Testimony of Christina Montgomery, Chief Privacy and Trust Officer, IBM

Before the

U.S. Senate Judiciary Committee

Subcommittee on Privacy, Technology, and the Law

Hearing on “Oversight of AI: Rules for Artificial Intelligence”

Tuesday, May 16, 2023

Chairman Blumenthal, Ranking Member Hawley, members of the Subcommittee:

Thank you for today's opportunity to present before the subcommittee. My name is Christina Montgomery, and I am IBM's Chief Privacy and Trust Officer. I also co-chair our company's AI Ethics Board.

Introduction

AI is not new, but it has advanced to the point where it is certainly having a moment. This new wave of generative AI tools has given people a chance to experience it first-hand. Citizens are using it for help with emails, their homework, and so much more.

While IBM is not a consumer-facing company, we are just as active – and have been for years – in helping business clients use AI to make their supply chains more efficient, modernize electricity grids, and secure financial networks from fraud. IBM's suite of AI tools, called IBM Watson after the AI system that won on TV's Jeopardy! more than a decade ago, is widely used by enterprise customers worldwide. Just recently we announced a new set of enhancements, called watsonx, to make AI even more relevant today.[1] Our company has extensive experience in the AI field in both an enterprise and cutting-edge research context, and we could spend an entire afternoon talking about ways the technology is being used today by business and consumers.

But the technology's dramatic surge in public attention has, rightfully, raised serious questions at the heart of today's hearing. What are AI's potential impacts

[1] See https://newsroom.ibm.com/2023-05-09-IBM-Unveils-the-Watsonx-Platform-to-Power-Next-Generation-Foundation-Models-for-Business.

on society? What do we do about bias? What about misinformation, misuse, or harmful and abusive content generated by AI systems?

Senators, these are the right questions, and I applaud you for convening today's hearing to address them head-on.

IBM has strived for more than a century to bring powerful new technologies like artificial intelligence into the world responsibly, and with clear purpose. We follow long-held principles of trust and transparency that make clear the role of AI is to augment, not replace, human expertise and judgement. We were one of the first in our industry to establish an AI Ethics Board, which I co-chair, and whose experts work to ensure that our principles and commitments are upheld in our global business engagements.[2] And we have actively worked with governments worldwide on how best to tailor their approaches to AI regulation.

It's often said that innovation moves too fast for government to keep up. But while AI may be having its moment, the moment for government to play its proper role has not passed us by. This period of focused public attention on AI is precisely the time to define and build the right guardrails to protect people and their interests.

It is my privilege to share with you IBM's recommendations for those guardrails.

Precision Regulation

The hype around AI has created understandable confusion among some in government on where intervention is needed and how regulatory guardrails should be shaped. But at its core, AI is just a tool, and tools can serve different

[2] See https://www.ibm.com/artificial-intelligence/ethics.

purposes. A wrench can be used to assemble a desk or construct an airplane, yet the rules governing those two end products are not primarily based on the wrench — they are based on use.

That is why IBM urges Congress to adopt a "precision regulation" approach to artificial intelligence. This means establishing rules to govern the deployment of AI in specific use-cases, not regulating the technology itself.

A precision regulation approach that we feel strikes an appropriate balance between protecting Americans from potential harms and preserving an environment where innovation can flourish would involve:

- **Different Rules for Different Risks** – A chatbot that can share restaurant recommendations or draft an email has different impacts on society than a system that supports decisions on credit, housing, or employment. In precision regulation, the more stringent regulation should be applied to the use-cases with the greatest risk.
- **Clearly Defined Risks** – There must be clear guidance on AI end uses or categories of AI-supported activity that are inherently high-risk. This common definition is key to ensuring that AI developers and deployers have a clear understanding of what regulatory requirements will apply to a tool they are building for a specific end use. Risk can be assessed in part by considering the magnitude of potential harm and the likelihood of occurrence.
- **Be Transparent, Don't Hide Your AI** – Americans deserve to know when they are interacting with an AI system, so Congress should formalize disclosure requirements for certain uses of AI. Consumers should know when they are interacting with an AI system and whether they have recourse

to engage with a real person, should they so desire. No person, anywhere, should be tricked into interacting with an AI system. AI developers should also be required to disclose technical information about the development and performance of an AI model, as well as the data used to train it, to give society better visibility into how these models operate. At IBM, we have adopted the use of AI Factsheets – think of them as similar to AI nutrition information labels – to help clients and partners better understand the operation and performance of the AI models we create.

