April 3, 2019

Councilmember Mike Bonin
Los Angeles City Council
Transportation Committee Chair
Room 395, City Hall
200 N. Spring Street
Los Angeles, CA 90012
councilmember.bonin@lacity.org
Eric.bruins@lacity.org

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

RE: Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification

Dear Honorable Councilmember Bonin & Ms. Reynolds:

I am writing on behalf of the Electronic Frontier Foundation (EFF) and New America's Open Technology Institute (OTI) to express serious concerns regarding the Los Angeles Department of Transportation's (LADOT) response to the privacy issues raised regarding its data-sharing requirements for dockless mobility permit holders. EFF is a non-profit, member-supported civil liberties organization that works to protect privacy and civil liberties in the digital world. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open and secure communications networks.

LADOT's Mobility Data Specification (MDS) requires dockless mobility providers to share granular trip data with the Department, which constitutes sensitive personal data about Los Angeles residents, yet LADOT has refused and continues to refuse to treat this data as such. It has failed to adopt clearly articulated policies regarding how it will use the data, how long it will retain the data, when it will delete the data, and the conditions on which it share data with third parties—all despite that LADOT has been collecting data via the MDS for months[1] and is

[1] LADOT has been collecting data via the Provider API—the first stage of its MDS, which allows LADOT to demand that service providers share information, including precise geolocation and time-stamped information about individual trips taken by users—since at least October or November 2018.

already sharing data with at least one third party, a private for-profit company called Remix. LADOT's recently-released high level "Data Protection Principles" are no substitute for clear policies on use, retention, deletion, and access/sharing.[2] Perhaps most concerning, LADOT is forging ahead with the next stage of the MDS, scheduled for enforcement on April 15, 2019, before addressing the grave privacy implications of the initial stages of the MDS.

Moreover, the MDS appears to violate the California Electronic Communications Privacy Act (CalECPA), which prohibits any government entity from compelling the production of electronic device information, including raw trip data generated by electronic bikes or scooters, from anyone other than the authorized possessor of the device without proper legal process.

EFF has urged LADOT to hold off on moving forward with the second stage of the MDS—the Agency API, which requires that operators provide LADOT with raw trip data for *each and every* ride taken in Los Angeles—until after it has addressed and resolved the serious privacy concerns raised by the initial stage of the MDS, the Provider API. LADOT has cited the City Council's Ordinance No. 185785, which directs the implementation of a shared mobility pilot program, as the impetus behind its lack of willingness to delay enforcement of the Agency API. The Ordinance, however, makes no mandate about what LADOT must collect from dockless mobility operators in order to issue a permit.[3]

LADOT should not use the Ordinance as a license to ignore both the privacy interests of Los Angeles residents and the law. LADOT may have a legitimate need for information regarding how dockless scooters and bikes are used on the streets of Los Angeles, but any data-sharing mandates must protect the privacy interests of Los Angeles residents—and comply with the state's privacy laws. That has not happened here.

LADOT can begin its pilot program without moving forward with the MDS. The agency already has access to *tremendous amounts of data* about Los Angeles residents via the Provider API. LADOT needs to address the serious privacy and civil liberties issues implicated by Provider API—and it needs to do so *before* moving forward with any further stages of the MDS. LADOT also needs to commit to addressing the serious privacy and civil liberties issues

---

[2] *See generally* LADOT Data Protection Principles (Mar. 22, 2019), https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf.

[3] The Ordinance generally cites LADOT's Dockless On-Demand Personal Mobility Conditional Permit Rules and Guidelines, which generally requires operators to comply with the MDS without describing any details of the MDS, but the Ordinance itself imposes no data collection mandates on LADOT. *See* Ordinance No. 185785 (effective Oct. 5, 2018), http://clkrep.lacity.org/onlinedocs/2017/17-1125_ORD_185785_10-05-2018.pdf; *see* Dockless on Demand Personal Mobility Conditional Permit, at 25, https://ladot.lacity.org/sites/g/files/wph266/f/LADOTDocklessCP.pdf (containing LADOT's Dockless On-Demand Personal Mobility Conditional Permit Rules).

implicated by the MDS transparently, with real opportunities for stakeholder and community awareness and engagement.

