Royal United Services Institute
for Defence and Security Studies

EMERGING INSIGHTS

How Ride-Share Apps Collect and Store Data: A National Security Risk?

Elisabeth Braw with Franco Palazzolo

ACKNOWLEDGEMENTS

The author would like to thank Malcolm Chalmers and two peer reviewers for their comments on earlier versions. This paper was commissioned by the Albright Stonebridge Group through funding from Bolt. The funder had no involvement in the research, writing or peer review process of this paper.

EXECUTIVE SUMMARY

Concerns about ride-share companies have largely focused on physical risks to passengers. However, ride-share apps collect enormous amounts of data – a fact which has so far received minimal attention. This data includes ride details, address books and search history, with some apps also tracking the riders after they leave the car.

This raises concerns about how the data is stored and managed. The most obvious concern is that hackers can gain access to it. More serious, however, is the threat that authoritarian governments can demand access to the data to, for example, track specific citizens or groups in other countries. China poses a particular concern, as its new Personal Information Protection Law gives the government significant power over data collected by Chinese companies. This paper explores the emerging security threats from ride-share data collection and provides suggestions for further areas of enquiry.

INTRODUCTION

The ride-sharing industry is booming. Led by Uber, app-based taxi services featuring drivers using their own cars grew from transporting just a small number of passengers in 2012 to nearly 4 billion in 2018.[1] The following year, Goldman Sachs declared 'new mobility' to be 'a massive long term opportunity',[2] predicting 'global ride-hailing miles to expand at a 5-year CAGR [Compound Annual Growth Rate] of 15% vs. personal vehicles at +2% over the same period'.[3] By October 2021, the global ride-share market had reached $117.34 billion in size.[4] Uber has been joined by numerous similar app-based providers of varying size and geographical reach.

Like most apps, ride-share apps collect a considerable amount of data from their users. To date, however, the public discussion around ride-share apps has primarily been focused on the physical risks associated with having ordinary people chauffeur fellow citizens in their private cars, not on the

[1] Union of Concerned Scientists, 'Ride-Hailing's Climate Risks', 2020.

[2] Goldman Sachs, 'The Future of Mobility', 4 June 2019, p. 4.

[3] *Ibid*.

[4] Statista, 'Ride-Sharing Market Size Worldwide in 2020 and 2021', <https://www.statista.com/statistics/1155981/ride-sharing-market-size-worldwide/>, accessed 23 November 2021.

considerable amount of user data ride-share apps can collect. Indeed, considering the limited governance of ride-share apps' treatment of user data, the situation has created an anarchic environment where riders have no way of knowing how their data is stored and who has access to it. The issue of personal data collected on apps was recognised as a national security challenge in 2019, when the Committee on Foreign Investment in the United States reversed the acquisition of dating app Grindr by the Chinese firm Beijing Kunlun on account of national security risks.[5] In 2019, the Indian government banned TikTok and 58 other Chinese apps after it gave them a 'chance to explain their position on compliance with privacy and security requirements' and was not satisfied by their policies.[6]

This Emerging Insights paper provides an initial exploration of how ride-share companies collect and store user data, and the potential implications for national security. To date, there are no comprehensive studies on ride-hailing companies' collection and treatment of user data. Indeed, like all app-based businesses, the ride-hailing industry is still evolving, with new players constantly entering the market and governments struggling to decide how to treat the industry. This paper, therefore, aims to provide early insights into ride-hailing apps' data use and outline a basis for future research. The paper is based on an initial review of corporate filings, statements and the privacy policies of a selection of firms (mainly those already active in Europe and North America). The author also consulted a number of independent experts in the technology and automotive industries. The paper first briefly examines the history of ride-hailing apps. It then explores how data is currently used and the extent to which it is accessed by governments, and assesses the potential for governments to more systematically access and exploit such data. Finally, the paper evaluates the degree to which this poses a national security risk.

BACKGROUND

In September 2021, Uber reported that predicted gross bookings between July and September 2021 would reach between $22.8 and $23.2 billion.[7] That constitutes explosive growth for an industry that did not exist 12 years ago. Uber was created in March 2009 and produced cheaper rides than conventional taxi-cabs, with a more convenient booking system. It circumvented the regulated but sometimes mediocre taxi-cab market then dominant in the US. Other ride-share firms were soon launched,

[5] Carl O'Donnell, Liana Baker and Echo Wang, 'Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App', *Reuters*, 27 March 2019.

[6] *Nikkei Asia*, 'India Permanently Bans TikTok and 58 Other Chinese Apps', 26 January 2021.

[7] Dave Lee, 'Uber on Course to Post First Profitable Quarter', *Financial Times*, 21 September 2021.

including Lyft (2012) in the US and Canada and China's DiDi Kuaidi (now DiDi Chuxing, 2012).[8]

However, the physical risks involved[9] in catching a ride from a driver lacking thorough vetting or certified skills – and the risks to pedestrians posed by such drivers – quickly became a key concern. For example, a 2019 study found the introduction of ride-sharing apps had increased US traffic fatalities by 3% between 2010 and 2016.[10]

In recent years, companies have made significant efforts to improve riders' physical safety.[11] However, physical issues have obscured data-collection problems.