- **Showing the Impact** – For higher-risk AI use-cases, companies should be required to conduct impact assessments showing how their systems perform against tests for bias and other ways that they could potentially impact the public, and attest that they have done so. Additionally, bias testing and mitigation should be performed in a robust and transparent manner for certain high-risk AI systems, such as law enforcement use-cases. These high-risk AI systems should also be continually monitored and re-tested by the entities that have deployed them.[3]

IBM recognizes that certain AI use-cases raise particularly high levels of concern. Law enforcement investigations and credit applications are two often-cited examples. By following the risk-based, use-case specific approach at the core of precision regulation, Congress can mitigate the potential risks of AI without stifling its use in a way that dampens innovation or risks cutting Americans off from the trillions of dollars of economic activity that AI is predicted to unlock.

Generative AI

The explosion of generative AI systems in recent month has caused some to call for

[3] See https://www.ibm.com/policy/ai-precision-regulation/.

a deviation from a risk-based approach and instead focus on regulating AI in a vacuum, rather than its application. This would be a serious error, arbitrarily hindering innovation and limiting the benefits the technology can provide. A risk-based approach ensures that guardrails for AI apply to any application, even as this new, potentially unforeseen developments in the technology occur, and that those responsible for causing harm are held to account.[4]

When it comes to AI, America need not choose between responsibility, innovation, and economic competitiveness. We can, and must, do all three now.

Business' Role

This focus on regulatory guardrails established by Congress does not – not by any stretch – let business off the hook for its role in enabling the responsible deployment of AI.

I mentioned that IBM has strong AI governance practices and processes in place across the full scope of our global enterprise. We have principles grounded in ethics and people-centric thinking, and we have strong processes in place to bring them to life. This is also good business: IBM has long recognized ethics and trustworthiness are key to AI adoption, and that the first step in achieving these is the adoption of effective risk management practices.

Companies active in developing or using AI must have (or be required to have) strong internal governance processes, including, among other things:

[4] See https://newsroom.ibm.com/Whitepaper-A-Policymakers-Guide-to-Foundation-Models.

- Designating a lead AI ethics official responsible for an organization's trustworthy AI strategy, and
- Standing up an AI Ethics Board or similar function to serve as a centralized clearinghouse for resources to help guide implementation of that strategy.

IBM has taken both steps and we continue calling on our industry peers to follow suit.

Our AI Ethics Board plays a critical role in overseeing our internal AI governance process, creating reasonable internal guardrails to ensure we introduce technology into the world in a responsible and safe manner. For example, the board was central in IBM's decision to sunset our general purpose facial recognition and analysis products, considering the risk posed by the technology and the societal debate around its use. IBM's AI Ethics Board infuses the company's principles and ethical thinking into business and product decision-making. It provides centralized governance and accountability while still being flexible enough to support decentralized initiatives across IBM's global operations.

The board, along with a global community of AI Ethics focal points and advocates, reviews technology use-cases, promotes best practices, conducts internal education, and leads our participation with stakeholder groups worldwide. In short, it is a mechanism by which IBM holds our company and all IBMers accountable to our values, and our commitments to the ethical development and deployment of technology.

We do this because we recognize that society grants our license to operate. If businesses do not behave responsibly in the ways they build and use AI, customers will vote with their wallets. And with AI, the stakes are simply too high, the

technology too powerful, and the potential ramifications too real. AI is not some fun experiment that should be conducted on society just to see what happens or how much innovation can be achieved.

If a company is unwilling to state its principles and build the processes and teams to live up to them, it has no business in the marketplace.

Conclusion

Mr. Chairman, and members of the subcommittee, the era of AI cannot be another era of move fast and break things. But neither do we need a six-month pause – these systems are within our control today, as are the solutions. What we need at this pivotal moment is clear, reasonable policy and sound guardrails. These guardrails should be matched with meaningful steps by the business community to do their part. This should be an issue where Congress and the business community work together to get this right for the American people. It's what they expect, and what they deserve.

IBM welcomes the opportunity to work with you, colleagues in Congress, and the Biden Administration to build these guardrails together.

Thank you for your time, and I look forward to your questions.