No. 21-55285

United States Court of Appeals

for the

Ninth Circuit

JUSTIN SANCHEZ,

Plaintiff-Appellant,

v.

LOS ANGELES DEPARTMENT OF TRANSPORTATION AND CITY OF LOS ANGELES,

Defendants-Appellees,

On Appeal from the United States District Court
for the Central District of California
Case No. 2:20-cv-05044-DMG-AFM, Hon. Dolly M. Gee

BRIEF OF *AMICUS CURIAE* KEVIN WEBB IN SUPPORT OF APPELLANT

JORDAN R. JAFFE
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111-4788
Telephone: (415) 875-6600

Counsel for Amicus Curiae Kevin Webb

July 30, 2021

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

RULES AND REGULATIONS

ADDITIONAL AUTHORITIES

"We don't want to be accidentally creating the next redlining."

–Anonymous public transit official[1]

STATEMENT OF INTEREST[2]

Amicus Kevin Webb has spent over a decade building public digital infrastructure both as part of nonprofits and as an entrepreneur working with public transportation officials. Currently, he is Director of the Open Transport Partnership, a nonprofit organization operating the SharedStreets project, which builds freely-available open-source software, digital infrastructure, and governance frameworks to support public-private collaboration and the seamless privacy protecting exchange of transport data.[3] Prior to his work at Open Transport Partnership, Amicus worked in leadership roles at nonprofits that support the creation of public sector digital infrastructure. He also served as an "entrepreneur

---

[1] *See* David Alpert, *Why a battle between tech visionaries, privacy advocates, Uber, and transportation officials is about much more than scooter data*, GREATER GREATER WASH. (May 20, 2020), https://ggwash.org/view/77285/mobility-data-standard-scooters-bikes-autonomous-vehicles-uber-lyft-ddot-los-angeles. For context, the full quote is: "'We don't want to be accidentally creating the next redlining,' said one official who could not speak publicly. But, 'Do I think dockless [micromobility] is the thing that will push this over the line? Probably not.'"

[2] Pursuant to Fed. R. App. Proc. 29(a), no counsel for a party authored this brief in whole or in part, and no person other than amicus or their counsel has made any monetary contributions to fund the preparation or submission of this brief. All parties have consented to the filing of this brief.

[3] As part of his work with SharedStreets, Mr. Webb was invited in 2018 by LADOT to informally work with LADOT regarding the design of its data collection for dockless scooters. Mr. Webb initially endorsed the project, but later withdrew his support.

in residence" at Alphabet's urban technology incubator, Sidewalk Labs, where he collaborated with some of the world's leading experts on location data analysis and privacy. Given his experience in building digital infrastructure, Amicus has a significant interest in the factual claims dismissed by the district court on its Rule 12(b)(6) motion.

SUMMARY OF ARGUMENT

This appeal arises out of the alleged large scale and indiscriminate collection of dockless scooter data by the City of Los Angeles and its Department of Transportation ("Appellees" or "LADOT"). As a precondition for authorizing the operation of scooter services, Appellees require the submission of individual, route-by-route, real-time data for every scooter, which Appellees term "Mobility Data Specification" or MDS.

As alleged by Appellant, MDS requires "granular trip data from the providers to LADOT about every ride taken within Los Angeles—including the starting point of the ride, the starting time of the ride, the end point for the ride, and the ending time of the ride. LADOT requires that start and end locations be provided in real-time, and the route that the trip took between those points provided after 24 hours." 3 Excerpt of Record ("ER") 311 ¶ 25. Again as alleged by Appellant, this data can be easily attributed to a specific individual, which allows the government to track a person's movements in real time. 3-ER-311–12 ¶ 28.

This wide-scale collection of data is a search pursuant to the Fourth Amendment. Under *Jones* and *Carpenter*, this warrantless collection of detailed location information uses technology that surpasses traditional surveillance methods and therefore is an unreasonable search. *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Even if considered an administrative search, MDS is not a reasonable search under *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822 (2002). In particular, when considering Appellees' objectives, there is no reasonable basis to collect the granular and real-time data required by MDS. As shown below, for each of Appellees' potential legitimate regulatory goals, there are well-known methods to accomplish the same goal without collecting the same volume or type of data required by MDS. Amicus has himself implemented and worked with transportation officials to create such systems in other jurisdictions, belying Appellees' purported need for the vast scope of data collected and stored under LADOT's MDS. By contrast, the type of data collected with MDS is not even helpful for some of these policy goals. For example, transportation planning goals require aggregate data, not records of individual rides like those provided by MDS.