CUSTOMER DATA COLLECTION

Data collection by apps and websites has triggered government action in recent years. The EU has taken a lead role in trying to rein in the collection of consumer data. As a result of GDPR, which applies to EU citizens' internet use anywhere in the world, users can choose not to have their data shared with other companies. GDPR limits ride-sharing companies' data collection in the same way it does other apps' and websites' data-harvesting. When launching GDPR, the European Commission said that 'a car-sharing service may request a user's name, address, credit card number, and potentially whether the person has a disability, but can't require a user to share their race'.[12] GDPR does not, however, ban apps from collecting other data.

Uber collects data on users' purchases, contact information and search history and tracks them and receives data on its users from commercial partners.[13] Lyft collects data including users' purchases, financial information, location, contact information, user content and search history. DiDi also collects details from its users' social media accounts, as well as users' albums, contact lists and digital devices. It also tracks users and records audio and video of drivers and passengers.[14] BlaBlaCar, which focuses on the French market

[8] Uber owns a 12% stake in DiDi, having acquired it in 2016 when Uber sold its Chinese business to DiDi in exchange for equity in DiDi. See Ari Levy, 'Uber's Stake in Didi Shrank by $2 Billion This Week Amid China Crackdown on U.S. Listings', *CNBC*, 23 July 2021.

[9] Nick Statt, 'Uber's First Ever Safety Report Discloses 3,045 Sexual Assaults and Nine Murders in the US Last Year', *The Verge*, 5 December 2019.

[10] John Barrios and Hanyi Livia Yi, 'The Cost of Convenience: Ridesharing and Traffic Fatalities', BFI Working Paper, No. 2018–80, Becker Friedman Institute, p. 4.

[11] Steve Dent, 'Uber Unveils Much-Needed Passenger Safety Features', *engadget*, 12 April 2018.

[12] Nitasha Tiku, 'Europe's New Privacy Law Will Change the Web, and More', *Wired*, 19 March 2018.

[13] See Annex for more details on data-collection methods and policies.

[14] Rosie Perper, 'China's Largest Ride-Hailing Company Is Now Recording In-Car Audio During Passenger Trips', *Business Insider*, 13 September 2018.

and car-pooling as opposed to a taxi-like arrangement, collects less data but requests mini-biographies from its users. Ola Cabs, a Bangalore-based company whose app offers rides in India, the UK, Australia and New Zealand, collects similar data to Uber and Lyft, and like Uber it tracks its users.

Ride-hailing companies have thus amassed huge amounts of data, which they can analyse. For example, DiDi knows 'what times people in certain cities finish work, or which employers have the longest work hours. Didi also equips cars with cameras monitoring road conditions, and what is happening in the car, collecting data on 100 billion kilometres of Chinese roads per year'.[15] In July 2021, the Cyberspace Administration of China ordered DiDi to stop enrolling new users on the grounds that DiDi had 'illegally collected users' personal data'.[16] The Chinese government's sudden intervention – the first of this kind[17] – caused DiDi to suspend its planned expansion in Europe, where it had wanted to, for example, set itself up in several British cities.[18] In August 2021, news media reported that DiDi was in talks with Westone, a Chinese state-owned information security firm, to handle its data-management and monitoring activities.[19] In November 2021, it was reported that DiDi was about to relaunch its app in China;[20] as of the end of November 2021 the DiDi Rider app is available on the App Store.

While the Chinese government itself collects an enormous amount of citizen data through CCTV and facial-recognition cameras, the regulatory crackdown is part of a broader effort to assert state power over the country's largest and most successful technology companies.[21] Indeed, Alibaba has been reprimanded for its approach to consumer privacy.[22] In September 2021, it also emerged that the Chinese government had plans to force Alibaba's parent company Ant Group to turn over Alipay's considerable financial data 'to a new and separate credit scoring joint-venture that would be partly state-

[15] Josh Horwitz and Yilei Sun, 'Explainer: What Is Driving China's Clampdown on Didi and Data Security?', *Reuters*, 7 July 2021.

[16] Vincent Ni, 'Didi Ride-Hailing Service Pulled from App Stores in China', *The Guardian*, 5 July 2021.

[17] Hunter Dorwart and Gabriela Zanfir-Fortuna, 'Spotlight on the Emerging Chinese Data Protection Framework: Lessons Learned from the Unprecedented Investigation of Didi Chuxing', Future of Privacy Forum, 23 June 2021.

[18] Amy Thomson and Ivan Levingston, 'China Ride-Hailing Giant Didi Puts Europe Expansion on Hold', *Bloomberg*, 23 August 2021.

[19] Julie Zhu, 'Didi in Talks with State-Backed Westone to Hand Over Data Control-Sources', *Reuters*, 6 August 2021.

[20] Julie Zhu and Yilei Sun, 'Didi Prepares to Relaunch Apps in China, Anticipates Data Probe Will End Soon – Sources', *Nasdaq,* 11 November 2021.

[21] Hiroshi Murayama, 'China's Tech Crackdown Widens to Tencent from Alibaba', *Reuters*, 8 August 2021.

[22] *Reuters*, 'Factbox: China Crackdown Wipes Hundreds of Billions off Top Companies' Values', 16 September 2021.

owned'.[23] This suggests the Chinese government is trying to gain access to the enormous amounts of data companies possess. The potential for this sort of state control over consumer data is significant for any discussion about ride-share apps.

