Opening Statement of Chair Cathy McMorris Rodgers As Prepared for Delivery Committee on Energy and Commerce Subcommittee on Innovation, Data, and Commerce Hearing entitled "Safeguarding Data and Innovation: Building the Foundation for the Use of Artificial Intelligence" October 18, 2023

Good morning everyone.

Welcome to the first in our series of AI hearings, and the seventh data privacy related hearing we've held this year.

The promises of artificial intelligence are extensive—from more affordable energy and better health care, to a more productive workforce and a better standard of living.

Unlocking this technology's potential could radically strengthen American economic and technological leadership across the board.

In addition, the power of AI can also be abused, and raises serious concerns and challenges that must be addressed.

It's critical that America —not China—is the one addressing those challenges and leading in AI's development and deployment.

The best way to start is by laying the groundwork to protect people's information with a national data privacy standard.

This is a foundational first step towards a safe and prosperous AI future.

If used correctly, AI can be a source for good.

It can help us unlock life-changing technologies like self-driving vehicles and enhanced health diagnostics systems...

... enhance protections against national security threats and data breaches...

...while assisting companies and law enforcement to better scan Internet platforms for illegal activity, like child sexual abuse material and fentanyl distribution.

To unlock these benefits though, we need to first establish foundational protections for the data that powers many of these new AI tools, and it's vital that this be led by the U.S.

Data is the lifeblood of artificial intelligence. These systems learn from processing vast amounts of data.

As we think about how to protect people's data privacy, we need to be considering first and foremost how this data is collected, how it was meant to be used, and ensure it is secured.

It's time that we provide people with greater transparency and put them back in control over the collection and use of their personal information.

Key to this is ensuring the safety of the algorithms used by online platforms, which serve as the instruction manuals for artificial intelligence.

By making sure algorithms are being developed, operated, and "training" AI responsibly...

...we can provide Americans with greater transparency for how their data is analyzed...

...how these systems identify patterns, how they make predictions...

... and how their interactions with online platforms are used to determine what content they see.

Put simply, trustworthy algorithms are essential components in the responsible deployment of AI.

Failing to enact a national data privacy standard, or allowing China to lead the way, heightens the risk for the over collection and misuse of data, unauthorized access and transfers, and greater harms for Americans and our families.

We need to prioritize strengthening data security protections to safeguard people's information against threats.

The theft and exploitation of sensitive information, especially biometric data, pose severe risks to individuals and organizations.

Even if we establish stronger data privacy protections for Americans...

...without equally robust data security requirements alongside those rules on collection and use, the number of data breaches and abuses will continue to rise and compromise people's information.

Building those laws early will ensure greater public trust in AI, which will help ensure future innovations are made in the U.S.

To ensure American leadership, we must strike the right balance with AI, one that gives businesses the flexibility to remain agile as they develop these cutting-edge technologies...

...while also ensuring the responsible use of this new technology.

A national standard for the collection and handling of data will provide businesses, creators, and every American with clear and understandable protections wherever they are.

I look forward to discussing the path forward today and I yield back.