Finally, the impacts of collecting this type and volume of data cannot be viewed in a vacuum. While Appellees have offered vague rationales for collecting

this data, it will no doubt eventually be used for other objectives once it is collected and stored, including for law enforcement purposes. Use of data and algorithms such as "geofences" to limit where scooters can operate in real-time could be a prelude to limit who can use public streets in ways that exacerbate existing structural inequalities, creating a risk of future algorithmic "redlining." News reports already detail how the Los Angeles Police Department ("LAPD") is using police "cruisers and helicopters" to chase down and arrest electric scooter riders.[4] And in other instances the LAPD "teamed up with some of the scooter companies and used new technology to disable many of the scooters," via remote control.[5] In the context of today's policing environment, the collection of a treasure trove of granular real-time transportation data that can easily be tied to a particular individual creates real and serious privacy concerns.

ARGUMENT

I. LADOT'S MDS DATA COLLECTION CONSTITUTES A SEARCH UNDER THE FOURTH AMENDMENT

New technologies do not vitiate our Fourth Amendment rights. *See* *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) (quoting *Olmstead v.*

---

[4] Bill Melugin, *LAPD cracking down on illegal electric scooter flash mobs taking over city streets*, FOX 11 L.A. (Nov. 13, 2019), https://www.foxla.com/news/lapd-cracking-down-on-illegal-electric-scooter-flash-mobs-taking-over-city-streets.

[5] *Only On 2: LAPD Stops 'Flash Scooter Mob' Takeover Of DTLA*, CBS L.A. (Sept. 22, 2019), https://losangeles.cbslocal.com/2019/09/22/lapd-stops-flash-scooter-mob-takeover-of-dtla/.

United States, 277 U.S. 438, 473–474 (1928)) ("[T]he Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections."). At a minimum, new technologies must protect the "degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). The Fourth Amendment's objective is "to curb arbitrary exercises of police power and prevent "a too permeating police surveillance."" *United States v. Jones*, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

A. The District Court Distinguished *Carpenter* and *Jones* Without Any Proper Basis

Applying old case law to rapidly expanding technologies is dangerous, and courts have been "careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. This is because "[t]he ever-accelerating pace of technological development carries serious privacy implications." *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527 (7th Cir. 2018). Relatedly, to avoid "embarrass[ing] the future," courts "must take account of more sophisticated systems" when crafting their rules. *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944); *Kyllo*, 533 U.S. at 36.

In both *Jones* and *Carpenter*, the Supreme Court held that location tracking constituted an unreasonable search. Here, the district court below held that location tracking did not constitute any search at all. While uncritically extending existing precedents can be dangerous, the district court here erred in the opposite way—by not faithfully applying existing precedent to similar circumstances. The district court distinguished Appellant's search-based claims from these precedents on three primary bases: (i) because the data collected was, according to the district court, anonymous; (ii) because the data was for a shared device, whereas the data in *Jones* and *Carpenter* were for private, individual devices; and (iii) based on application of the third-party doctrine. 1-ER-6–7. The district court's analysis was incorrect as a factual matter, as discussed below. But it also failed to consider the deference owed to Appellant's well-pleaded factual allegations in ruling on a motion to dismiss. Taking each point in turn:

Data "Anonymization": The district court acknowledged that Appellant alleged—with support from academic studies—that the collected MDS data can be readily "de-anonymized." 1-ER-6. The district court, however, failed to accept that allegation as true, as required on a motion to dismiss. That purportedly anonymous data can be readily tied to a specific individual is a fact of modern

society.[6] Despite this, the district court concluded the opposite, finding the anonymous data was the "most apparent" distinction from *Jones* and *Carpenter*. 1-ER-6.

The recent *en banc* decision in *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330 (4th Cir. 2021), explains the error in this analysis. It found that Baltimore's aerial surveillance program was a search even though the pictures generated were not clear enough to see an individual person. *Id.* at 343. No matter: The government "could use any number of context clues to distinguish individuals and deduce identity." *Id*. *Leaders* even credited ***the same study cited in Appellant's complaint***, stating: "Plaintiffs submitted research showing that, because people's movements are so unique and habitual, it is almost always possible to identify people by observing even just a few points of their location history." *Id.* "[T]he study shows that identity is easy to deduce from just a few random points of an individual's movements." *Id.* at 344. The district court erred in rejecting Appellant's factual allegations that "anonymous" data could be easily combined with other public information to deduce a person's identity.

