CENTER FOR DEMOCRACY & TECHNOLOGY

March 20, 2020

Director Jeff Marootian
District Department of Transportation
55 M Street, SE, Suite 400
Washington, DC 20003

Conveyed via email to jeff.marootian@dc.gov

RE: Urgent Privacy Concerns With City's Decision To Collect Traveler Mobility Location Information

Dear Director Jeff Marootian:

We hope you and your colleagues at the Department of Transportation are safe and well in these uncertain and challenging times. The Center for Democracy & Technology is a nonpartisan, nonprofit technology policy advocacy organization dedicated to advancing individual rights in the digital age.[1] We write regarding the District Department of Transportation's (DDOT) decision to compel mobility service providers to regularly disclose, in real time or near real time, granular location information reflecting their customers' travels as a condition of operating in the District of Columbia. We are alarmed that the DDOT decided to not only adopt the Mobility Data Specification (MDS),[2] but also by its recent decision to compel providers to update the (/events) data field as close to real-time as possible with no more than a 3 minute delay of vehicle status change, and (/trips, /status_change) no more than 2 hours after completion of a trip. The collection of this granular location data is unnecessary for transportation planning purposes and is extremely problematic for privacy.

We share the attached memo that describes some of the privacy and security risks in MDS that we communicated to the Los Angeles Department of Transportation. As outlined in the attachment, the data the DDOT intends to compel is very sensitive and potentially identifiable. MDS's data fields include 'device_id', 'vehicle_id', 'trip-id', 'route', 'start_time', and 'end_time'. This data is quite granular and revealing. The 'route' field for example "includes every observed point in the route, even those which occur outside the municipality boundary."[3] Location data, even de-identified (not directly tied to a credit card or customer profile) is very difficult to anonymize,[4] and we are concerned that the data the DDOT intends to compel could be associated with an individual traveler.

---

[1] Center for Democracy & Technology, https://cdt.org/.
[2] District Department of Transportation, *Data and Reporting Standards*, at 5 (Jan. 1, 2020), https://ddot.dc.gov/sites/default/files/dc/sites/ddot/page_content/attachments/2019.11.6%20Dockless%20Permit%20TC%20Attatchments.pdf.
[3] Open Mobility Foundation, Mobility Data Specification, https://github.com/openmobilityfoundation/mobility-data-specification/tree/dev/provider#routes.
[4] See e.g, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, Neustar (Sep. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/ (From one

CENTER FOR DEMOCRACY & TECHNOLOGY

Courts have found that location information is a highly sensitive category of personal data. The United States Supreme Court recognized in *Carpenter v. United States*, that time-stamped location data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[5] As the Court explained, "location records hold for many Americans the privacies of life."[6] The data the DDOT seeks to compel could reveal an individual's visit to a house of worship, Planned Parenthood, a political protest or a sensitive meeting such as Alcoholics Anonymous. Patterns in the data could reveal social relationships and personal habits including when people leave for work, run errands, and where they like to go.

We understand that the DDOT has a number of goals for its Dockless Vehicle Sharing Program, including ensuring equitable access to devices,[7] and that data may play a role in assessing whether the program is meeting those goals. However, given the considerable risks to privacy, we urge the DDOT to adopt a different approach to data reporting, preferably one limited to the reporting of aggregated data, rather than individual trip level data. Properly aggregated, such data can serve legitimate planning needs and protect privacy at the same time.

Please do not hesitate to reach out with any questions in response to this letter to the Center for Democracy & Technology's Gregory Nojeim at gnojeim@cdt.org (202.407.8815) or Mana Azarmi at mazarmi@cdt.org (202.407.8828).

Sincerely,

Gregory Nojeim
Senior Counsel & Director, Freedom Security and Technology Project

Mana Azarmi
Policy Counsel

Center for Democracy & Technology

---

dataset released in 2013, which included pickup and drop off times and locations, as well as anonymized versions of taxi license and medallion numbers, a researcher was able to identify rides taken by specific celebrities and the identities of people who frequented strip clubs).