I. LADOT Fails to Acknowledge the Sensitive and Personal Nature of the Information of Granular Trip Information.

Both the Provider and Agency APIs require mobility operators to share granular trip data with LADOT. The Provider API requires that mobility operators respond to requests for trip data, including time-stamped route information with both the start and end points of a trip as well as "all possible GPS samples collected by a Provider" reported at "the maximum accuracy of the specific measurement."[4] Meanwhile, the Agency API requires providers to share with LADOT, for every trip taken, "temporal and location data for every 300 ft (91 meters) while [a] vehicle is in motion"—or, for providers who do not calculate distance in real time, every "14 seconds"—and every "30 seconds while at rest."[5]

This trip information can be deeply revealing. As the United States Supreme Court recognized in *Carpenter v. United States*, 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.'"[6] As the Court explained, "location records hold for many Americans the privacies of life."[7] Indeed, the time-stamped geolocation data that LADOT will be indiscriminately ingesting for each and every trip taken in Los Angeles via the Agency API could reveal trips to Planned Parenthood, specific places of prayer, and gay-friendly neighborhoods or bars. Patterns in the data could reveal social relationships, and potentially even extramarital affairs, as well as personal habits, such as when people typically leave for work, go to the gym, or run errands, how often they go out on evenings and weekends, and where they like to go.

LADOT has, however, refused to acknowledge the sensitive nature of the trip data implicated by the MDS, maintaining that the MDS requires "no personally identifiable

---

[4] *See* City of Los Angeles, Mobility Data Specification: Provider, Branch 0.3x, https://github.com/CityOfLosAngeles/mobility-data-specification/tree/0.3.x/provider (noting, to illustrate the level of precision expected, that "a-GPS is accurate to 5 decimal places, differential GPS is generally accurate to 6 decimal places").

[5] City of Los Angeles, Mobility Data Specification: Agency, Branch 0.3x, https://github.com/CityOfLosAngeles/mobility-data-specification/blob/0.3.x/agency/README.md. The Agency API requires this information to be shared within 24 hours.

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

[7] *Id*. at 2217 (2018) (internal quotations and citations omitted).

information about users *directly*" (emphasis added).[8] The critical qualifier in that statement is the word "directly." Even with names stripped out, location information is notoriously easy to re-identify,[9] particularly for habitual trips. This is especially true when location information is aggregated over time. As one 2013 study on human mobility data concluded, "human mobility traces are highly unique."[10] Researchers found that only "four spatio-temporal points [were] enough to uniquely identify 95% of the [1.5 million] individuals" in the study.[11]

In another example, when a database of every cab ride taken in New York City in 2013 containing records on 173 million trips—including pickup and drop-off locations and times as well as putatively anonymized hack license number and medallion number and other metadata—was released, one researchers was able to de-anonymize the entire set (thus re-identifying the hack license numbers and medallion numbers for each trip) with relative ease.[12] Another researcher then used the data—in combination with other readily available data tying particular individuals to particular locations—to identify individual riders, where they went, and their personal habits or routines.[13]

Even more on point here, New York City's public bikeshare database—which contains only dock-to-dock data and is therefore less specific than the point-to-point data collected under

---

[8] 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.

[9] *See* CDT, Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility (Nov. 29, 2018), https://cdt.org/insight/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/.

[10] *See* Yves-Alexandre de Montjoye et al., Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports 3, Article Number 1376 (Mar. 23, 2013), available at http://www.nature.com/articles/srep01376.

[11] *See id.* The study relied on 15 months of human mobility data for 1.5 million individuals, where the location of each individual had been specified hourly.

[12] The researchers were able to re-identify the hack license number and medallion numbers, because New York had used an insufficient hashing algorithm to anonymize the data. Vijay Pandurangan, On Taxis and Rainbows, Lessons from NYC's improperly anonymized taxi logs, Medium (June 21, 2014), https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1.

[13] Anthony Tockar, Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset (Sep. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/; *see also* J.K. Trotter, Public NYC Taxicab Database Lets You See How Celebrities Tip, *Gawker* (Oct. 24, 2014), https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546.

LADOT's MDS—readily reveals the travel habits of unique individuals.[14] In a cursory analysis of the data, EFF's staff technologists discovered a route (from one specific docking station to another) that appears to be frequented almost exclusively by a single individual, who leaves home between 7:30 am and 8:00 am most mornings and returns home just after 6:00 pm each evening.[15] The individual first began biking the route in November 2018, and since then has taken it between four and seven days a week, including most weekends. The rider bikes home more often than they bike to work, but they've used the system diligently through the winter. They did not take the route on Christmas, but were back at it as of December 26. One only needs to identify the individual at the start or end of the route on a single occasion—either via seeing the individual pick up or dropping off a bicycle in person or via some other dataset revealing their location in that place at that time—in order to link them to this extensive and potentially revealing history of behavior.

