SMART NEWS & RESEARCH FOR LATIN AMERICA'S CHANGEMAKERS

DiDi and the Risks of Expanding Chinese E-Commerce in Latin America

Evan Ellis | September 2, 2021
Global Americans Contributor

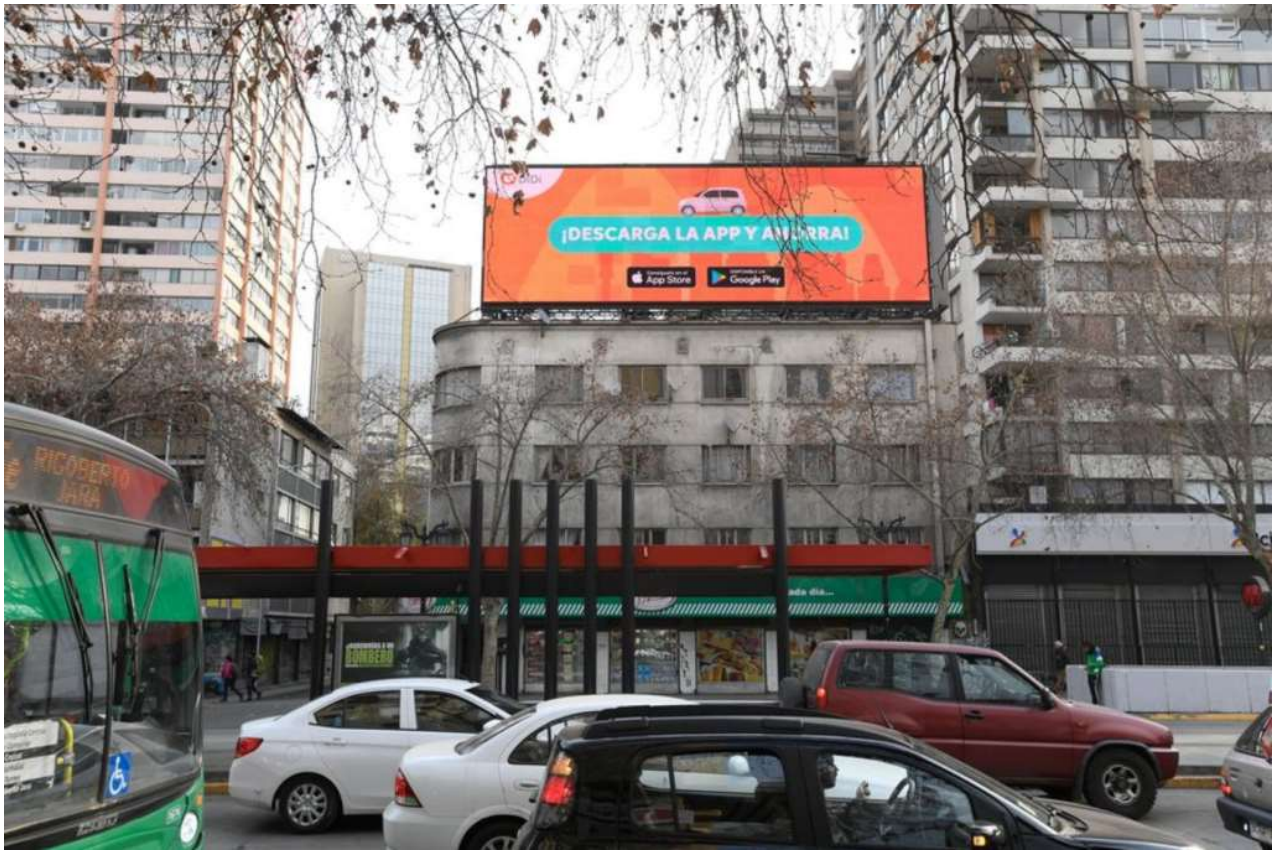

Photo Source: Jorge Villegas

Note: This article was originally published in Spanish in Infobae. To read the original version, please click here.

In July 2021, Chinese regulators launched a cybersecurity review of the ride-share company DiDi Chuxing, entering its offices to conduct inspections and removing its app from digital marketplaces in the country. The action resembled the government's November 2021 blocking of an Initial Public Offering (IPO) by Chinese billionaire Jack Ma's Ant Group; both appear to be moves by Xi Jinping, President of the People's Republic of China (PRC) and General Secretary of the Chinese Communist Party, against increasingly powerful tech giants who could potentially threaten his power. By July 2021, the Chinese government was imposing increased controls across a range of e-commerce firms. Evidence soon emerged that some of Xi's prospective rivals possibly stood to benefit from the Ant IPO,

suggesting that the action against DiDi may indeed have had a political motivation. At the same time, the fact that DiDi collects data on on hundreds of millions of users within China, including business and party officials, highlights how it could present a threat to the state's control of information and monopoly on exploitable intelligence.

Yet such actions also help the Chinese government exploit the opportunity that domestic e-commerce firms theoretically pose to its hegemony within China's borders. Increasingly globally engaged information technology entities like Ant, Tencent, and DiDi manage data and economic power that the Chinese Communist Party, much to its consternation, can at this moment not totally control; but if they and the data they collect in their increasingly ubiquitous *internationa*l operations are brought solidly under state control, they will become powerful weapons for advancing China's strategic commercial, political and other objectives abroad. In August 2021, the Chinese government passed a sweeping "data privacy" law, applicable to a broad range of data collected by Chinese technology firms, from ride-sharing apps to internet and surveillance systems. (Despite its name, this law did not ensure the absolute privacy of user data, but rather ensured that such data would be under the control of trusted agents of the Chinese state, rather than of private technology firms.) Also in August, DiDi was talking of ceding control of its collected user data to a third-party company with strong ties to the Chinese state. Moreover, both the actions against DiDi, and the law regarding the collection of data from Chinese users in China highlighted that the same companies, using the same technologies, are also collecting data through their operations abroad on foreign government, business, and other populations, equally sensitive and valuable, which would now be even more readily accessible to the Chinese state.

