Welcome everyone to what I hope will be a productive, fact-finding hearing on the current state of the data broker ecosystem.

It is obvious from the testimony that a staggering amount of information is collected on Americans, every day, frequently without their knowledge or consent.

This data then gets shared, analyzed, combined with other data sets, bought and sold.

In some cases, this data is not even anonymized, meaning that is easy for bad actors to find deeply personal information on individuals such as their location, demographic data, and health information.

Some of these data brokers are companies that most people are familiar with, but others operate in the shadows, with many Americans

never knowing that they have collected, bought, or sold their data.

The Federal Trade Commission recently fined an online mental healthcare company, BetterHelp, $7.8 million for disclosing patients' personal health information to advertising platforms such as Facebook and Google without the users' consent.

Siphoning off private data of Americans on mobile apps is so incredibly easy, all a data broker has to do is pay an app developer a nominal fee to implant a program within the app that is designed to capture the data of all users.

Companies rely on these convoluted and unclear terms of service and privacy policy documents, knowing full well users will find it far too tedious to read them before unwittingly agreeing to have their sensitive data accessed by 3rd party strangers.

There is a complete lack of safeguards surrounding this data and I am particularly concerned with the implications that has on the sick, the elderly, the youth, and the military.

Recent research from Duke University has found data brokers, without any accountability, can freely collect and share Americans' private mental health data.

We have all heard about the national security concerns raised about the Chinese Communist Party-influenced Bytedance, the parent company of the Tik Tok video app operating in our country and collecting data on Americans while also having the ability to potentially manipulate American public opinion on any given subject.

Well, the current state of play in the data broker industry presents some of those same concerns.

According to what we will hear today from these our invited experts, data brokers gather, package, and advertise highly sensitive data on current and former members of the US military, posing privacy and safety risks to all servicemembers. This, in and of itself, could be considered a security risk if the data collected is identifiable.

By collecting and selling data at will, these companies put all Americans at risk.

I look forward to learning from our witnesses today more about how data brokers are collecting, packaging, and analyzing data on Americans and possible safeguards that should be explored.