Questions for the Record Responses:

1. What privacy protections exist in instances where surveillance technology, such as facial recognition cameras, are used in public spaces?

   A: When it comes to privacy protections, when surveillance technology like facial recognition technology is utilized in public spaces, Americans have no federal protections. At the state level, there are a multitude of regimes that attempt to put some guardrails in place, but they only apply to local law enforcement. However, there is no single comprehensive federal privacy law that directly governs how facial recognition is used in public spaces. Congressional efforts to do so to date have stalled out. While the Carpenter case at the Supreme Court affirmed some Fourth Amendment protections, it is also limited to the situations addressed in that case.

2. How are law enforcement and national security agencies making use of newly developed surveillance technologies? Which of these technologies are they using?

   A: When it comes to how law enforcement is leveraging newly developed surveillance technologies, there is a lot we simply don't know. Given the sheer amount of data that is collected, we imagine that intelligence agencies are leveraging AI and other software to sift through that information to acquire actionable intelligence. There has been reporting of Immigration and Customs Enforcement leveraging a tool provided by Zenilabs to monitor social media platforms to flag individuals for deportation. This is particularly alarming given the tens of millions of Americans who utilize social media daily, being needlessly subjected to 24/7 monitoring by their government. AI is an incredibly powerful tool that can help law enforcement with their mission, but it is also a developing technology, prone to bias and hallucination, so it is important that there is oversight in its use by government agencies to ensure that civil liberties are being protected.

3. Do law-abiding American citizens have an option to protect their personal data, such as phone records or location data, private from third party data broker transactions?

   A: To reiterate from a previous answer, it depends on where the individual lives. Privacy laws currently are a patchwork across the states. Often, they conflict with each other. In our view, this only reinforces the need for a clear federal privacy law that can set a uniform approach to privacy for consumers around the country. It is worth noting that in a commercial sense, this data can be helpful for connecting Americans to potential goods and services they may be interested in. However, the problem arises when the government can buy that information, surveil its own citizens, and use its monopoly on force to undermine core constitutional protections. Additionally, we believe it is important to place limitations on the ability of federal agencies to simply purchase data to circumvent Americans' 4th Amendment rights in this surveillance context.