United States Senate
WASHINGTON, DC 20510-0908

March 29, 2022

The Honorable Antony Blinken
Secretary
U.S. Department of State
2201 C Street NW
Washington, D.C. 20522

The Honorable Lloyd Austin
Secretary
U.S. Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301

The Honorable Gary Gensler
Chairman
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Dear Secretaries Blinken and Austin and Chairman Gensler:

We write to express our concern with the risk posed by the Chinese Communist Party's (CCP) control over a rapidly growing number of technology companies and the sensitive data that these companies collect when operating outside of the People's Republic of China (PRC). The CCP's ability to exploit this data poses an immediate threat to U.S. national security, the stability and sovereignty of our allies and partners, and the defense of democracy and human rights around the world.

For the past several years, the CCP has worked steadily to build an expansive legal framework that explicitly requires any Chinese company, even nominally privately-owned ones, that collects sensitive data to turn it over to Beijing's intelligence agencies and security services on demand. This explicit legal requirement, repeated throughout the PRC's national intelligence, national security, counter-terrorism, cybersecurity, and data security laws, means that Chinese technology companies operating abroad pose serious risks to other countries' national security and sovereignty, as well as their individual citizens' privacy and safety.

Today, the risk has become even more acute. In its 2021 annual report, the bipartisan, bicameral U.S.-China Economic and Security Review Commission described how the CCP is contemplating requiring Chinese companies "to hand over management of their data to third-party Chinese information security firms … allow[ing] the information security firms, likely to be backed by China's government, to monitor Chinese companies' data." The Commission also noted that "[t]he Chinese government's efforts to gain control over data are leading it to assume greater ownership stakes in nonstate firms."

The risk extends far beyond the handful of 5G network, surveillance camera, and social media companies that have received the overwhelming majority of attention to date. Didi Chuxing, a ride-hailing platform with concerning links to the CCP, provides the most recent and high-profile example of just how pervasive the risk has become. Didi, which operates its ride-

hailing platform in 17 countries beyond China, including key allies and partners such as Australia, New Zealand, Japan, Mexico, Colombia, and Brazil, is preparing to soon begin operations in the United Kingdom and across the European Union. Wherever Didi operates, it collects large amounts of highly sensitive data on who is traveling, at which times, and along which routes. The collection of data is concerning as it allows for the identification and surveillance of individuals that the CCP perceives as its enemies – independent journalists, human rights activists, private businesspeople, or anyone promoting a message contradicting the CCP's carefully-crafted propaganda.

Recent news suggests that the CCP is now making efforts to exercise their legal claim to data collected by Didi. Ministry of State Security intelligence agents are now stationed inside of Didi's offices with direct access to this data. The company is also reportedly in talks to turn over all its data to a state-controlled third party and to grant Beijing a direct ownership stake with board representation and special governance rights over the data that Didi collects. Didi is further demonstrating its use as a political tool of the CCP by its most recent actions in Russia. On February 21, Didi had announced it would leave the Russian market citing market challenges. After Putin's invasion of Ukraine on February 24, Didi changed course, making an announcement on February 26 that the company would remain active in the country. This is clearly a political not an economic decision, undermining claims the company is simply a private business not beholden to the Chinese Communist Party.

With these deeply concerning facts in mind, we ask you to address the threat posed to our national security by China's access to the sensitive data collected by companies like Didi. We urge the U.S. Department of Defense and the U.S. Department of State to enact a global prohibition on U.S. military personnel and diplomats from using digital transportation platforms that collect users' personal information and sensitive geo-location data and are obligated to share that data with Beijing's intelligence and security services. We also urge the Department of State to update its travel advisories to U.S. citizens traveling to countries in which any such digital transportation platform operates, especially where these platforms may be operating under a different local brand from their parent company. We also urge the Securities and Exchange Commission to ensure that issuers on U.S. exchanges fully disclose their legal obligation to assist Beijing's intelligence agencies and security services. We also urge that any future SEC rulemaking or guidance on environmental, social, and governance reporting requires companies to fully report any such legal obligations to assist Beijing's intelligence agencies and security services, given these entities' extensive record of human rights abuses and repression both inside and outside of the PRC.

We thank you in advance for your attention to this matter.

Sincerely,

Marco Rubio
U.S. Senator

Todd Young
U.S. Senator