The district court's error in rejecting Appellant's well-pleaded, and amply supported, allegation that data can be easily "de-anonymized" is particularly

---

[6] *See* Boris Lubarsky, *Re-Identification of "Anonymized Data*," 1 GEO. L. TECH. REV. 202, 203 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

problematic for the type of data collected here. Because in all but the rarest instances no two people take the same precise journey at the same time unless traveling together, trip data is "data that can be indirectly, yet unambiguously, linked to an individual." *See* Boris Lubarsky, *Re-Identification of "Anonymized Data*," 1 GEO. L. TECH. REV. 202, 203 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

Shared Device: The district court also found that de-anonymization alone was insufficient to turn MDS into a search because the scooter devices are shared, rather than private devices as in *Jones* and *Carpenter*. 1-ER-6–7. In other words, the district court reasoned, de-anonymizing scooter data does not necessarily reveal which specific individual was using the scooter. This proposition is factually incorrect: researchers have demonstrated that anyone with knowledge of even rudimentary data analysis methods can easily identify specific users from public trip data and reveal sensitive travel histories. *See* Anthony Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, WORDPRESS (Sept. 15, 2014); Morgan Herlocker, *Citizen Privacy and City Oversight Needs Are Compatible: Our views from the California Senate hearing*, SHAREDSTREETS (Feb. 26, 2020), https://medium.com/sharedstreets/citizen-privacy-and-city-oversight-needs-are-compatible-26fb262cc7a. Moreover, the district court's finding again

fails to credit Appellant's well-pleaded factual allegations that, even in the shared scooter context, location history for a specific person can be "readily de-anonymized." 1-ER-6.

The only purported barrier to compiling the data that the district court identified is that it may be a time intensive project. 1-ER-7 n. 6. But this is exactly the type of barrier that modern data analysis methods can easily resolve, by using contextual data to identify an individual even in the context of shared modes of travel, such as rental scooters or taxis. *See* Tockar, *supra* (identifying where one of Hustler's customers lives, his property value, ethnicity, relationship status, court records, a profile picture, and other establishments he frequented from taxi data supplemented with public data).

Third-Party Doctrine: Finally, the district court found that Appellant did not have a reasonable expectation of privacy in this type of location data because it was shared with a third party (scooter companies). 1-ER-7. But as courts have begun to recognize, *Carpenter's* exception to the third-party doctrine is not limited to cell phone location data. *See Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527 (7th Cir. 2018).

Instead, where technological advancements "enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [the Supreme Court] has sought to "assure [ ] preservation of that degree of privacy

against government that existed when the Fourth Amendment was adopted.'"' *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

The third-party doctrine does not override this basic protection of the Fourth Amendment. The Supreme Court first questioned the applicability of the third-party doctrine in 2009. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). Nine years later, the Supreme Court "decline[d] to extend *Smith* and *Miller* to cover" CSLI data—"a detailed and comprehensive record of the person's movements." *Carpenter*, 138 S. Ct. at 2217. *Naperville* further declined to extend the third-party doctrine to an individual's energy consumption data. *See Naperville*, 900 F.3d at 527. *Naperville* reasoned that "a choice to share data imposed by fiat is no choice at all," and without a choice the third-party doctrine is inapplicable. *Id*.

Just as in *Naperville*, this court should find the third-party doctrine inapplicable because the *Carpenter* exception applies to more than just cell phone data. First, whether or not Appellant has a "choice" to ride a scooter or to share his location data is a factual question that is inappropriate to resolve at the motion to dismiss stage. Depending on how frequently Appellant uses dockless scooters, he

may be completely dependent on them for essential aspects of his life such as commuting to work or school. Second, just as in *Carpenter*, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected" in this case. *Carpenter*, 138 S. Ct. at 2219. "[T]he fact that such [physical location] information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 2223. Accordingly, Appellant's right to privacy should not be shed merely because he is required to share his information to access and utilize the dockless scooters.

MDS's encyclopedic collection of location data—both historically and in real time—creates the same type of constitutional concerns that *Carpenter* and *Jones* found to be searches pursuant to the Fourth Amendment. Because this detailed personal data can be "easily" traced to a single individual under Appellant's allegations, it constitutes an illegal search.