Even in liberal democracies, citizens' constant use of apps today means they are persistently being monitored. 'Israeli intelligence used to be the most sophisticated when it came to having a complete mapping of people's details. Today, technology means it's far from being alone', noted a leading automobile industry academic.[24] Data collection, he continued, allows companies 'to build a profile of you thanks to the access users give them. A while ago I spoke with the CIO of a ride-sharing company that has since gone bust. It specialised in rides for several people per car. He described how every time a person hailed a ride the company's algorithm computed several thousand options before it would optimally allocate the car/van with the commuter and their sequence in pick-up and drop-off. For example, the user behaviour algorithm could calculate that if a woman was likely to wear high heels, a 30 metre walk to the nearest intersection for a pick-up may be tolerable, but perhaps not 75 metres. These apps seek to know more than you realise'.[25] Indeed, 'if riders don't turn off location access after completing their rides the app could potentially track and collect data around the clock on where the user is, where they go, and, sometimes, even how long they stay there'.[26]

Citizens' constant use of apps today means they are persistently being monitored

PRIVACY POLICIES AND DATA USE

The fact that a great amount of personal data is collected makes it vital to know how the information is collected and used, especially given the personal nature of ride-sharing data.[27] In 2014, it emerged that Uber had a tool labelled God View, which allowed employees to track specific drivers and riders in real time.[28] In 2018, Lyft launched an investigation after allegations that employees had used app data to track current or former significant others and to track attractive people they had met on shared rides.[29] In

[23] Sun Yu and Ryan McMorrow, 'Beijing to Break Up Ant's Alipay and Force Creation of Separate Loans App', *Financial Times*, 13 September 2021.

[24] Venkat Sumantran, Charles Fine and David Gonsalvez, *Faster, Smarter, Greener: The Future of the Car and Urban Mobility* (Cambridge, MA: MIT Press, 2018).

[25] Author online interview with automotive industry executive and academic, 29 September 2021.

[26] Norton, 'How Ridesharing Services Can Take Your Privacy for a Ride', <https://us.norton.com/internetsecurity-privacy-ridesharing-privacy-ride.html>, accessed 17 November.

[27] Shahid Buttar, 'Principles for Corporate Platforms in the Gig Economy', Electronic Frontier Foundation, 7 November 2018.

[28] Johana Bhuiyan and Charlie Warzel, '"God View": Uber Investigates its Top New York Executive for Privacy Violations', *Buzzfeed*, 18 November 2014.

[29] Stephen Edelstein, 'Lyft Investigates Claim That Employees Improperly Accessed Customer Data', *The Drive*, 26 January 2018.

2020, it emerged that a flaw in Uber's Jump electric scooters allowed people to track users in real time.[30]

Uber shares data with, among others, subsidiaries, business partners and research firms. DiDi shares details with commercial partners, as do BlaBlaCar and Ola. There is, however, a difference in how much data ride-share apps share with governments. This issue is discussed in a following section of this paper.

Much of the large amount of user data collected by ride-sharing apps (such as social media contacts) is not necessary for the functioning of the app. 'Ride-share apps are like utilities – they're part of our daily lives. But they're not regulated like utilities. In the past your daily life took place within one country and was regulated there', a leading technology lawyer noted.[31] Indeed, it is unclear where apps' data is stored, as this is a decision made by each company. In its 2019 Securities and Exchange Commission (SEC) filing, for example, Uber explained that it uses 'a combination of third-party cloud computing services and co-located data centers in the United States and abroad. We do not control the physical operation of any of the co-located data centers we use or the operations of our third-party service providers'.[32] In a 2019 SEC filing, Lyft described the threats, such as cyber attacks, facing its data-storage facilities, but did not explain where they are located or whose data they host.[33] In a 2021 SEC filing, Xiaoju Kuaizhi Inc (the name under which DiDi submitted its filing) likewise described its efforts to protect data against cyber intrusion, but did not say where its data is stored.[34] This matters because, in the case of DiDi, the Chinese government could request access to individual or specific data in a way that is not possible in Western countries.

Because there is no global regulatory framework for ride-sharing data use, companies can disseminate the data as they wish, as long as users agree, which they do by signing up with the app. Indeed, at the moment the collection and use of app users' data could be described as a free-for-all. GDPR has become a global data-collection standard for websites. But with

[30] Issie Lapowsky, 'Uber Flaw Let Anyone Track Scooter Trips in US Cities', *protocol*, 5 March 2020.

[31] Author online interview with technology lawyer, 4 October 2021.

[32] US Securities and Exchange Commission, 'Form S-1 Registration Statement Under the Securities Act of 1933, Uber Technologies, Inc', 1 April 2019, p. 48, <https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm>, accessed 23 November 2021.

[33] US Securities and Exchange Commission, 'Form S-1 Registration Statement Under the Securities Act of 1933, Lyft, Inc.', 1 March 2019, p. 34, <https://www.sec.gov/Archives/edgar/data/1759509/000119312519059849/d633517ds1.htm>, accessed 23 November 2021.