Given that *dockless* scooters and bikes may be parked directly outside a rider's home or work, the potential to associate specific trips—particularly habitual trips or patterns of travel—with a single individual is far greater. And the data shows that riders are using dockless mobility vehicles for their regular commutes. For example, as documented in Lime's Year End Report for 2018, 40 percent of Lime riders, and 30 percent of Lime riders in Los Angeles, reported commuting to or from work or school during their most recent trip.[16]

As the California Legislature determined last year in enacting the California Consumer Privacy Act (CCPA), any information that can be reasonably linked, *directly or indirectly,* with a particular consumer should be considered "personal information."[17] The Legislature explicitly listed geolocation information as one such category of information.[18]

Here, there can be no dispute that the MDS requires mobility operators to share information that can be linked, directly or indirectly, with particular consumers. LADOT must acknowledge that the trip data implicated by the MDS is personal information pertaining to the movements of individual people. And it must delay moving forward with its plans to collect this

---

[14] Available at https://www.citibikenyc.com/system-data.

[15] EFF's staff technologists identified this individual based on the docking station pairs and timestamps alone; they were able to confirm that these trips were likely taken by the same individual because New York City's bikeshare database also publishes, for each trip, the gender and birth year listed for the rider.

[16] Lime, Year End Report 2018, https://www.li.me/hubfs/Lime_Year-End%20Report_2018.pdf.

[17] *See* Cal. Civ. Code § 1798.140(o)(1) ("'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: . . . (G) Geolocation data.") (effective Jan. 1, 2020).

[18] *Id*.

geolocation data for each and every dockless mobility trip taken within Los Angeles until it has set forth adequate policies detailing how it will protect it.

II. LADOT Has Failed to Set Out Detailed Policies Limiting the Use and Retention of Precise Location Data.

On March 22, 2019, LADOT publicly posted a working draft of high-level "Data Protection Principles" that LADOT says it will work toward for the data obtained from mobility companies pursuant to the MDS.[19] While these high-level principles are a good preliminary step, they are a far cry from actual data protection policies, which LADOT should have finalized before ever implementing the MDS. They do not, for example, delineate the specific purposes for which LADOT will use the data, describe how LADOT will ensure that the data is only used for those purposes, explain now long LADOT will retain raw data, lay out a destruction schedule for the raw data, or detail how and when LADOT will aggregate/de-identify data.

Despite LADOT's lack of any real privacy protocols, LADOT has refused to entertain the idea of delaying the next stage of the MDS until it has carefully thought through how it will protect the data it is collecting and the privacy of its residents. LADOT must set out clear data use policies—not merely high-level principles—to protect individual privacy by specifying how it will use, and how long it will retain, sensitive geolocation information collected about Los Angeles residents via the MDS. And it must do so before it forges ahead with the next stage of the MDS. Failing to do so is not only irresponsible and inconsistent with fundamental data protection best practices, but it is also in violation of the right to privacy afforded by the California Constitution.

Article I, Section 1 of the California Constitution explicitly lists privacy as an inalienable right of all people.[20] As the California Supreme Court has recognized, "[i]nformational privacy is the core value furthered by" the explicit inclusion of the right to privacy in the state

---

[19] The document does not include any indication of when LADOT will set out specific policies to ensure compliance with these high level data protection principles. *See generally* LADOT Data Protection Principles (Mar. 22, 2019), https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf.

[20] Cal. Const., art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*.") (emphasis added); *see also* Civ. Code § 1798.1 ("The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them.").

constitution.[21] The Court has further explained that "the moving force" behind California's constitutional right to privacy was concern over "the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society[.]"[22] Inclusion of the right to privacy recognizes that "[t]he proliferation of government . . . records over which we have no control limits our ability to control our personal lives."[23] And pursuant to the right to privacy, any incursion into individual privacy "must be justified by a compelling interest."[24]

The right of privacy not only "'prevents government and business interests from collecting and stockpiling unnecessary information about us[,]'" but also "'from misusing information *gathered for one purpose in order to serve other purposes*[.]'"[25] Indeed, such "improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party[]" is among the "principal 'mischiefs'" targeted by the right.[26]

LADOT's failure to outline and limit the specific purposes for which LADOT plans to use geolocation data collected via the MDS, or to delineate how it will minimize its collection of personal information (including trip data) to data necessary to achieve those objectives, violates both the letter and the spirit of the California Constitution's right to privacy.[27] Until LADOT

---

[21] *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35 (1994); s*ee also Los Angeles Gay & Lesbian Ctr. v. Superior Court*, 194 Cal. App. 4th 288, 307 (2011) (citation and internal quotations omitted) ("[T]he privacy right protects the individual's reasonable expectation of privacy against a serious invasion.").