Increasing concern in the United Kingdom and the European Union over the vulnerability of their own citizens' user data, underscored by the

Chinese government's attempt to muscle DiDi, forced the Chinese ride-share company to postpone important expansion plans in Europe.

In Latin America, as of November 2020, DiDi operates in Argentina, Brazil, Chile, Panama, Colombia, Costa Rica, the Dominican Republic, Ecuador, Mexico, Panama, and Peru, among other countries. Prior to the COVID-19 pandemic, it was expanding aggressively, having captured half of the region's ride-share market by November 2020, with over one billion total rides provided. In Brazil alone, DiDi has 600,000 registered drivers.

For Latin American governments and consumers, as well as for the United States and other global actors, therefore, the question of DiDi Chuxing and the expanding presence of Chinese e-commerce companies in general is particularly urgent.

U.S. officials from the administration of President Joe Biden and Congressional leaders have focused much attention on the risk of participation by Chinese companies such as Huawei in telecommunications infrastructure, especially as the number of internet-using devices and their associated data is multiplied with the deployment of 5G technology and the "Internet of Things" (IOT). Similarly, there has been increasing attention paid to the risks posed by the global spread of surveillance systems and "smart cities" technologies built by Chinese firms using Chinese components. Such systems potentially allow Chinese

intelligence services to access data regarding the movements, bank and credit accounts, and other sensitive information of government and commercial elites wherever those systems are deployed. Such vulnerable networks include ECU-911 in Ecuador, BOL-110 in Bolivia, Uruguay's border surveillance infrastructure, the security apparatus installed at the Colón Free Trade Zone in Panama, and even thermal cameras donated by China to help governments identify infected persons during the COVID-19 pandemic.

The clearest demonstration of the intent and ability of the Chinese state to use the overseas information architectures built or accessible by its companies to collect data on targets of interest is the 2017 National Intelligence Law, which obliges Chinese firms to turn over material deemed important to state security to the government. Such coercive legal power over companies easily reachable by Chinese authorities obviates assurances by companies like Huawei that they would never turn over user data. The law does not only apply to telecommunications and surveillance firms, however, but to all companies able to access data of potential security relevance to the Chinese state. These include a broad range of PRC-based e-commerce companies, including the ride-share firm DiDi.

Precisely because ride-share trips capture data from both the driver and customer, they are considered more secure than common taxis against certain types of robbery, and are thus popular among precisely the types of people of most interest to the Chinese intelligence services (Ministry of State Security (MSS)): white-collar business and government personnel traveling to and from meetings. Acquiring ride-share data from multiple travelers, and multiple trips over time, it is not difficult to identify important government and commercial meetings (yielding both commercial and other intelligence), as well as improper liaisons (providing blackmail opportunities for obtaining future intelligence data, or "favors").

The risk posed by DiDi is only the tip of the iceberg, as PRC-based companies expand their reach in the e-commerce space as part of the expansion of China's "Digital Silk Road." While their presence remains limited in Latin America and the West compared to established players like Amazon, PRC-based companies, once fully subordinated to the Chinese state, potentially provide China's MSS unfettered access to the spending habits and sensitive data of countless persons of interest. "Business-to-business" (B2B) platforms could similarly be used to obtain technical data and information on competitor bids or vulnerabilities as Chinese firms continue their global expansion. The PRC roll-out of the Digital RNB, just in time for Beijing's Winter Olympics in February 2022, will further broaden such risks.

The vulnerabilities that arise from China's expanding global position in e-commerce are not limited to transport, commercial and financial data. The espionage scandal associated with the Israeli company NSO and its Pegasus software highlights how sophisticated hackers can exploit trusted software on user devices to access a broad range of data. Yet the resources available for NSO to develop Pegasus pales in comparison to those available to the Chinese state. Moreover, China's MSS itself has been subject to investigation by the U.S. Department of Justice regarding its patronage of cybercriminals, as well as cyber-espionage against commercial and government targets.

Washington, its partners, and the Western private sector need to pay more attention to the threat posed by the growing presence of Chinese firms in the e-commerce market, and its potential to support China's commercial (as well as political and military) advances. The challenge is far broader than that presented by Huawei and 5G. Moreover, China's assertion of control over its e-commerce companies deserves more attention as a potential preliminary step to its ability to access the informational fruits of their expanding global presence. Washington must do more to show its

partners in Latin America and elsewhere how the expanding Chinese presence threatens their own sovereignty and the security of investors in locating their core intellectual property in countries with vulnerable information and e-commerce architectures. The consequences of failure will be borne most by those who dismiss such dangers as mere "great power competition" in which they compromise their future development and autonomy by closing their eyes to avoid turning away Chinese money.

R. Evan Ellis *is a Latin America Research Professor with the U.S. Army War College Strategic Studies Institute.*

Related Posts

Chinese Surveillance Complex Advancing in Latin America

The installation of Chinese surveillance systems, acquired through PRC government donations or commercial contracts, is...

Russian Influence in Latin America

As 2015 unfolded, one-by-one Russia's principal political supporters in Latin America and the Caribbean entered...

Chinese engagement in Latin America and the U.S. response: taking off the gloves?

China has sought a bigger role overseas, seemingly seeking to wean the region off of...

Filed Under: Asia & Latin America, Economics, Trade & Development

Tagged With: 5G, Brazil, China, data privacy, DiDi Chuxing, E-commerce, Huawei, Xi Jinping

Menu