II. MDS IS NOT A PERMISSIBLE ADMINISTRATIVE SEARCH BECAUSE IT IS UNREASONABLE WHEN THE GOALS OF THE GOVERNMENT ARE CONSIDERED

Both parties agree that MDS, if it is a search, is an administrative search. 1-ER-9. Administrative searches are tolerated so long as they are "appropriately limited." *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000). An analysis of the reasonableness of an administrative search focuses on: (i) "the nature of the

privacy interest allegedly compromised," (ii) "the character of the intrusion imposed by the Policy," and (iii) "the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them." *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 830–34 (2002).

A. Data Can Be Helpful to LADOT For Planning, Oversight, and Enforcement; But None of These Purposes Justify the Granular Data That LADOT Demands

The district court, largely based on its own analysis, found that "the government's interests are legitimate and substantial," including to avoid scooters cluttering sidewalks, lacking safety features, or interfering with disabled access to city streets. 1-ER-9. The district court then found that the data MDS collects is "immensely useful" for regulating city transportation, and thus reasonable under *Earls*. *Id.* at 10.

The district court cites *Naperville* for the proposition that effective regulation requires data. 1-ER-9. Amicus agrees. Regulators have both a need for and a right to data to develop effective policy and to regulate private sector operators of mobility services. But all data is not equal, and the volume, granularity, and type of data must be carefully considered as compared to specific regulatory objectives. Data collection (and retention) methods should be designed to serve specific regulatory purposes. *Earls* requires balancing the nature and

character of the privacy intrusion against the "government's concerns and the efficacy of the [search] in meeting him." *Earls*, 536 U.S. at 830–34.

Applying *Earls* in today's modern and data-centric world, the government should not be collecting data for which there is little or no justification. Such a search would fail the *Earls* balancing test because the "government's concerns" and the efficacy of the search would not match up with the nature and character of the privacy intrusion. Accordingly, ***data minimization***—that is, collecting and keeping only what is necessary—must be accounted for when the government is collecting this type of data.[7] Put simply, data must be collected with and proportional to a specific and legitimate policy purpose.

Naperville allowed the collection of granular data because it was necessary to the specific, stated regulatory purpose. *See Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 529 (7th Cir. 2018) ("[O]ur holding depends on the particular circumstances of this case. Were a city to collect the data at shorter [more privacy invasive] intervals, our conclusion could change."). The issue with MDS is not that Appellees do not have the right to collect ***some*** data. Instead, to be reasonable, Appellees have a responsibility to first define the regulatory purposes as a prerequisite step and then narrowly tailor its data collection to support those purposes. It has not done so. While Appellees have not

[7] Even LADOT agrees that data minimization must be accounted for. 2-ER-231.

articulated all its specific objectives in the context of the motion to dismiss below, based on Amicus's experience and widely known literature in the field, data can be helpful for planning, oversight, and enforcement objectives. Each of these categories requires differing granularity of data for effective regulation, but none supports the collection of the amount and detail of data required by MDS.

1. Planning Requires Aggregate Data, at Most

Data can be helpful for planning the transport infrastructure of a city. An example is deciding whether to add a bike lane to the city transport grid. To effectively plan, regulators may need access to historical and carefully aggregated data. *See* HUGH LOUCH ET AL., INNOVATION IN BICYCLE AND PEDESTRIAN COUNTS (2016), https://altago.com/wp-content/uploads/Innovative-Ped-and-Bike-Counts-White-Paper-Alta.pdf. By design, "planning" does not occur by fiat or in real time; planning is a collective, forward-looking process through which communities interpret their needs and design responses.

Importantly however, planning does not occur by anecdote, but rather by understanding behavior in the aggregate. Individual trips alone are in a sense irrelevant to transportation planning. Knowing that one person traveled from location A to B should not by itself affect planning for transportation infrastructure. It is only travel patterns in the aggregate, either based on analysis of historical data or the creation of future projections, that are relevant to planning. In

fact, the direct use of disaggregated personal data, like citizen-generated trip information, actually undermines public discourse crucial to planning processes because that data cannot be freely shared with the public.

