Reply to Questions for the Record

Ms. Courtney Lang, Vice President of Policy, Trust, Data, and Technology, The Information Technology Industry Council

House Energy and Commerce Committee
Subcommittee on Communications and Technology
"Leveraging AI to Enhance American Communications"
November 14, 2023

Attachment —Additional Questions for the Record

The Honorable Earl L. "Buddy" Carter

1. How do Big Tech platforms make use of AI systems when making content moderation decisions? How should companies ensure AI is used responsibly when they use AI for content moderation?

While ITI cannot speak to individual companies' practices, in general, digital platforms leverage AI to quickly sift through and organize extraordinarily large amounts of online data and user-generated content. AI plays a role in automating content moderation decisions, identifying and removing inappropriate or violent content, and upholding community standards and guidelines. Companies operating in the U.S. also account for the First Amendment and other freedom of speech protections. There are complex questions and ultimately human decisions about where to draw the lines on graphic or harmful content.

There are several ways in which companies are ensuring that AI is used responsibly in content moderation. For example, companies may leverage AI in addition to a human-in-the-loop approach, where flagged content is reviewed by human moderators to ensure accuracy, especially in ambiguous or complex cases. They also take steps to ensure that models are trained on representative and diverse datasets that reflect a wide range of content and user behaviors to mitigate bias. Consistent evaluation of models throughout their lifecycle also ensures that they are performing as they should and if not, are updated in a way that addresses noted issues. Finally, collaborative initiatives with external experts, industry stakeholders, and user communities can also contribute to creating more inclusive AI systems.

2. It is notably difficult to determine how an AI system came to a particular conclusion. How well does the AI understand the context of content, especially in cases where content might be controversial or ambiguous?

AI systems are trained on vast amounts of data and in the case of generative AI, can generate responses, text, or information that reflect important context. At the same time, it is important to recognize that AI systems are also limited by the data that they are trained on, which is why it is important that they are trained on diverse and representative datasets. Additionally, while AI systems are trained to recognize and infer things based on patterns, and they can, in certain instances, emulate human characteristics, they lack moral understanding or specific personal, human experience that can aid in digesting complex or ambiguous topics. With that being said, human authentication and/or including a human-in-the-loop in high-risk instances is one way to bolster understanding. Additionally, developers are working to improve the ability of AI systems to recognize context by continuously evaluating and fine-tuning systems, as mentioned above, which is an ongoing process.

The Honorable Randy Weber

1. ITI has been engaged in conversations around the world about "where do we go from here" with regards to AI regulation for years. I'm also interested in "where we've been," so that we don't repeat a mistake. What sorts of regulations have been, in your opinion, the worst at creating an innovative climate for the AI sector? How would you suggest that the federal government place more emphasis on innovation without neglecting accountability and protecting Americans' private data?

Federal privacy legislation is fundamental to protecting Americans' private data and is an important way to address risks stemming from AI use in that regard. AI systems are often trained on large datasets. A privacy law would ensure that the users' personal information is collected, processed, and stored responsibly and protect individual privacy rights.

Overly broad, prescriptive regulation will serve to hamper innovation. We advocate for a risk-based approach to AI regulation to ensure that it is narrowly targeted at those use cases that have the most significant impact on human rights or safety and allow innovation to continue unfettered in low-risk use cases. In defining high-risk, legislation should avoid classifying entire sectors as high-risk, and take a nuanced approach that reflects the multitude of uses of AI within a sector that could be low-risk. An approach should also reflect the roles of different stakeholders in the AI ecosystem – for example, developers and deployers -- and ensure that responsibilities are allocated accordingly. Beyond that, the federal government should support efforts that aim to advance research and development.

2. Automated features—which we could liken to "pre-AI"—have long been used by the telecommunications industry to ensure network stability and safety. Would you mind going into a little more detail about how the use of AI wouldn't be the introduction of something new, but the continuation of technology that has been used safely for years?

