Emerson Collective

November 21, 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Raffi Krikorian's Responses to Additional Questions for the Record

Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on October 18, 2023 to testify at the hearing entitled "Safeguarding Data and Innovation: Setting the Foundation for the use of Artificial Intelligence."

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thank you again for your help, and please let me know if you have any questions.

Sincerely,

Raffi Krikorian
Chief Technology Officer
Emerson Collective

Mr. Raffi Krikorian

Attachment – Additional Questions for the Record

The Honorable Russ Flucher

1. **Where do you "draw the line" when it comes to the liability attached between the developer and the deployer on the use of AI programs?**

This topic we are delving into is profoundly complicated, and it's important to clarify at the outset that I am not a lawyer. My expertise lies in being a technologist and engineer with hands-on experience in implementing AI systems. I bring a combined technical and philosophical perspective to the discussion of liability between AI developers and deployers. This is a complex area, best illustrated with practical examples.

Let's consider self-driving cars first. In this domain, it is crucial for the vehicle to communicate its capabilities and limitations clearly to the human driver. The driver needs to understand where and when the robot will not be able to be in control, and when he or she needs to take over. Moreover, these systems are designed to monitor the driver's state, ensuring his or her alertness and engagement so as to ensure that robot and the driver are operating together. Finally, the importance of maintaining detailed logs of the robot's actions and decisions cannot be overstated, as these records are vital for post-incident analysis and determining liability in the event of an accident.

When we shift our focus to the emerging field of generative AI systems, the complexity of liability issues increases significantly – there are also more stakeholders here: those who created the content that these systems are trained upon, the developers who create these systems, the application developers who build upon these systems, and the users who use the systems. One could consider applying the end-to-end principle here, pushing liability towards the application layer or the end user, however, the nature of these systems complicates this approach. Generative AI is being developed in a manner that makes it not only complex in operation but also incredibly easy to integrate and build upon.

Given this ease of use and the push for widespread adoption, it seems unfair to shift the burden of dealing with issues like copyright infringement, disinformation, and bias entirely onto end users and application developers. Expecting sophistication and comprehensive understanding from these parties, especially given the power and rapid deployment of these systems, is unrealistic. Therefore, a gradient approach to liability is more suitable, where responsibility is more heavily weighted towards the foundational layer of the AI system. This layer significantly influences the AI's overall behavior and capabilities, and hence, should bear a greater portion of the liability.

For this gradient approach to be effective, transparency regarding the AI system's capabilities and limitations is essential. This can be achieved through clear and comprehensive impact assessments, which must be accessible and understandable to all parties involved, from developers to end-users. These assessments should clearly delineate the strengths and potential weaknesses of the AI system, enabling informed decision-making.

In addition, similar to the logging system in self-driving cars, a detailed record of decision-making in generative AI systems is crucial. This log would offer clarity and transparency in

decision-making, which is vital for post-analysis. It would enable a comprehensive understanding of how decisions were made or influenced at various stages, from the foundational model to the end user. Such transparency and record-keeping are indispensable in navigating the complex landscape of AI liability, ensuring that all parties understand their roles and responsibilities in the development and deployment of these advanced technologies.

The Honorable Debbie Dingell

Privacy should be of utmost importance to this Committee and our country, and it is a fundamental aspect in the digital age. We need to act now. The status quo in this ever-changing landscape is insufficient. And relying on self-regulation has proven repeatedly to be inadequate. Privacy – as we all know – is a fundamental right, and we must protect our families. This Committee's job is to ensure that consumers have the final say over their personal data. These privacy implications also put at risk the security of our personal information that can easily be exploited by our adversaries, like China and Russia. It is crucial that Congress addresses this. Artificial intelligence is here and continuing to evolve. It has major implications on our health and safety, economy, and national security.

1. **Mr. Krikorian, without a national privacy law, do companies have incentives to act in good faith? Will these state laws suffice? Will voluntary standards be enough? Why must we act now?**

First off, it's my belief that the majority of companies and developers in the tech industry are good actors. However, I have concerns regarding their background, education, and experience in handling privacy issues, as well as the incentive systems under which they operate. These incentives can sometimes conflict with the imperative to protect user privacy.

As I mentioned in my oral testimony, we are living in an age of increasing digital surveillance. And, we are witnessing substantial technological advancements, particularly in fields like deep learning. Deep learning algorithms, which are at the forefront of these advancements, require vast datasets to effectively make decisions and identify patterns that are beyond human capability. This need for data is further incentivizing a culture of extensive data collection, often at the expense of user privacy. And, the pace at which this technology is evolving is noteworthy. The urgency to protect user data becomes increasingly paramount.

Therefore, people's privacy should be the foundational element of any legislative work in this area and we need to start now. Given the current incentive systems, the recent technological and research advances, and the fast pace at which everything is moving, it is critically important that the needs of consumers and users are taken into account. Comprehensive privacy legislation is necessary not just to protect individuals but also to provide clear and robust guidelines for developers. This will enable them to innovate responsibly, in a direction that respects and safeguards user privacy.

In sum, the current state of technological advancement, particularly in AI and deep learning, combined with the incentive structures within the tech industry, underscores the need for

Attachment – Additional Questions for the Record

immediate and thoughtful legislative action. We must ensure that privacy is not just a consideration, but a cornerstone in the development and deployment of these powerful technologies.