[34] US Securities and Exchange Commission, 'Form S-1 Registration Statement Under the Securities Act of 1933, Xiaoju Kuaizhi, Inc.', 10 June 2021, p. 27, <https://www.sec.gov/Archives/edgar/data/1764757/000104746921001194/a2243272zf-1.htm>, accessed 23 November 2021

apps, users can merely ask the app not to track. They cannot ask the app not to collect the data they continuously feed into the app. Indeed, while the US and other countries have a range of policies relating to data protection, these primarily concern the safekeeping of data, not its initial collection.[35] This may be because it is extremely difficult to formulate laws that specify what data collection should be allowed within the dynamic internet economy. The California Consumer Protection Act (CCPA) comes closest to protecting consumer data. Even the CCPA, however, only allows consumers to ask companies which personal data they collect, and to request that the data not be sold.[36]

THE POTENTIAL FOR ABUSE

While there have so far been no major movements against ride-sharing apps' collection of data, other companies such as Facebook have come under enormous scrutiny for the amount of user data they collect and how they use this data to influence customers. During the 2016 US election campaign, Russia bought Facebook ads that targeted LGBT voters, Evangelical Christians, and those interested in the Black Panthers.[37] These ads appeared in users' feeds based on algorithmic analysis of those users' personal data.

The collection of significant amounts of data from every ride-share user, and the fact that the ride-share industry is booming, raises an important question: who – beyond companies trading user data with one another – might get access to this 21st-century gold?

In applying the whip to DiDi in summer 2021, the Chinese government told the company to stop accepting new customers, which resulted in DiDi quickly losing more than half of its value soon after its initial public offering in the US.[38] Beijing highlighted the risk of the US government accessing Chinese users' data via DiDi servers in the US as a reason for its actions, even though DiDi said it was 'impossible' for Chinese users' data to be accessed by US authorities.[39] In Western countries, including the US, the UK and EU member states, law enforcement agencies can request data from ride-share companies. In the UK, for example, Uber complied with around 2,000 police requests for data in 2019.[40] Indeed, ride-share apps operating in Europe

[35] DLA Piper, 'Data Protection Laws of the World', last updated 28 January 2021, <https://www.dlapiperdataprotection.com/?t=law&c=US>, accessed 19 November 2021.

[36] State of California Department of Justice, 'California Consumer Privacy Act (CCPA)', <https://oag.ca.gov/privacy/ccpa>, accessed 17 November 2021.

[37] Scott Shane, 'These Are the Ads Russia Bought on Facebook in 2016', *New York Times*, 1 November 2017.

[38] Ethan Wu, 'Didi Has Fallen a Stunning 52% Since its US IPO as China's Crackdown Pummels the Ride-Hail Giant', *Markets Insider*, 23 July 2021.

[39] Horwitz and Sun, 'Explainer'.

[40] Christopher Carey, 'Concerns Raised Over Uber's Data Sharing with UK Police', *Cities Today*, 23 September 2020.

and North America comply with the vast majority of subpoenas.[41] This is unsurprising, as individuals and companies are obliged to cooperate with law enforcement agencies if presented with such orders, and the availability of app data can significantly aid police investigations.

Furthermore, counterterrorism legislation allows the surveillance of suspected terrorists.[42] The USA PATRIOT Act 2001, for example, allows the US government to access documents held by third parties.[43] However, because courts oversee terrorism investigations there is far less risk in liberal democracies of authorities abusing app data.

Authorities in Western countries do, however, increasingly request mobility data for traffic-planning purposes.[44] This has caused concern among some privacy advocates. In Los Angeles, a plan by the Los Angeles Department of Transportation to reduce congestion by collecting data from e-scooter firms ran into opposition from privacy advocates, and Uber, which seems to consider the move a form of hidden regulation.[45] In addition, the presence of enormous quantities of personal data creates a risk of criminal exploitation. Sophisticated criminal gangs – perhaps working in conjunction with disgruntled employees – could, for example, retrieve data and, using AI tools to sift through bulk data, blackmail or smear people. Data loss presents another risk as individuals and companies in charge of data storage may be careless. Uber's note to the SEC – 'we do not control the physical operation of any of the co-located data centers we use or the operations of our third-party service providers'[46] – highlights a responsibility gap that creates an opportunity for data theft or loss.

The presence of enormous quantities of personal data creates a risk of criminal exploitation

Personal data can also be used to track individuals and map group structures. In 2019, the Russian opposition activist Ivan Golunov was arrested on spurious charges, after police officers found him using data from Yandex. Taxi, a Russian ride-share app co-owned by Uber.[47] The risk of governments accessing data harvested by ride-share apps for nefarious purposes is particularly high in non-democracies. This does not mean that companies

[41] Uber, 'Guidelines for United States Law Enforcement', last updated 3 April 2021, <https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=guidelines-for-law-enforcement>, accessed 19 November 2021.

[42] 'USA PATRIOT Act 2001 (US)'.

[43] ACLU, 'Surveillance Under the USA/PATRIOT Act', <https://www.aclu.org/other/surveillance-under-usapatriot-act>, accessed 17 November 2021.

[44] *Automotive News*, 'Chelsey Colbert on New "Gold Standard" for Transportation Data Privacy', 17 October 2021.

[45] Scott Ikeda, 'Collection of Mobility Data by Los Angeles Government Sparks Creation of Privacy Coalition With a Surprising Leader: Uber', *CPO Magazine*, 20 March 2020.

[46] US Securities and Exchange Commission, 'Form S-1 Registration Statement Under the Securities Act of 1933, Uber Technologies, Inc.', p. 48.