[5] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

[6] *Id*. at 2217 (2018).

[7] District Department of Transportation, *Dockless Sharing Vehicles Permit Application 2020*, at 2 (Nov. 6, 2019), https://ddot.dc.gov/sites/default/files/dc/sites/ddot/page_content/attachments/2020%20Permit%20Application.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

November 29, 2018

Seleta Reynolds, General Manager
City of Los Angeles
Department of Transportation
100 S. Main St., 10th Floor
Los Angeles, CA 90012

RE: Privacy Considerations in Dockless Mobility Pilot Program

Dear Ms. Reynolds:

The Center for Democracy & Technology is a nonpartisan, nonprofit technology policy advocacy organization dedicated to promoting digital privacy, free expression, and individual liberty. CDT works to develop and promote balanced public policy that encourages new technology while empowering consumers to make informed choices about sharing their personal data online.

We write to urge the Los Angeles Department of Transportation (LADOT) to further evaluate and implement safeguards for its data sharing requirements for dockless mobility (DM) permit holders. The current Mobility Data Specification (MDS) gives LADOT access to highly sensitive and potentially identifiable location information, both historically and in real time to a greater degree than the existing General Bikeshare Feed Specification (GBFS). LADOT must take seriously the risks to privacy and security this data collection poses. The department should ensure that the data collection is justified by legitimate needs, appropriately limited to serving those needs, and protected by privacy and security safeguards that respect the Fair Information Practice Principles (FIPPs).

Location information is among the most sensitive data, especially when collected over extended periods of time.[1] People's movements from place to place can reveal sexual partners, religious activities, and health information.[2] The U.S. Supreme Court has recognized a strong privacy interest in location data, holding that historical cell site location information is protected by the Fourth Amendment warrant requirement. As explained below, even de-identified location data can be re-identified with relative ease.

LADOT must take deliberate steps to protect this highly sensitive information. The department has recognized the need to protect the privacy of MDS data and has taken the important step of classifying

[1] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, & V. D. Blondel, Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific Reports 3: 1376 (2013).
[2] Andrew Blumberg & Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, Elec. Frontier Foundation (Aug. 2009), https://www.eff.org/wp/locational-privacy.

the data as "confidential" under the City's Information Handling Guidelines.[3] However, LADOT should further clarify how it will safeguard MDS data, including how long it will retain the data; the specific purposes for which the data will be used; and how the department will limit access and use to those specific purposes. Further, LADOT should use the current pilot period to determine how it can achieve its legitimate needs while minimizing data collection. Taking rider privacy seriously will help Los Angeles lead the way for other cities adopting similar pilot programs.

I. The MDS raises significant privacy and security concerns.

LADOT has acknowledged that user privacy is an important consideration in the DM pilot program,[4] but the MDS raises serious privacy issues that warrant further attention by regulators and the public. The MDS will result in detailed, real-time trip data being collected, analyzed, and stored through the DM pilot program. This information is without question valuable to the city, but it also presents a detailed map of the individual riding habits of residents of Los Angeles.

As Justice Sotomayor has acknowledged, tracing people's movements reveals information that is "indisputably private in nature," including their intimate relationships and visits to health care providers such as abortion clinics and AIDS treatment centers.[5] Monitoring location data also reveals First Amendment-protected activities such as religious and political affiliation. In the wrong hands, this information can be used to stalk or harass riders, compromising their physical safety. Ride-sharing APIs have been abused for things like spying on ex-partners,[6] and a 2016 Associated Press study found that law enforcement officers across the country abused police databases to stalk romantic partners, journalists, and business associates.[7] The risk of harm from exposing this information is particularly high for survivors of gender-based assault and hate-motivated violence.