The district court suggests that the expansive collection of "robust data" is necessary for regulation—even without a guiding policy question. 1-ER-9. This is incorrect. *See generally* Lisa Gitelman, *Raw Data Is an Oxymoron* (2013); Mitchell Whitelaw, *This is Data? Arguing with Data Baby*, BLOGGER (May 19, 2010), http://teemingvoid.blogspot.com/2010/05/this-is-data-arguing-with-data-baby.html. Further, the history of quantitative social sciences demonstrates that collection of policy-relevant data depends on the careful design of collection methods to mitigate potential bias and to ensure data is accurate and relevant to the questions at hand. *See generally* Joshua M. Epstein, *Why Model?*, J. ARTIFICIAL SOC'YS & SOC. SIMULATION, no. 4, 2008, https://www.jasss.org/11/4/12.html (stating theories precede and guide data collection because without scientific theories it is not clear what data to collect).

Contrary to the district court's analysis, transportation organizations do not need the individual trip data collected by MDS for planning purposes. There are many feasible—and commonly used—ways to aggregate this data to give the government meaningful information and protect citizens privacy. One method that has already been applied to mobility data is K-anonymization clustering. Morgan

Herlocker, *Aggregating Trip Data Using K-Anonymization*, SHAREDSTREETS (July 21, 2021), https://medium.com/sharedstreets/aggregating-trip-data-using-k-anonymization-727d5a6413f3. This is a simple, widely used technique that sets a threshold privacy level which stands for the number of trips that originate in a designated geographic area. Both the threshold level and the designated geographic area can be easily adjusted to achieve the desired level of granularity. *Id*. The technique then filters out any trips that do not meet that threshold level as that information would reveal too much about an individual. *Id*.

Another option is Synthetic Simulation which has also already been applied to mobility data. *See* Cherish Weiler, *Replica: Informing Urban Planning with Synthetic Simulations*, HBS.EDU (July 21, 2021), https://digital.hbs.edu/platform-digit/submission/replica-informing-urban-planning-with-synthetic-simulations/#. Synthetic data operates by taking the raw data for each trip in a defined geographic region and translating it into a "travel behavior model" which is attached to a synthetic person. *Id*. This synthetic person, representing an entire region, can then simulate a week of someone's trips to show how the population moves over a period. *Id*.

2. MDS Fails to Effectively Serve Structural and Operational Oversight

The second category of transportation regulation is oversight of mobility operators. Oversight falls into two categories: structural oversight and operational

oversight. Structural oversight examines the behavior of companies and the impact they have on communities. Structural oversight of mobility operators is not concerned with citizens' whereabouts, but rather assessing the often negative externalities of mobility services (*e.g.*, how different business models impact access to mobility, how different pricing models shape customers' travel behavior, or the effect of different compensation structures on the wages and economic security of workers operating mobility services). *See* Rusul L. Abduljabbar et al., *The role of micro-mobility in shaping sustainable cities: A systematic literature review*, 92 TRANSP. RES. PART D: TRANSPORT & ENV'T article 102734 (2021); Joseph Hollingsworth et al., *Are e-scooters polluters? The environmental impacts of shared dockless electric scooters*, 2019 ENVTL. RES. LETTERS 14 (2019), https://iopscience.iop.org/article/10.1088/1748-9326/ab2da8.

Implementing structural oversight of this nature is a long-standing challenge for regulators. However, MDS trip data is an ineffective tool for structural oversight of mobility companies because it focuses on data about the precise movement of vehicles (and in turn, their riders), rather than defining a more expansive understanding of the companies' operational and economic performance crucial to many current regulatory challenges. For example, one concern of structural oversight is the number and compensation of individuals working for mobility companies as so-called "gig workers." Some scooter operators use

independent contractors to deploy and charge their fleets on a per-scooter basis. Yet, MDS collects no information about how mobility fleets are managed, or the arrangements between mobility companies and the workers that operate these services—or how many miles workers drive to collect, charge, and redistribute scooters. MDS provides no data to support answering this critical question regarding the economic viability and environmental impact of shared mobility services.

Structural oversight of mobility firms based on collection of citizen-generated personal location data is akin to regulating banks based on the collection of individual citizens' checking account ledgers—it simply does not accomplish its objective of better understanding systemic risks, or empowering regulators to prevent harmful practices. Like bank regulators, mobility regulators should be more interested in the ledger reflecting the actions and performance of ***the company***, rather than in the data about actions of any specific customer. In this regard, aggregate data about how people use mobility services and how a company manages that demand is substantially more relevant for structural regulation than disaggregated trip information. This data is similar to aggregate data collected for planning, but a key difference is that it allows regulators to differentiate and examine the impact of individual companies in the context of broader mobility policy concerns. As shown above in Section II(A)(1), data of this nature can be

collected in aggregate forms that pose no risk to citizen privacy. *See* Grant McKenzie, *Urban mobility in the sharing economy: A spatiotemporal comparison of shared mobility services*, 79 COMPUTERS, ENV'T AND URB. SYS. article 101418 (2020), https://www.sciencedirect.com/science/article/pii/S0198971519303060.