[47] Gautama Mehta, 'Russian Rideshare App Yandex.Taxi Shares User Data with Police', *CodaStory*, 6 March 2020.

operating on digital platforms must stay away from countries that are not liberal democracies. The challenge of offering a service that an authoritarian regime may want to access does, however, put ride-share apps in a difficult position. For example, Uber operates in a range of semi-democratic and non-democratic countries including Egypt, El Salvador, Guatemala, Honduras, Morocco, Qatar and Russia. DiDi operates in Russia and Latin America, in addition to its Chinese home market, where leaked government documents show authorities have been monitoring the Uyghur minority by tracking their use of the Kafya Koran app.[48]

But exploitation of app data could involve the targeting of other countries' citizens as part of intelligence gathering or population monitoring. In an interview with the author, an automotive industry executive noted:

> We trust that the data apps collect will be used for its intended purposes. But gradually, with cumulative information like this, someone can build a detailed composite picture of each user. The reality is that users have no way of knowing how their data may be used. Potentially, a supermarket can send the user a discount coupon when the user is known to be in the vicinity. To some this may be a benefit but for many this could be unauthorised invasion of privacy. Furthermore, the potential for use of such data by authoritarian governments is a different matter. And it's very different to bestow trust in an authoritarian government that it will treat your user data with respect.[49]

The executive described the opportunities for authoritarian regimes intent on using ride-share data to monitor individuals or groups in other countries:

> The app has your personal information, your financial information such as a wallet and credit cards. And it has geographical information: where are you in the mornings, the evenings, and the places you frequent. If you go regularly to a favourite Starbucks, that's information they can use. But they can also learn whether a user is frequently dropped off near, say, a defence installation or a strip club. Or imagine, say, a Boeing engineer who regularly takes a ride-share car. They can figure out who else he's in contact with based on his rides, and from that they can figure out who he's seeing. The algorithms are so comprehensive that they can potentially capture such details.[50]

Writing a concurring opinion in a 2012 US Supreme Court case, Justice Sonia Sotomayor made a similar point: 'GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations'.[51] GPS and other satellite-navigation systems form the engine of ride-share apps, allowing drivers and riders to connect and conduct the trip, and allows the app to calculate the fare.

[48] Scilla Alecci, 'How China Targets Uighurs "One by One" for Using a Mobile App', International Consortium of Investigative Journalists, 24 November 2019.

[49] Author online interview with automotive industry executive, 29 September 2021.

[50] *Ibid.*

[51] Legal Information Center, 'United States v. Jones', <https://www.law.cornell.edu/supremecourt/text/10-1259#writing-10-1259_CONCUR_4>, accessed 17 November 2021.

This information makes ride-sharing apps a goldmine for intelligence. While some Western government agencies might want to access app data, the rule of law in liberal democracies stipulates that authorities can only request and receive data on individuals on the basis of subpoenas or search warrants, or in bulk for infrastructure purposes such as traffic planning.

Authoritarian governments, though, have far more significant opportunities, as their courts and legislatures are only formally independent and governments can impose their will on domestically based companies and even on foreign companies operating in their countries. In the US, there is such widespread concern that TikTok videos can be accessed by the Chinese government that the US armed forces have banned service members from using the app.[52] While TikTok says it does not share user data with Beijing, users and foreign governments have no way of confirming this, let alone preventing it from happening. As stated by a technology lawyer interviewed by the author, 'the reality is that today data flies across borders, and there's a lot of pressure on private companies to share data with the Chinese government'.[53]

Indeed, China's new Personal Information Protection Law (PIPL) – billed as a Chinese version of the GDPR and which came into effect on 1 November 2021[54] – asserts state power over data belonging to both Chinese and foreign companies. As lawyers with the international law firm Morgan Lewis noted, 'the PIPL exerts certain exterritorial jurisdiction over data processing activities that happen outside China if the purpose is to provide products or services to individuals located in China, or to analyze or assess the behaviors of individuals located in China'.[55]

On the basis of the PIPL, the Chinese government can force Chinese and other companies to turn over their data as soon as it involves any Chinese citizens. According to the technology lawyer, 'the PIPL is like a legal landgrab. The Chinese government says it wants to ascertain the safety of Chinese citizens' data, but you can't compartmentalise Chinese citizens' data, so China gets access to all the data. The new legislation wasn't anticipated to be as strict as it turned out to be'.[56] Conversely, as the volume of app data continues to grow, potentially becoming the primary source of information about individuals, close intelligence allies, such as the Five Eyes countries, may begin to systematically share (legally obtained) data from servers based in their respective countries.

The PIPL follows the informal arrangement that has seen US technology giants, including Apple, turning over data to the Chinese authorities, despite the fact that doing so is prohibited under US law. Apple has circumvented the US ban

[52] Ben Kesling and Georgia Wells, 'US Military Bans TikTok Over Ties To China', *Wall Street Journal*, 3 January 2020.

[53] Author telephone interview with technology lawyer, 4 October 2021.

[54] Todd Liao et al., 'Personal Information Protection Law: China's GDPR Is Coming', Morgan Lewis, 24 August 2021.

[55] *Ibid*.