[22] *White v. Davis*, 13 Cal. 3d 757, 774 (1975).

[23] *Id.* at 775.

[24] *White*, 13 Cal. 3d at 775.

[25] *Hill*, 7 Cal. 4th at 17 (citation omitted; emphasis added).

[26] *White*, 13 Cal. 3d at 775.

[27] LADOT's Data Protection Principles mention data minimization—the practice of "limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specific purpose," *see* Bernard Marr, Why Data Minimization Is An Important Concept In The Age of Big Data, Forbes (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#373005ed1da4. But the principles do not include a single binding data minimization practice. They state generally that LADOT will aggregate, obfuscate, de-identify, *or* destroy data where it no longer needs the raw data for the management of the public right of way, but because it provides no insight into what it "needs" this data for in the first place, these hollow pronouncements impose no true restrictions at all.

outlines how exactly it will use this data—and thus why it needs the data—and imposes clear restrictions on data use to ensure it is not used for other purposes, LADOT cannot show that collection of this data is justified by a compelling interest. Nor can it protect against one of the principal mischiefs targeted by the right to privacy: use of the data for a purpose other than the one for which it was collected.

LADOT must also delineate how long it will retain raw data, set a destruction schedule for that data, explain the specific circumstances under which it will retain aggregated/obfuscated data, and indicate the specific methodologies it will to use to ensure that the data is sufficiently aggregated to prevent re-identification. LADOT's promise to "rely on established standards" to aggregate/obfuscate data is not sufficient. Given the particular challenge presented by the task of sufficiently de-identifying geolocation data, as outlined above, LADOT must set out the specific methodologies it plans to use to protect the sensitive personal geolocation data it is collecting.[28]

The fact that this is a "pilot program" is no excuse for LADOT's failure to implement adequate data protection policies. The MDS implicates the collection of sensitive personal data of real individuals, so clearly articulated data use policies are imperative. LADOT should have finalized such policies prior to implementation of the Provider API, yet months after its launch, these policies are still not in place. LADOT should start taking seriously the privacy of Los Angeles residents and delay the second stage of the MDS until after it has grappled with these serious privacy and civil liberties concerns.

III. LADOT Has Failed to Commit in Writing to Require a Warrant for Location Data.

LADOT's Data Protection Principles also fail to commit the agency to not sharing geolocation data with law enforcement without a warrant. The principles do not even mention a warrant—despite that a LADOT spokesperson told Politico in March that it would only share data with the Los Angeles Police Department when presented with a warrant.[29] Rather, the principles state that "law enforcement will not have access to raw trip data other than as required by law, such as by a court order, subpoena, or other legal process."[30] This does not comport with the Supreme Court's holding in *Carpenter v. United States*, which requires a warrant before the police can gain access to historical location data. *See Carpenter*, 138 S. Ct. at 2221.

---

[28] It may update those methodologies in the future as advancements are made.

[29] Jeremy White, 'This is creepy': In LA, scooters become the next data privacy fight, Politico (Mar. 6, 2019), https://www.politico.com/states/california/story/2019/03/01/this-is-creepy-in-la-scooters-become-the-next-data-privacy-fight-883121.

[30] Draft LADOT Data Protection Protocols, ¶ 2(a), https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf.

As the Center for Democracy and Technology (CDT) pointed out in November, "Without proper access controls, agency collection of location data can become an end-run around constitutional protections."[31] Months later, this opportunity for an end-run around the Fourth Amendment rights of Los Angeles residents has still not been addressed. LADOT must commit in writing to requiring a warrant for location information.

IV. LADOT Has Been Sharing Geolocation Data With At Least One Third Party Without Appropriate Privacy Protections.

LADOT's Data Protection Principles state that the agency "*will* prohibit any third party access or use of raw trip data for third party purposes, including for data monetization purposes" and that "[t]he City *will* only allow access to raw trip data by third parties under contracts that limit the use of the raw trip data to purposes directed by LADOT and as needed for LADOT's operational and regulatory needs."[32]

LADOT, however, has already been sharing data collected via the MDS with Remix, a private for-profit company that partners with cities to aid in transportation and transit planning.[33] To date, LADOT has not provided any details about its data-sharing arrangement with Remix, including information regarding any limitations that it has imposed on Remix, such as prohibitions on commercial use of MDS information. It appears that, at least up until now, LADOT has been sharing MDS data with Remix—including sensitive geolocation information about Los Angeles residents—*without any contract* limiting Remix's use of the raw trip data to purposes directed by LADOT.