---

[3] LADOT Guidelines for Handling of Data from Mobility Service Providers (Oct. 25, 2018), *available at* https://static1.squarespace.com/static/57c864609f74567457be9b71/t/5bd38544b208fc6deefa4b0c/1540588869826/LADOT+Guidelines+for+Handling+of+Data+from+MSPs++%282018-10-25%29.pdf.

[4] Seleta J. Reynolds, Dep't of Transportation, Dockless Bike/Scooter Share Pilot Program at 3 (Council File #17-1125) (May 18, 2018), *available at* http://clkrep.lacity.org/onlinedocs/2017/17-1125_rpt_DOT_05-18-2018.pdf; LADOT Guidelines for Handling of Data from Mobility Service Providers (Oct. 25, 2018), *available at* https://static1.squarespace.com/static/57c864609f74567457be9b71/t/5bd38544b208fc6deefa4b0c/1540588869826/LADOT+Guidelines+for+Handling+of+Data+from+MSPs++%282018-10-25%29.pdf. *See also* NACTO Guidelines for the Regulation and Management of Shared Active Transportation (2018), https://nacto.org/home/shared-active-transportation-guidelines/. The NACTO Guidelines acknowledge data privacy considerations for commercial transportation providers but are silent on what practices are required of government entities.

[5] United States v. Jones, 132 S. Ct. 945 (2012) (citing People v. Weaver, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009)) (Sotomayor, J., concurring).

[6] Alex Hern, *Uber employees 'spied on ex-partners, politicians and Beyoncé'*, Guardian (Dec. 13, 2016), https://www.theguardian.com/technology/2016/dec/13/uber-employees-spying-ex-partners-politicians-beyonce.

[7] Associated Press, *Police sometimes misuse confidential work databases for personal gain* (Sept. 30, 2016), *available at* https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/.

In its report to the City Council, LADOT states that its proposed data sharing requirements are "respectful of user privacy" because LADOT asks "for no personally identifiable information about users directly."[8] This is an unreasonably limited view of what constitutes personally identifiable information (PII), given the sensitivity of the data LADOT is asking for. MDS trip data includes the precise start and end times and locations of trips, tied to persistent, unique device identifiers (UDIDs) for each bike or scooter. UDIDs can be PII. According to the Federal Trade Commission (FTC), persistent identifiers like UDIDs, MAC addresses, and static IP addresses are often reasonably linkable to a particular person, computer, or device.[9] The recently enacted California Consumer Privacy Act also recognizes that UDIDs and other technical information are often PII. While such information by itself is often categorized as anonymous, the technical identifiers LADOT is asking for do not exist in a vacuum.

As LADOT links or appends additional information (such as trip data) to a UDID, it becomes more identifiable. When persistent identifiers are connected to historical location information, individuals can be personally identified with reasonable ease. Moreover, studies regularly demonstrate that de-identified data can be "reverse engineered" to identify passengers and connect them to pick-up and drop-off location information.[10] One researcher, Anthony Tockar, demonstrated how individual riders' movements could be reconstructed using a de-identified trip dataset from the New York Taxi and Limousine Commission alongside other available information. In one experiment, Tockar was able to identify individuals with a high probability who frequented Larry Flynt's Hustler Club. Evidence shows that even with robust de-identification, the more data points that are added to a data set, the easier it is to re-identify individuals.[11] This is especially true with respect to location data, where just a handful of location and time-stamped data points are needed to identify individuals.[12]

DM trip data may be even more revealing than trip data from other types of transportation because users are more likely to rely on DM for first- and last-mile transportation, taking it directly to their homes or final destinations. Car trips, for instance, often end some distance away from a user's final destination due to parking issues or other space constraints; even where taxicabs or other vehicles-for-hire, riders can specify a generic address or intersection to obfuscate their final destination.