[56] Author telephone interview with technology lawyer, 4 October 2021.

by hosting Chinese customers' data on servers in China that are owned and run by a Chinese state-owned company.[57] 'Without separate servers like the ones Apple set up, people could sit in California uploading their information there and Beijing would have access to it', the technology lawyer pointed out.[58] Western companies creating separate servers in China can thus help protect Western users' data, even as it puts it out of the reach of authorities in Western countries. Indeed, against the background of the Chinese government asserting its power over domestic technology giants and even Western ones like Apple, lawyers have begun advising Western companies to separate their activities in China from the rest of their operations. China-based companies, meanwhile, would clearly struggle to do so.

While companies handing over user data to hostile states is already a major concern, it will grow more acute as the use of biometric data increases. According to the technology lawyer, 'We won't be using passwords that much longer, but will instead sign on with our faces. You can tell a great deal from people's faces, including their life expectancy'.[59]

Traditionally, intelligence services have kept persons of interest under physical surveillance. Today, the Chinese government's power over technology companies – especially domestic ones – means that it could, for example, use ride-share apps' wealth of data to gather information on members of government, the armed forces or private sector workers.

Indeed, in 2018, the US armed forces banned service members in conflict zones from using GPS software on smartphones, watches and fitness bands, after data collected by the fitness app Strava revealed the exercise routes of soldiers at US military bases around the world, including Syria, Iraq and Afghanistan.[60] Strava had, in fact, inadvertently revealed the bases' locations by publishing 'heat maps' of its users' activity.[61] In October 2021, members of the US Congress wrote an open letter to the Biden administration, noting that while DiDi is not yet available in the US, US government personnel in countries where it is available should be banned from using it for much the same reason: 'Given the aggressive nature of the PRC Government's espionage tactics, and the general heightened danger towards U.S. officials overseas with new threats arising over recent years, it is imperative that we get ahead of these potentially devastating risks to national security'.[62]

The espionage potential of ride-share apps is clear:

[57] Jack Nicas, 'Apple's Compromises in China: 5 Takeaways', *New York Times*, 17 May 2021.

[58] Author telephone interview with technology lawyer, 4 October 2021.

[59] *Ibid*.

[60] Thomas Gibbons-Neff, 'Pentagon Cracks Down on GPS Software on Devices in Combat Zones', *New York Times*, 6 August 2018.

[61] *BBC News*, 'Fitness App Strava Lights up Staff at Military Bases', 29 January 2018.

[62] Anthony Gonzalez et al., 26 October 2021, <https://twitter.com/RepAGonzalez/status/1453822126272700421?s=20>, accessed 23 November 2021.

> Say you go to a foreign capital for meetings. Those meetings could be identified based on where the car-share car drops you off. And considering that many ride-share companies now record conversations between the driver and the passenger, if an intelligence agency wanted to record your conversations you might have with contacts while riding in the car they'd be able to do that too.[63]

This threat is heightened by public transport agencies potentially shutting some late-night services to incentivise passengers to use ride-share services during those times, as the Washington Metro did in 2016.[64] Ride-share app data could also be used for hostile-state monitoring of social behaviours. Consider the public's reaction to various contingencies: power cuts or terrorist attacks, for example. With access to ride-share data, a state could study the reaction of different parts of a population (grouped by gender, age or place of work, for example). In the hands of a hostile government, such data could be useful in the planning of cyber or hybrid attacks, especially on critical infrastructure.

Furthermore, ride-share users' personal information and contact details would be a useful tool for hostile states designing a disinformation campaign to cause confusion or discord in a target country. This is another advantage authoritarian regimes have. It is very difficult to imagine a situation where Western governments could force popular apps based in China, Russia or other authoritarian countries to share their users' data and use it to target them with disinformation. During the 2016 US presidential election, Russia demonstrated – using Facebook's legal commercial tools – the opportunities available to hostile regimes wishing to disseminate misinformation and disinformation based on user data.[65]

KEY ISSUES FOR NATIONAL SECURITY RISK

The treatment of ride-share users' data is part of the 'convenience trap': the more convenient technology-aided life in liberal democracies becomes, the more vulnerable it makes society.[66] Even if governments consider specific apps a national security vulnerability because of the amount of data collected, they cannot force residents to stop using them.

[63] Author telephone interview with chief technology officer of global cyber intelligence company, 4 October 2021.

[64] Martine Powers, 'Should Metro Outsource Late-Night Service to Uber and Lyft?', *Washington Post*, 23 September 2016.

[65] US Senate Committee on Intelligence, 'Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 1: Russian Efforts Against Election Infrastructure with Additional Views', 2019, <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf>, accessed 23 November 2021.

[66] Elisabeth Braw, 'The Case for Joint Military–Industry Greyzone Exercises', *RUSI Briefing Papers*, 6 April 2021.