In contrast to structural oversight, operational oversight does require ongoing, and potentially even real-time, data to monitor day-to-day adherence to permit requirements and hold companies accountable. Examples of operational oversight split into two types: (i) an individual customer's dispute about, for example, a receipt for a trip, or (ii) a broader regulatory requirement such as the number of vehicles deployed, or that vehicles are deployed in appropriate locations, as stipulated in a permit. *See* GUIDELINES FOR REGULATING SHARED MICROMOBILITY (NATIONAL ASSOCIATION OF CITY TRANSPORT OFFICIALS 2019). On the individual level, regulators need access to specific customer records to adjudicate a specific complaint. At the broader level, detailed information about the fleet as a whole may be needed.

Neither of these types of operational oversight requires the government to collect detailed location data about individual customer trips. The broader regulation does not implicate citizens' trips at all. And at the individual level the government merely needs to access data about, at most, a specific trip to address individual complaints. In this regard, MDS actually fails to meet the needs of

adjudicating complaints, as the de-identified data it collects is insufficient for ensuring that mobility service operators uphold their obligations to customers. A better designed operational oversight framework would collect aggregate information to proactively ensure companies are meeting their operational obligations, and at the same time define a mechanism through which the government can compel access to detailed individual trip information ***on behalf of citizens*** (and with their explicit consent, and necessary privacy guardrails in place) in response to a specific complaint. Oversight systems such as this are commonly used by taxi regulators and could even be improved by the LADOT with more modern practices. *See* Ryan Browne, *Uber stripped of its London license as regulator says it put passengers at risk*, CNBC (Nov. 25, 2019), https://www.cnbc.com/2019/11/25/uber-stripped-of-its-london-license-in-huge-blow-dealt-by-tfl.html.

Under *City of Los Angeles v. Patel*, it could be entirely appropriate for the scooter companies to provide individual trip data on an as-needed basis to the government. 576 U.S. 409 (2015) (hotel operators provide specific guest information upon request). But the *Patel* court explicitly acknowledged that even the threat of falsifying the data did not warrant giving the government access to the hotel data in the first instance. *Id*. at 427. The solution to falsified data is an audit, not the *ex ante* over-collection of data by the government in the first instance. In

the mobility data context, there are many data compliance technologies and practices available to audit and to ensure that any data shared with regulators is accurate and complete, including sharing of "hashed" signatures of individual records or using immutable, auditable logs. *See* Mustafa Suleyman & Ben Laurie, *Trust, Confidence and Verifiable Data Audit*, DEEPMIND (July 21, 2021), https://deepmind.com/blog/article/trust-confidence-verifiable-data-audit.

3. Enforcement Is Not Possible Given the Precision of the GPS Location Data Collected by MDS Today

The third type of regulatory purpose in this context is enforcement. Enforcement does require real-time identification of violations. Examples of enforcement include identification of traffic safety violations such as speeding or illegal parking, and other rules regulating travel behavior in the name of public safety. Enforcement could require analysis of real-time information from vehicles while in motion.

However, enforcement of traffic safety using the GPS data collected by MDS is not possible. This is because the accuracy of the scooter's GPS data, in practice, is only accurate to a few dozen of feet,[8] 3-ER-313 ¶ 30; this makes it

[8] Mobility devices can convey their geolocation data via GPS coordinates out to seven decimal places, which corresponds to a level of accuracy within 1.11 centimeters at the equator. This is what the API requests, but in current practice travel data derived from GPS sensors in an urban environment is less precise, often providing positional accuracy of approximately 10 meters. This is too imprecise to accomplish LADOT's stated goals, like parking enforcement (a street parking

impossible to monitor speed or accurately assess any parking violation. *See* Morgan Herlocker, *Using Location Data for Guiding Micromobility Outcomes*, SHAREDSTREETS (Mar. 26, 2019), https://sharedstreets.io/using-location-data-for-guiding-micromobility-outcomes/. Further, many scooters have temporal delays that can slow the data collection by up to thirty seconds, which prevents enforcement from occurring in real time as well. *See* John Seabrook, *The E-Scooters Loved by Silicon Valley Roll Into New York*, New Yorker (Apr. 19, 2021), https://www.newyorker.com/magazine/2021/04/26/the-e-scooters-loved-by-silicon-valley-roll-into-new-york/. Moreover, violations of speed limits or illegal parking do not require knowledge of the route that an individual took. Thus, detailed route information about each trip is not even necessary for those enforcement purposes.