The surveillance implications of DM location tracking could disproportionately burden underserved and marginalized riders. While DM alone will not solve transportation inequity, it has some potential to improve mobility for communities that are underserved by traditional transportation.[13] The dockless nature of new bike and scooter programs could make them more accessible than traditional docked bike

[8] Seleta J. Reynolds, *supra* note 4, at 3.
[9] Jessica Rich, *Keeping Up with the Online Advertising Industry*, Fed. Trade Comm'n (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.
[10] Neustar Research, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset* (Sept. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.
[11] Montjoye et al, *supra* note 1.
[12] *Id*. "Four spatio-temporal points are enough to uniquely identify 95% of the individuals . . . whereas two randomly chosen points still uniquely characterize more than 50% of the users."
[13] Aarian Marshall, *Not Just Tech Bros: E-Scooter Fans Are Surprisingly Diverse*, Wired (July 24, 2018), https://www.wired.com/story/electric-scooter-share-demographics-report-study-populus/.

shares, which can be inequitably distributed.[14] Some cities and companies have initiatives aimed at ensuring that DM is accessible to underserved residents.[15] LADOT's permitting application requires that DM providers submit plans for providing equitable service.[16]

The practical result of the data sharing requirements of the pilot program is that DM riders' movements will be disproportionately tracked compared to people using other forms of transportation.[17] Overbroad tracking could itself become a barrier to entry for low-income and minority riders, who already face disproportionate surveillance and scrutiny from law enforcement and other authorities. Without appropriate safeguards restricting access to the data, its collection could deter underserved riders.[18]

II. LADOT should adopt clear and robust privacy and security safeguards for MDS data.

The duration of the DM pilot program provides an opportunity for the LADOT to establish specific privacy and security policies to address how LADOT and any other governmental or private actors may access or receive MDS data. These policies should address each of the FIPPs[19] and include appropriate data security and access controls. The availability of this information to third parties including researchers must also be addressed.[20]

CDT was pleased to see that LADOT has taken the important first step of classifying MDS Trip Data as Confidential data under the City of Los Angeles Information Handling Guidelines. Under the guidelines,[21] confidential information is exempt from disclosure under the California Public Records Act (CPRA), and its access or disclosure is limited to those with a "need to know." The guidelines also include certain

---

[14] Julia Ursaki & Lisa Aultman-Hall, Quantifying the Equity of Bikeshare Access in U.S. Cities (Aug. 1, 2015), http://chi.streetsblog.org/wp-content/uploads/sites/4/2016/03/Bikeshare_TRB_submission.pdf.

[15] Angie Schmitt, *Dockless Companies Deliver Bike-Share to Underserved Areas*, StreetsBlog USA (May 10, 2018), https://usa.streetsblog.org/2018/05/10/dockless-companies-delivering-bike-share-to-underserved-areas/; John Greenfield, *LimeBike and Zagster Dockless Bikes Launch in Chicago, Ofo and Jump Are Coming*, StreetsBlog Chicago (May 1, 2018), https://chi.streetsblog.org/2018/05/01/limebike-and-zagster-dockless-bikes-launch-in-chicago-ofo-and-jump-are-coming/.

[16] Seleta J. Reynolds, *supra* note 4, at 11.

[17] Populus has found, for instance, that "African-American residents of D.C. (which represent 47% of the D.C. population) have adopted dockless services at a significantly higher ratio: 2.6 times more (versus 1.2 times more for white residents)." Regina Clewlow, *DC is growing its dockless bike and scooter program: We partnered with them to evaluate how it's expanding access in underserved communities*, Populus (Nov. 15, 2018), https://medium.com/populus-ai/measuring-equity-dockless-27c40af259f8.

[18] *E.g.*, Sarah Brayne, Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment, American Sociological Review. 79: 367-391 (2014).

[19] *See, e.g.*, U.S. Department of Homeland Security Privacy Policy Guidance Memorandum, Hugo Teufel III (Dec. 29, 2008), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[20] Joseph Jerome, *Ethically Scraping and Accessing Data: Governments Desperately Seeking Data*, Ctr. for Democracy & Tech. (May 3, 2018), https://cdt.org/blog/ethically-scraping-and-accessing-data-governments-desperately-seeking-data/.