The telecommunications industry has relied upon automation and machine-learning for years (and in some cases decades) to perform certain tasks. The use of AI systems should therefore not be viewed as the introduction of entirely new technology, but as an evolution of existing technology. Automation has been used to help with network provisioning and management for decades, whereby networks are monitored and analyzed in order to adjust as necessary for optimized performance and efficiency. AI can be seen as building upon automation by allowing for more predictive inferences to be made, allowing for the introduction of things like self-healing networks. Cybersecurity risks are also something that telecom operators have been considering for many years and one of the reasons for the proliferation of basic encryption standards such as "https." However, AI is helping to bolster network security further by monitoring network traffic and detecting anomalous behavior, allowing for immediate action to be taken in order to protect the network from malicious actors.

The Honorable Anna Eshoo

1. Your written testimony discusses the need for a risk-based approach to artificial intelligence (AI) regulation and encourages the adoption of risk-based governance frameworks.

For the record, how should Congress determine what the risks associated with AI are? Who should be consulted? Should Congress require auditing of AI systems pre and post deployment? If so, should the auditing be overseen by federal agencies or a third party?

Determining risk is an important component of a risk-based approach. We encourage Congress to view risk as a combination of the negative impact / magnitude of harm that would occur if an event happens and 2) the likelihood of that event happening, as discussed in NIST's AI Risk Management Framework. In general, we encourage Congress to consider high-risk applications of AI as those applications in which a negative outcome could significantly or legally impact a person's human rights or safety. This includes things like access to basic services, such as housing, education, or a loan. With that being said, we have encouraged NIST as a part of its AI risk management work to establish risk evaluation criteria to help guide organizations as they seek to establish risk thresholds and understand their risk tolerance. Such methodology would be helpful for organizations in determining the risk-level of a specific AI use case, informing the steps that they should take to mitigate or treat the risk. More broadly, it could help to inform the development of targeted legislation. Such a methodology should also identify the appropriate roles for AI developers, deployers, users, and other stakeholders in making risk determinations. These determinations are also crucial for helping stakeholders identify specific technological mechanisms for measuring, mitigating, and controlling high-risk attributes of AI systems, where applicable.

It is important to note that there are different mechanisms that can help to foster accountability. Audits are one mechanism, as are assessments and certifications. Internal audits, assessments, and certifications can play a role in facilitating trust, communicating information, and driving internal change and that all organizations in the AI value chain should adopt practices focused on driving accountability. At the same time, requirements related to audits, assessments, or certifications should be scoped based on the level of risk posed and relevant context.

That being said, we encourage Congress to exercise caution in considering mandating external audits of AI systems. Currently, we believe that mandating external audits of AI systems is premature due to several practical challenges, including the lack of a standardized framework on which to base an external assessment or audit and workforce capacity.

2. Your written testimony discusses how policymakers should evaluate the existing legal and policy landscape in the United States, considering existing laws that may already protect against identified risks. You discuss the need for a sector-specific approach, given agencies have unique expertise in their areas of jurisdiction and can most effectively understand the unique risks that may stem from the use of AI in their sectors. For the record, please elaborate on how the federal government can enforce existing laws that interact with AI. What resources are necessary for federal agencies to enforce these laws when considering AI? Do the agencies have all the authority and resources they need to do so effectively?

There are several existing laws that address concerns related to key AI risks. For example, the Civil Rights Act of 1964, the Fair Credit Reporting Act of 1970, the Health Insurance Portability and Accountability Act of 1996, and the Federal Trade Commission Act, are all existing laws that protect users against some of the possible harms stemming from the use of AI. Legal

frameworks, like product liability law, contract law, or tort law, could also be used to address concerns related to AI. On multiple occasions various government agencies have reiterated their existing authority – see for example, the joint statement issued by the Equal Opportunity Employment Commission (EEOC) with the Consumer Financial Protection Bureau (CFPB), the Department of Justice's Civil Rights Division (DOJ) and the Federal Trade Commission.[1] The FTC has also publicly issued a blog on its ability to enforce Section 5 of the FTC Act, which prohibits unfair or deceptive practices, including the use of biased algorithms.[2] The CFPB has noted in Circular 2023-03 that it will enforce the Equal Opportunity Credit Act, under which it is unlawful to discriminate against any applicant based on protected attributes.[3]