By contrast, there are technologies available that are better suited to accomplish this type of enforcement but that do not require transmitting or collecting real time location data. For example, a company named Luna employs scooters which use on-board software and computer vision systems to regulate speed and location constraints. *See* LUNA, HTTPS://LUNA.SYSTEMS/ (LAST VISITED

---

space for a car is often about 3 meters long) or identifying sidewalk riding. But it is more than accurate enough to precisely identify a specific trip and traveler identity. In all but the rarest circumstances, no two people travel to and from the same 10-meter origin and destination at the same time unless they are traveling together. *See* Tockar, *supra*.

JULY 21, 2021); Superpedestrian, *Pedestrian Defense - LINK Scooters by Superpedestrian,* (July 19, 2021), https://www.youtube.com/watch?v=3kSYnFPc80Y. Similar on-board sensing technology is used by other scooter systems to overcome the limits of GPS-based safety enforcement. Techniques similar to those used by Luna and Superpedestrian scooters are also widely used in autonomous vehicle systems and the Advanced Driver Assistance Systems available in most modern cars. None of these safety systems require sharing of sensitive travel data *en masse*. LADOT and other transportation organizations can use this type of technology (or similar technology) to accomplish its enforcement goals without requiring the real time location data to be collected by the government in wholesale fashion. Instead, Appellees can require deployment of appropriate traffic safety enforcement technologies on the scooters, and audit companies to hold them accountable.

B. MDS Is an Administrative Search That Is Not Appropriately Limited, and Therefore Is Unreasonable

An analysis of the reasonableness of an administrative search focuses on: (i) "the nature of the privacy interest allegedly compromised," (ii) "the character of the intrusion imposed by the Policy," and (iii) "the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them." *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 830–34 (2002). The nature of the privacy interest and the character of the intrusion

imposed by MDS involves the government knowing detailed route information about every single scooter ride that any individual takes in Los Angeles. This detailed route information can "reflect[] a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

As explained above, none of the planning, oversight, nor enforcement policies require the comprehensive collection of the detailed individual trip information that Appellees demand in MDS. In each category—planning, oversight and enforcement—Amicus has provided not only an explanation of why MDS data is not helpful or relevant, but also specific examples of accomplishing the same goals through less invasive means. ***Given this large mismatch between the need for the MDS data and the available methods to accomplish the relevant objectives without it, MDS's mass data collection practice cannot be reasonable under Earls.***

While the government is not required "to adopt the least intrusive practicable alternative, there must be a fairly close fit between the weight of the government's interest in searching and the intrusiveness of the search. *Ruskai v. Pistole*, 775 F.3d 61, 69 (1st Cir. 2014). There is far from a "close fit" in this instance. *See also Mann v. Cty. of San Diego*, 907 F.3d 1154, 1166 (9th Cir. 2018) (citing *Earls*, 536 U.S. at 829) ("Nor has the County demonstrated that compliance with the

Fourth Amendment, i.e., providing parental notice and obtaining consent or judicial authorization, would be "impracticable.""); *see also Lebron v. Sec'y, Fla. Dep't of Child. & Fams.*, 710 F.3d 1202, 1213 (11th Cir. 2013).

More data does not mean better data. Appellees' concerns and the efficacy of the policy in meeting them do not justify collecting this data absent the government identifying how this detailed data would help with regulation. While aggregate data can help with planning and access to specific individual rides can aid with individual operational oversight, giving the government the keys to the entirety of the raw location data generated by the traveling public does not benefit regulation and needlessly interferes with its citizens' privacy rights.