[21] LADOT Guidelines for Handling of Data from Mobility Service Providers (Oct. 25, 2018), *supra* note 4.

security requirements; for example, confidential data must be encrypted in electronic transmission. However, these guidelines still leave many unanswered questions as to how LADOT will handle trip data.

LADOT should (1) limit access to and use of MDS data to specified purposes; (2) establish a reasonable retention and deletion policy; (3) clarify how MDS data will be secured or obfuscated to protect against breaches and minimize the likelihood of disclosure of identifiable data; and (4) communicate DM data collection and use transparently to DM users. These considerations are consistent with the FIPPs. CDT offers the following more specific recommendations:

- **Purpose limitation and access controls:** LADOT has stated that it intends to use MDS data for permit enforcement, communication of events, parking restrictions, and city planning. To the extent possible, LADOT should communicate the specific purposes for and ways in which trip data will be used and what other entities, if any, it will be shared with. The City of Los Angeles Information Handling Guidelines limit access to Confidential information (including trip data) to those with a "need to know" who are individually designated by the information owner. In its 2016 Urban Mobility in a Digital Age: A Transportation Technology Strategy for Los Angeles, LADOT acknowledge that "growing interest in sharing data" raises privacy issues. It concluded "[e]valuating how the data may be used for analysis can help define the level of detail and anonymity necessary."[22] We agree: data sharing exacerbates privacy and security challenges posed by any collection of information. LADOT should clarify that it will limit access to the MDS API to designated officials within the agency or city government solely for enforcing DM permits, communicating events, enforcing parking restrictions, and city planning. The uses of trip data for "city planning" should be further specified.

  Specifically, LADOT should commit that it will not share trip data with law enforcement without a warrant. The U.S. Supreme Court has recognized that people have an expectation of privacy in their physical movements. In *Carpenter v. U.S.*, the Court held that police must get a warrant before collecting historical cell site location information.[23] Without proper access controls, agency collection of location data can become an end-run around constitutional protections.

- **Duration of access and retention:** The period in which LADOT intends to retain DM data should be clearly specified. The NACTO Shared Active Transportation Guidelines note that locaties must require companies to retain all records in "full accordance with local and state records retention policies."[24] LADOT's guidelines indicate that, to the extent that confidential MDS data is used for transportation policymaking, LADOT will retain the data unobfuscated for *no less than* two years. The Department appears to have established a minimum retention requirement, but has not articulated any retention limits or deletion requirements. While the City's Data Handling

[22] Urban Mobility in a Digital Age: A Transportation Technology Strategy for Los Angeles 29 (Aug. 2016), https://static1.squarespace.com/static/57c864609f74567457be9b71/t/57c9059b9de4bb1598eeee49/1472793280502/Transportation+Technology+Strategy_2016.pdf.
[23] Carpenter v. United States, No. 16-402, 585 U.S. __ (2018).
[24] NACTO Guidelines, *supra* note 4, at 8.

Guidelines specify a destruction method for hard copies of confidential data (shredding), they also do not provide a retention or electronic deletion schedule. Again, we would note that lengthy retention periods of historic location information present significant privacy risks, and additional real-time transmission of this information enables invasive tracking of individual movements in near real-time. A formal deletion policy pairs well with data minimization to ensure that data is kept for the minimum amount of time necessary to extract value before deleting it.

- **Security of transmission and storage:** While transportation officials have emphasized the importance of real-time data transmission for DM, the information security challenges of constantly transmitting data have not been adequately addressed.[25] The City of LA's Data Handling Guidelines require confidential information to be encrypted in transmission and password protected in storage. To the extent possible, LADOT should also obfuscate trip data in storage to minimize the likelihood that personally identifiable information will be revealed through database queries or potential breaches.