Here again, it is evident that the privacy of Los Angeles residents has been an afterthought. LADOT's decision to begin sharing data with Remix—and/or forcing mobility operators to share data with Remix—without first ensuring that sufficient contractual limitations were in place to restrict Remix's use of trip data is out of step with basic data protection best practices and raises serious concerns under the California Constitution's right to privacy. It is

---

[31] CDT, Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility (Nov. 29, 2018), https://cdt.org/insight/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/.

[32] *See* LADOT Data Protection Principles, ¶ 2(b) (Mar. 22, 2019), https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf.

[33] Skip Descant, Lime and Spin to Share Detailed Use Data with LADOT, Government Technology (Nov. 9, 2018), https://www.govtech.com/fs/Lime-and-Spin-to-Share-Detailed-Use-Data-with-LADOT.html; Michael Grass, Los Angeles Inks New Data-Sharing Agreement With Scooter and Bikeshare Companies, Route Fifty (Nov. 9, 2018), https://www.routefifty.com/smart-cities/2018/11/ladot-data-sharing-agreement-scooters-bicycles/152727/.

also inconsistent with California's recently enacted consumer privacy statute, the California Consumer Privacy Act ("CCPA"), which specifically imbues Californians with a right to opt out of data sharing with third parties, a right to request that their data be deleted, and a right to know how their data is being used. The MDS undermines users' ability to assert these rights with regard to their mobility data—some of their most sensitive personal information—as they cannot request that their data be deleted by LADOT given the CCPA's lack of application to government entities. And LADOT's lack of transparency regarding the MDS data it shares with third parties, like Remix, and how those third parties will be using that data, further exacerbates the conflict with the CCPA, because consumers may not realize that they must direct their opt-out, deletion, and right-to-know requests to Remix. Consumers currently have no understanding of and no control of how their data is being used by LADOT or by Remix.

LADOT must cease any data sharing with Remix until after (a) it has executed a contract with Remix that protects the privacy of Los Angeles riders' and limits the company's use of trip data to specific purposes on behalf of LADOT; and (b) it has made public the nature of its relationship with Remix, along with a description of the data that will be shared with Remix and the limitations it has imposed on Remix's use of that data.

V. The MDS Violates the California Electronic Communications Privacy Act.

Not only has LADOT failed to set out adequate policies to protect the sensitive personal geolocation information implicated by the MDS, but the MDS also appears to violate the California Electronic Communications Privacy Act (CalECPA). CalECPA provides that "a government entity shall not . . . [c]ompel the production of or access to *electronic device information* from any person or entity other than the authorized possessor of the device" except in specific circumstances.[34] This section covers both (a) electronic bikes and scooters—which are "electronic devices," *i.e.*,"device[s] that store[], generate[], or transmit[] information in electronic form"[35]—and (b) the geolocation information they generate—which constitutes both "electronic device information"[36] or "electronic information"[37] under the statute. The section thus applies when LADOT, or any other government agency, attempts to obtain raw trip data

[34] Cal. Pen. Code § 1546.1(a).

[35] Cal. Pen. Code § 1546(f).

[36] "'Electronic device information' means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." Cal. Pen. Code § 1546(g).

[37] "'Electronic information' means electronic communication information or electronic device information." Cal. Pen. Code § 1546(h).

collected from a bike or scooter from anyone other than the rider (*i.e.*, the authorized possessor).[38]

CalECPA provides that a government entity may "compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device" only with a warrant, a wiretap order, or in cases where the information is not sought in connection with a criminal offense, a subpoena issued pursuant to existing state law so long as access to the information via a subpoena is not otherwise prohibited by law. None of CalECPA's exceptions apply here. LADOT does not have a warrant or a wiretap order. And even if it obtained a subpoena for this information, as outlined above, accessing raw location data with a mere subpoena is prohibited by the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2221 ("the Government must generally obtain a warrant supported by probable cause before acquiring" location records).