III. ALLOWING SEARCHES OF THIS NATURE WILL LEAD TO INCREASED RISK OF DISCRIMINATORY ENFORCEMENT

Giving Appellees unconstrained access to both detailed travel information and expanded enforcement capabilities linked to travel behavior opens the door for discriminatory policy. Laws that pave the way for discriminatory enforcement, in part through expanded surveillance capabilities that violate Fourth Amendment rights, are disfavored. *See Papachristou v. City of Jacksonville*, 405 U.S. 156, 162 (1972) (striking down a city ordinance in part because "it encourages arbitrary and erratic arrests and convictions."). The City of Los Angeles is no stranger to this. *See Desertrain v. City of Los Angeles*, 754 F.3d 1147, 1149 (9th Cir. 2014) (striking down statute against living in parked cars because it "promotes arbitrary

and discriminatory enforcement."). Access to detailed information with no guiding principles or stated direction could "lend[] itself to harsh and discriminatory enforcement by local prosecuting officials, against particular groups deemed to merit their displeasure." *Thornhill v. State of Alabama*, 310 U.S. 88, 97–98 (1940).

In fact, the potential for discriminatory policy is already visible in the two-tiered enforcement system MDS enables today, with one set of rules (and privacy risks) for personally owned cars, and another more arbitrary and invasive set of rules for those who depend on shared services. The district court appeared to accept this inequity when stating that, "Riding a one-time rental scooter is not indispensable to modern life." 1-ER-8. This ignores that the "indispensability" of a given mode of travel may be more a matter of access, or economic circumstance than preference. And the combination of new data collection methods with new, unconstrained forms of algorithmic enforcement, such as "geofences," further expands the tools for implementing discriminatory policy.

With MDS, Appellees are not simply managing new mobility services, they are responding to this moment of technological change by proposing an expansion of the surveillance and enforcement capabilities that govern our use of public space. Yet history contains many corollaries of these practices that have been implemented (and abused) by police and urban policy makers. *See generally* Sarah

Schindler, *Architectural Exclusion: Discrimination and Segregation Through Physical Design of the Built Environment*, 124 Yale L.J. 1934 (2015). The lessons learned from these past steps (and missteps) inform how we understand both the Fourth Amendment and our collective right to use public space free from surveillance and arbitrary and discriminatory enforcement. *See Ex parte Daniels*, 183 Cal. 636, 639 (1920) ("The streets of a city belong to the people of the state, and every citizen of the state has a right to the use thereof, subject to legislative control.").

In *Papachristou v. City of Jacksonville*, the Supreme Court recognized the harm created by laws that enable arbitrary enforcement on public streets, and in turn their dependence on, and improper justification of surveillance. *See* 405 U.S. 156, 164 n. 6 (1972) (quoting Charles Reich, *Police Questioning of Law Abiding Citizens*, 75 YALE L.J. 1161, 1172 (1966)) ("If I choose to take an evening walk to see if Andromeda has come up on schedule, I think I am entitled to look for the distant light of Almach and Mirach without finding myself staring into the blinding beam of a police flashlight."). In *Police Questioning*, Reich recounted his frequent, and unconstitutional encounters with law enforcement when driving alone as a (then closeted) gay man:

> Although the experiences I have had are in themselves trivial, the increasing preventive activities of the police present an issue of first importance. What happens when the person stopped is [Black], or poor, or frightened? What intrusions upon privacy, what affronts to dignity, occur? How much

> discretion do the police have to invent an offense for anyone who objects to being questioned? May the police establish a regular routine of requiring pedestrians to carry identification and explain their presence, or of requiring motorists to stop and tell where they are going?

75 YALE L.J. 1161, 1162 (1966).

Today we are still grappling with the questions Reich asked about the relationship between policing and public life. Yet we now also have the technical ability to trigger even more invasive investigatory inquiry through entirely automated means, as part of routine administrative policy. This should give us pause.

As *Papachristou* noted, and *Desertrain* and *Leaders of a Beautiful Struggle* affirm, many ordinances that require expanded surveillance in the name of improving public life are either driven by discriminatory animus or exacerbate existing structural injustice in ways that render their intentions irrelevant. Without constraints, new technologies simply give the government new mechanisms to implement these old ideas, reducing the cost of enforcement, and obscuring both discriminatory intentions or outcomes behind a veneer of modern, tech savvy urbanism.

CONCLUSION

For the foregoing reasons, Amicus believes the district court decision should be reversed.

DATED: July 30, 2021

Respectfully submitted,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By: /s/ *Jordan R. Jaffe*
Jordan R. Jaffe

Counsel for *Amicus Curiae* Kevin Webb

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing Brief of Amicus Curiae Kevin Webb with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 30, 2021 */s/ Jordan R. Jaffe*

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,294 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Word Times New Roman 14-point font.

/s/ *Jordan R. Jaffe*
Jordan R. Jaffe