Instead, governments may want to consider the following:

- Is there potential to create globally binding rules, even weak ones, for ride-share apps' (and other companies) collection of user data?
- As a result of the PIPL, ride-share firms and other technology-heavy companies may need one system to collect data in the US, one in Europe and one in China. According to the technology lawyer interviewed by the author: 'We'll see Berlin Walls going up. There's a lot of fear in the market about this. It's going to be hugely expensive, and very logistically cumbersome. With one global system you can do lots of analytics; with lots of different datasets the analytics will be much more difficult'.[67] Should Western governments accelerate this trend through appropriate legislation? While separate data centres are very costly, they also help reduce national security risks linked to large-scale data collection.
- As China can now force foreign technology companies to turn over user data, do Western countries need new legislation to prevent these companies from doing so, especially if the companies do not establish separate data servers in China through which they can insulate the data of users in other countries? This has relevance beyond China, as governments in other countries may similarly demand access to user data.
- How can countries prepare themselves for grey-zone aggression that uses data harvested from ride-share apps?
- How can governments enhance public awareness of data collection and tracking? Public awareness – and associated action, such as Apple's 'Do Not Track' function – would help reduce the danger. It would also put pressure on governments to conduct more robust oversight of companies' data collection.

ABOUT THE AUTHOR

Elisabeth Braw is a Senior Fellow at the American Enterprise Institute. She was previously a Senior Research Fellow at RUSI.

Franco Palazzolo is a freelance risk consultant. He previously worked as a consultant at Control Risks.

[67] Author telephone interview with technology lawyer, 4 October 2021.

ANNEX

HOW RIDE-SHARE APPS COLLECT DATA

Table 1: Uber

Data provided by users	The App Store lists Uber as collecting the following data: Data used to track the user: purchases, contact information, search history, identifiers, usage data and other data. Data that may be collected and linked to the user's identity: purchases, financial information, location, contact information, user content, search history, identifiers, usage data, sensitive information, diagnostics, and other data.[68] Uber's privacy policy states that it additionally collects information provided by the user including name, email, phone number, login name, password, address, profile picture, payment or banking information, driver's license and other identification documents, and demographic data. It also collects location data from users' mobile devices if this function is enabled.[69] Data used to track the user: purchases, contact information, search history, identifiers, usage data and other data.
Data collected during the trip	According to its privacy policy, Uber collects transaction information related to the use of its services 'including the type of services requested or provided, order details, payment transaction information, distance traveled, and payment method. App Usage and device data'.[70]
Data from other parties	Uber collects data from other sources including 'business partners, financial partners, vendors and IT firms, insurance companies, marketing services entities'.[71]
With whom is the data shared?	Users' data is shared with 'Uber subsidiaries, service providers and business partners. Uber provides personal data to vendors, consultants, marketing partners, research firms, and other service providers or business partners. These include: payment processors and facilitators, background check and identity verification providers, cloud storage providers, Google, social media companies, including Facebook and TikTok, Marketing partners and marketing platform providers, insurance and financing partners, providers of bike and scooters that can be rented through Uber apps, such as Lime'.[72]

[68] App Store, 'Uber', <https://apps.apple.com/us/app/uber-request-a-ride/id368677368>, accessed 19 November 2021.

[69] Uber, 'Uber Privacy Note', <https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=privacy-notice>, accessed 19 November 2021.

[70] *Ibid*.

[71] *Ibid*.

[72] *Ibid*.

Table 2: Lyft

Data provided by users	The App Store lists Lyft as collecting information about purchases, financial information, location, contact information, user content, search history, identifiers, usage data, sensitive info, diagnostics and other data. Lyft also collects the user's contacts but does not link them to the user's identity.[73] Lyft's privacy policy states that it also collects 'the information you provide, usage information, and information about your device'.[74] This information includes 'name, email address, phone number, birth date, and payment information'.[75] Riders can choose to share additional information, including their photo or saved addresses.
Data collected during the trip	Lyft says in its privacy policy that it collects 'your device's precise location when you open and use the Lyft app, including while the app is running in the background from the time you request a ride until it ends'. In addition, '[w]e collect information about your use of the Lyft Platform, including ride information like the date, time, destination, distance, route, payment, and whether you used a promotional or referral code. We also collect information about your interactions with the Lyft Platform like our apps and websites, including the pages and content you view and the dates and times of your use'.[76] Like many other apps, Lyft also has the option to access users' address books.
Data from other parties	Lyft collects information about users from other sources including 'third-party services, and optional programs in which you participate, which we may combine with other information we have about you'. [77]
With whom is the data shared?	Lyft also shares with third parties, although it does not specify them. Instead the company states that users can request information regarding the third parties with which Lyft shares the respective user's details.[78]

[73] App Store, 'Lyft', <https://apps.apple.com/us/app/lyft/id529379082>, accessed 19 November 2021.

[74] Lyft, 'Lyft Terms of Service', last updated 1 April 2021, <https://www.lyft.com/terms>, accessed 19 November 2021.