  Further, LADOT's policy states that it will not disclose "unobfuscated Confidential Data" in response to a California Public Records Act (CPRA) request, but it does not define "unobfuscated." Not all methods of obfuscation are equally effective, and hashing of public location datasets has been broken before.[26] LADOT should determine and clarify the circumstances under which it anticipates disclosing MDS data and its plans for effectively obfuscating it and protecting against reverse engineering or re-identification. Ideally, LADOT would detail its own security policies and the expectations it has of permit holders.

- **Transparency:** While the publication of the MDS on Github provides one level of needed transparency, LADOT should also give consideration to how the department, as well as DM permit holders, will communicate to individual riders about the data collection and usage practices involved with scooters. As a practical matter, many of the LADOT documents referenced in this letter were not easily locatable or accessible. CDT recommends that LADOT consider how it can offer information about the department's privacy and security policies and practices in a centralized location.

III. LADOT should use the current pilot period to determine how it can achieve its legitimate needs while minimizing the amount and granularity of data it collects

CDT recommends that LADOT use this pilot program as an opportunity to assess what types of raw data are absolutely necessary to facilitate safe and equitable DM in Los Angeles. The scope of LADOT's data

[25] The LADOT Guidelines on handling DM data is only a page of high-level policy positions. *See* LADOT Guidelines for Handling of Data from Mobility Service Providers (Oct. 25, 2018), *supra* note 4.
[26] Vijay Pandurangan, *On Taxis and Rainbows*, MEDIUM (June 21, 2014), https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1.

collection should not exceed what is necessary to enforce DM permit requirements and regulations.[27] Courts have recognized the importance of narrowly tailoring government agency requests for companies' data absent a warrant. The Supreme Court has identified three criteria that a reasonable administrative search must meet: (1) There must be a substantial government interest that informs the regulatory scheme; (2) the inspection must be necessary to further the regulatory scheme, and (3) the inspection program must provide a "constitutionally adequate substitute for a warrant," in terms of the certainty and regularity of its application.

The city should take careful stock of the types and sensitivity of data for which it is asking, including potential PII such as UDIDs, and determine whether each data type is necessary for enforcement or how information can be obscured to minimize privacy risks. It should also consider the granularity of location information it needs. GPS coordinates, for example, are two numbers that describe the latitude and longitude of a location on a coordinate system (e.g., 38.9029818° N, 77.0319413 W). Imprecise geolocation generally captures coordinates having the precision of two or fewer decimal places.[28] LADOT should consider whether location to the third or fourth decimal, which captures individual street level and land parcel, are sufficient for its regulatory purposes.

--

LADOT's DM pilot program and its MDS are already being pointed to as a potential national standard.[29] It is worth acknowledging that part of LADOT's leadership role is establishing policies and procedures that can be followed by cities with fewer resources or less technical capacity and expertise. We hope the LADOT will consider these issues, as well as our recommendations, as it engages in its DM pilot program.

Sincerely,

Natasha Duarte
Policy Analyst
Privacy & Data Project

Joseph Jerome
Policy Counsel
Privacy & Data Project

[27] The 2016 Urban Mobility in a Digital Age: A Transportation Technology Strategy for Los Angeles specifically notes the need to take steps to minimize privacy impacts, arguing that "personal information is not needed for planning analytics and should be anonymized or aggregated for protection. Staff and consultants without authorization should never have access to this information and protocol for how data can be exchanged and used should be clearly articulated as a citywide policy." Urban Mobility in a Digital Age, *supra* note 20, at 29.
[28] *See* Network Advertising Initiative, Guidance for NAI Members: Determining Whether Location is Imprecise 1 (July 20, 2015), https://www.networkadvertising.org/sites/default/files/NAI_ImpreciseLocation.pdf.
[29] NACTO Guidelines, *supra* note 4, at 8.