VI. LADOT Has Failed to Consider Privacy-Protective Solutions.

Finally, LADOT has failed to seriously consider privacy-protective solutions that would achieve the goals of the pilot program while protecting the privacy of Los Angeles residents and comporting with both CalECPA and the CCPA. Given the sensitive nature of location data, in order to achieve its objectives while also respecting and protecting the privacy of Los Angeles residents, LADOT should be working with mobility operators to obtain aggregated, de-identified trip data, rather than raw trip data for each and every trip. Indeed, aggregate trip data is sufficient for many of the purposes for which LADOT claims it needs raw trip data: ensuring compliance with vehicle count caps, geofencing, and distribution requirements in low-income areas; better understanding how scooters and bikers are being used across the city; and planning and budgeting for the future.

LADOT maintains that it needs raw trip data because it cannot trust aggregate data provided by operators. But there are various technical auditing solutions to solve for such lack of trust. One solution might lie in immutable audit logs, such as the merkle tree-based technology that enables trusted communication on the Internet.[39] Such audit logs would ensure that cities could trust aggregated metrics, because operators would be required to maintain stores of data that could not be changed or deleted, and cities would be allowed to audit the data stores

---

[38] "'Authorized possessor' means the possessor of an electronic device when that person is the owner of the device or *has been authorized to possess the device by the owner* of the device." Cal. Pen. Code § 1546(b) (emphasis added).

[39] Certificate Transparency, How Log Proofs Work, https://www.certificate-transparency.org/log-proofs-work.

at any point to ensure that the data had not been fabricated or adjusted.[40] In addition, there are other technical methods, such as secure multi-party computation, cryptographic commitments, and zero-knowledge proofs, which could serve as the basis for more sophisticated privacy-protective auditing solutions. LADOT could and should be working with operators on building technical auditing solutions to meet its needs.

***

LADOT must start taking seriously the privacy of Los Angeles residents. We urge the City Council and LADOT to: (i) formally recognize the sensitive and private nature of the trip data implicated by the MDS; (ii) adopt real policies, in consultation with stakeholders and the public, addressing the privacy and civil liberties issues implicated by collection of this raw trip data; (iii) delay moving forward with any further stages of the MDS (*i.e.*, the Agency API) until LADOT has adequately addressed the privacy and civil liberties implicated by initial stages of the MDS (*i.e.*, the Provider API); and (iv) commit to working with operators on solutions that will achieve its goals without sacrificing the privacy of Los Angeles residents.

We thank you for your attention to our concerns. Should you have any questions, please contact Jamie L. Williams at (415) 436-9333, ext. 164, or jamie@eff.org.

Respectfully Submitted,

Jamie Williams, Staff Attorney
Bennett Cyphers, Staff Technologist
Nathan Sheard, Grassroots Advocacy Organizer
Electronic Frontier Foundation

Andi Wilson Thompson, Senior Policy Analyst
New America's Open Technology Institute

[40] *See also* Nat Buckley, New tools for building trust in digital services, Projects by IF (Oct. 24, 2018), https://www.projectsbyif.com/blog/new-tools-for-building-trust-in-digital-services.

CC: Councilmember Gilberto Cedillo
councilmember.cedillo@lacity.org, Mel.Ilomin@lacity.org

Councilmember Krekorian
councilmember.Krekorian@lacity.org, doug.mensman@lacity.org

Councilmember Bob Blumenfield
councilmember.blumenfield@lacity.org, cecilia.castillo@lacity.org

Councilmember David E. Ryu
david.ryu@lacity.org, justin.orenstein@lacity.org

Councilmember Paul Koretz
paul.koretz@lacity.org, jay.greenstein@lacity.org, jeff.ebenstein@lacity.org

Councilmember Nury Martinez
councilmember.martinez@lacity.org, arcelia.arce@lacity.org

Councilmember Monica Rodriguez
councilmember.rodriguez@lacity.org, humberto.quintana@lacity.org

Councilmember Marqueece Harris-Dawson
councilmember.harris-dawson@lacity.org, dina.andrews@lacity.org

Councilmember Curren D. Price, Jr.
councilmember.price@lacity.org, bryce.rosauro@lacity.org

Councilmember Herb J. Wesson, Jr.
councilmember.wesson@lacity.org, edw.johnson@lacity.org

Councilmember Greig Smith
councilmember.smith@lacity.org, eric.moody@lacity.org

Councilmember Mitch O'Farrell
councilmember.ofarrell@lacity.org, star.parsamyan@lacity.org

Councilmember Jose Huizar
councilmember.huizar@lacity.org, cassie.truong@lacity.org

Councilmember Joe Buscaino
councilmember.buscaino@lacity.org, aksel.palacios@lacity.org