The recently released AI EO directs federal agencies to examine their existing authorities and how they can exercise them. For example, Section 4 directs CISA and relevant sector risk management agencies (SRMAs) to assess risks posed by use of AI in critical infrastructure, in addition to incorporating the AI Risk Management Framework and other appropriate guidance into safety and security guidelines for critical infrastructure owners and operators. Longer term, it encourages SRMAs to consider incorporating mandatory guidance through regulatory action as they deem appropriate. Section 5 of the EO directs the FTC to consider whether to exercise its authority to ensure fair competition in the AI marketplace and ensure that consumers are protected from harms. Beyond this, it directs numerous sector-specific agencies to review existing authorities to protect consumers from risks that may arise from the use of AI and where necessary, clarify existing guidance or otherwise consider a rulemaking process in places where it becomes clear additional regulatory authority is necessary. These activities will help shed additional light on where agencies may need additional resources.

In general, there will likely be an increasing need for additional AI expertise within sector-specific agencies. In those cases, NIST, if appropriately resourced, could potentially play a consulting role in cases where additional expertise is needed to make determinations about risk, or about how to apply the RMF, or more generally about how to apply and execute risk management processes.

The Honorable Lizzie Fletcher

1. What would you recommend we be thinking about when it comes to fashioning digital privacy legislation in the context of AI? When we are thinking about how to put together a framework, what are the AI considerations that we should be taking into account in that process?

Congress should build upon the strong bipartisan work that has already been done in the Energy & Commerce Committee to advance comprehensive digital privacy legislation. The increasing adoption of AI and the accelerating development of models trained on large datasets of publicly available information only underscore the need for uniform national standards about the collection, processing, and storage of Americans personal information. However, policymakers

[1] https://www.eeoc.gov/joint-statement-enforcement-efforts-against-discrimination-and-bias-automated-systems
[2] https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai
[3] https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/

should also be mindful about where data collection is needed to protect or mitigate against potential harms, such as addressing concerns about bias.

The Honorable Debbie Dingell

1. Conversely, 5G also enables AI, as it enhances network speeds and other functionalities, which helps to improve AI efficiencies. Ms. Lang, how can this intersection – between 5G and AI – lead to technological advances for the future of autonomous vehicles (AVs)?

5G provides increased bandwidth, reduced latency, and greater capacity, all things that are integral to the successful deployment of AVs. In moving from 5G to 6G, AI will be increasingly integrated into networks, allowing for intelligent edge computing, dynamic spectrum allocation, and more. Importantly, AI can help cars to analyze data collected by the sensors, and using things like object recognition, can enable cars to more precisely and accurately make decisions. Additionally, self-healing capabilities (powered by AI), will assist in determining whether a vehicle has the necessary latency to continue driving unassisted (or otherwise switch back to manual control).

2. Ms. Lang, how can AI be leveraged to improve the accuracy of national broadband maps, and what potential benefits does this hold for telecommunications companies and consumers?

AI-based mapping systems can not only utilize US Census Bureau data but also can convert satellite images into real-world features to develop a map of broadband serviceable locations that can help identify communities that previous mapping models missed. More accurate mapping strategies can also assist in network deployment, which helps in determining optimal tower locations, estimate coverage areas, and predict network capacity requirements; thus, enabling providers to make informed decisions during network expansion. This holds great promise for network operators making capital expenditure and investment decisions and can help optimize the use of public funding to more precisely target unserved and underserved areas. Ultimately, consumers benefit from these efficiencies, which can speed network deployment to those who need it most.