provide individuals with a means to opt out of such advertising; would provide additional protections with respect to personal data of individuals under 17; and would prohibit companies from using personal data to discriminate based on specified protected characteristics; and
- the proposed [Algorithmic Accountability Act](#) (H.R. 6580), which requires companies to assess the impacts of the automated systems they use and sell, creates new transparency about when and how automated systems are used, and empowers consumers to make informed choices about the automation of critical decisions. Among other things, the bill would establish a baseline requirement that companies assess the impacts of automated critical decision-making.

The National Telecommunications and Information Administration (within the Commerce Department) [has called for comment](#) on policies to support the development of AI audits, assessments, certifications and other mechanisms to engender trust in AI systems – what it calls the “AI accountability ecosystem.”

The Federal Trade Commission (FTC) in February [launched](#) the Office of Technology, aimed at strengthening the FTC's ability to keep pace with technological challenges in the digital marketplace. Also in February, an attorney in the FTC Division of Advertising Practices, in a post entitled “Keeping your AI claims in check,” [called out](#) misleading or incorrect claims related to AI, including claims that exaggerate what AI can do, promises that AI can do something better than a non-AI product or baseless AI claims. Most interestingly, the post asks whether the provider is aware of the reasonably foreseeable risks and impacts of an AI product, including what happens if it fails or yields biased results.

In the meantime, in the absence of federal legislation, various jurisdictions including [Colorado](#), [Connecticut](#), [Virginia](#) and [New York City](#) are joining Californian and moving forward on privacy legislation governing “automated decision-making” (ADM), namely a process of making decisions by automated means, typically without any human intervention. Essentially these bills, which take effect in 2023, give consumers opt-out rights for automated decision-making that would result in the provision or denial of: financial services, housing, insurance, education enrolment, criminal justice, employment opportunities, health

care services and access to essential goods and services. Businesses would be required to assess data protection before using these tools to make decisions that pose reasonably foreseeable risks to consumers, ranging from unfair or deceptive practices to financial or physical injury to intrusion into private affairs.

There are parallels in the EU's [GDPR](#) (see article 22) and, as noted in my previous briefing note, the European Commission returned to the drawing board to tweak the proposed [Artificial Intelligence Act](#) (AIA). A group of European Parliament lawmakers, in an [open letter](#) issued last week, called for a set of rules specifically aimed at “foundation models” (which encompasses generative AI), within the framework of the AIA.² The lawmakers also called on President Biden and EC President Ursula von der Leyen to convene a high-level global summit on AI, to agree on a preliminary set of governing principles to address AI and called on the principals of the Trade and Technology Council (TTC)³ to agree on an agenda for that global summit, recognizing that involving the European Parliament and the US Congress is critical.

The European Data Protection Board [announced](#) last week that it would set up a task force to coordinate enforcement actions against OpenAI (following Italy's individual enforcement action).

Concluding Thoughts

The UK government last month released its [White Paper](#) entitled “A pro-innovation approach to AI regulation,” in which it envisions avoiding “heavy-handed legislation.” In fact, it envisions not enacting any new legislation at all. Whether it can do so will be the subject of a separate briefing note. More broadly, there is a tension when it comes to generative AI between self-regulation and regulation, just as there has been a tension for some time now on broader privacy concerns and on addressing the unchecked power of platform algorithms to amplify extremism and hate. The European Union recognized, when passing the Digital Services Act (see my previous briefing note, available [here](#)), that self-regulation is nowhere near sufficient.

As US policymakers ponder next steps, the first item of business should be passage of the American Data Privacy Protection Act. They should in parallel turn to generative AI, and when faced with calls to prioritize self-regulation over regulation, lawmakers should not be swayed by the China-is-getting-ahead argument. We really do need to get this right, and the more consistent the rules across the globe, the better for all concerned. The TTC may be a

² A [post](#) on Euractive.com reports that Members of the European Parliament are close to finalizing revisions to the AIA that involve distinguishing between foundation models and general purpose AI, and imposing a more restrictive regime on the former. [Coined](#) by researchers at Stanford, the term “foundation models” means models that are trained on broad data (generally using self-supervision at scale) that can be adapted to a wide range of downstream tasks (e.g., ChatGPT).

³ The TTC was established at the US-EU Summit in June 2021. It is a high-level set of working groups intended, among other things, to grow bilateral trade and investment relationship and seek common ground, and strengthen global cooperation, on technology, digital issues and supply chains. Among its working groups are groups focused on technology standards cooperation (including AI and emerging technologies) and data governance and technology platforms. (See [White House Statement](#).)

very a good place to start. Above all, we need to be cognizant that time is not on our side, even if industry heeds calls for a six-month pause. All to say, it is urgent.

* * *

Mark S. Bergman
[7Pillars Global Insights, LLC](#)
Washington, D.C.
April 25, 2023