[75] *Ibid.*

[76] *Ibid.*

[77] *Ibid.*

[78] *Ibid.*

Table 3: DiDi

Data provided by users	In July 2021, the Chinese government froze DiDi's abilitity to sign up new customers via the App Store. As of November 2021, the DiDi Rider app is available on the App Store. The App Store lists DiDi Rider as collecting location, contact information, contacts, user content, identifiers, usage data and diagnostics. Data used to track the user: identifiers.[79] According to its Australian privacy policy (the company lacks an international one), DiDi collects 'the information you provide us including when you create either a Passenger or Driver account with DiDi'.[80] It also collects '[y]our personal information in relation to your account such as your name, age, gender, address, email address(es) and mobile contact number' and '[y]our connection to other individuals whose personal information we may collect or hold, for example family members or referrals'.[81] In addition, DiDi states that 'personal information is required in order for DiDi to provide services to you' and that if , for example, 'you use social media to interact with us or other services provided by third parties through the DiDi app,' the app will collect 'any information that you allow the social media platform and/or the other third party site to share with us'.[82] DiDi also collects photos of drivers, Passengers and third parties and may collect, photo albums and contact lists'.[83] DiDi also collects details of the device on which the DiDi app is installed.[84]
Data collected during the trip	DiDi's Australian privacy policy states that the company collects details of when and where users book DiDi rides. It also collects recordings of voice commands by the user on the DiDi app.[85] Didi also states that it may collect wi-fi metadata from users' devices 'including whether your device is Wi-Fi and GPS enabled and connected to Wi-Fi, the Media Access Control (MAC) address or your device, the Set Service Identifier (SSID) and signal level of Wi-Fi networks within range of your device [and]the GPS location of your device'.[86]
Data from other parties	DiDi collects '[p]ersonal information collected and held via financial or third party payment systems'.[87]
With whom is the data shared?	DiDi states that it 'may disclose your personal information to related bodies corporate, other companies within the DiDi group, business partners and service providers or vendors we engage such as customer service providers. These entities may be located and operate overseas including in mainland China and Hong Kong, Singapore, Brazil, the Philippines, Ireland and the United States of America'.[88]

[79] App Store, 'DiDi-Rider', <https://apps.apple.com/us/app/didi-rider/id1362398401>, accessed 19 November 2021.

[80] DiDi Australia, 'Legal – Privacy Policy', <https://australia.didiglobal.com/legal/privacy-policy/>, accessed 19 November 2021.

[81] *Ibid.*

[82] *Ibid.*

[83] *Ibid.*

[84] *Ibid.*

[85] *Ibid.*

[86] *Ibid.*

[87] *Ibid.*

[88] *Ibid.*

Table 4: BlaBlaCar

Data provided by users	The App Store lists BlaBlaCar as collecting financial information, contact information, user content, search history, identifiers, usage data. It also collects location and diagnostics data but does not link this information to the user.[89] Registration details collected include: 'A photograph; A postal address; Details on your cars; Your mini-biography; A record of any correspondence between you and us; Passport, Driving Licence, ID Card and such other documents that you have agreed to provide to us'.[90] The mini-biography is warranted as BlaBlaCar is more akin to co-riding service than a taxi service. In addition, if users sign up via social media authentication methods, 'BlaBlaCar will access certain Personal Data (e.g. first name, surname, picture, email, number of Facebook friends, etc.)'.[91]
Data collected during the trip	BlaBlaCar says in its privacy policy that it keeps a 'record of any bookings you have made or trip related advertisements you have placed with or through our Platforms; details of accounting or financial transactions [...]; details of trips or legs you have booked or offered through our Platforms; details of your visits to our Platforms and the resources that you access'.[92] Like other ride-sharing services, it also collects location information when users have given consent.[93]
Data from other parties	Not specified.
With whom is the data shared?	BlaBlaCar shares user data with 'business partners who are social media platforms and which may provide you with connecting services, such as the connection of the information of your profile, from their social media platforms to our Platforms; our business partners who may advertise their services on our Platforms and to which you may decide to sign up for'.[94] These services can include insurance services, banking services and rental services. BlaBlaCar also shares user data with other business partners and with contractors and analytics providers.[95]

[89] App Store, 'BlaBlaCar', <https://apps.apple.com/md/app/blablacar-carpooling-and-bus/id341329033>, accessed 19 November 2021.

[90] BlaBlaCar, 'Privacy and Data Protection Policy', <https://blog.blablacar.co.uk/about-us/privacy-policy>, accessed 19 November 2021.

[91] *Ibid*.

[92] *Ibid*.

[93] *Ibid*.

[94] *Ibid*.

[95] *Ibid*.

Table 5: Ola Cabs

Data provided by users	The App Store lists Ola Cabs as collecting the following data: purchases, financial information, location, contact information, user content, search history, identifiers, usage data and diagnostics.[96] It uses financial information and contact information to track users. [97] In its New Zealand privacy policy (it lacks an international one), Ola Cabs states that it collects '[y]our personal details such as your name (including account username), addresses (including email addresses and website addresses), telephone numbers, account login details and passwords, age and gender, and certain personal details of your emergency contacts; the reference number you provide or which we allocate to you when engaged in services which we provide or services procured or booked using our services; the emergency contact information that you provide us'.[98] It also collects the contact information of friends that users have referred (refer-a-friend).[99]
Data collected during the trip	Not specified.
Data from other parties	Not specified.
With whom is the data shared?	Ola Cabs shares data with third parties including other parts of the OLA Group and its service providers, contractors and commercial partners, loyalty schemes and services, contact centre services, analytics or business services, marketing, promotions and advertising services, financial services, insurance services, and professional and legal services.[100]

[96] App Store, 'Ola Cabs', <https://apps.apple.com/us/app/ola-cabs/id539179365>, accessed 19 November 2021.

[97] *Ibid.*

[98] Ola Cars, 'OLA Privacy Policy for New Zealand', <https://www.olacabs.com/tnc?doc=nz-privacy-policy>, accessed 19 November 2021.

[99] *Ibid*.

[100] *Ibid*.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 190 years.

The views expressed in this publication are those of the author, and do not necessarily reflect the views of RUSI or any other institution.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)