No. 21-55285

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN SANCHEZ,

Plaintiff-Appellant,

v.

LOS ANGELES DEPARTMENT OF TRANSPORTATION, *et al.*

Defendants-Appellees.

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

BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AND ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

Brian E. Klein
Melissa A. Meister
WAYMAKER LLP
777 South Figueroa Street, Suite 2850
Los Angeles, CA 90017
(424) 652-7800
bklein@waymakerlaw.com
mmeister@waymakerlaw.com

Samir Jain
Gregory T. Nojeim
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, DC 20005
(202) 637-9800

Alan Butler
Megan Iorio
Melodi Dincer
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *Amici Curiae* Center for Democracy & Technology and the Electronic Privacy Information Center state that neither have parent corporations and that no publicly held corporation owns 10% or more of either of their stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF THE *AMICI CURIAE*[1]

The Center for Democracy & Technology ("CDT") is a non-profit public policy organization that works to promote democratic values and constitutional liberties—including free expression, privacy, and open access. In modern times, when new technologies have given governments unprecedented means to access an individual's private information, CDT advocates for the protection of both security and freedom through balanced laws and policies that preserve government accountability and provide meaningful checks on governments' ability to access, collect, and store individuals' private data.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., that focuses public attention on emerging privacy and civil liberties issues in the information age. EPIC routinely participates as *amicus curiae* in cases concerning constitutional rights and emerging technologies.

---

[1] The parties consent to the filing of this brief. No counsel for any party authored this brief, in whole or in part. Apart from *amici curiae*, no person contributed money intended to fund this brief's preparation and submission.

INTRODUCTION AND SUMMARY OF ARGUMENT

In *1984*, George Orwell presciently observed that, "[b]y comparison with that existing today, all the tyrannies of the past were half-hearted and inefficient. . . . Part of the reason for this was that in the past no government had the power to keep its citizens under constant surveillance." Historically, local, state, and federal governments had to expend significant resources to surveil citizens, and technology dramatically limited the types and amount of information that could be collected. With the advent of cellular telephones, dockless mobility platforms, and other technologies that generate sensitive data such as Cell Site Location Information ("CSLI"), Global Positioning System ("GPS") data, as well as data covered by the Mobility Data Specification ("MDS"), precise tracking of an individual's movements has become all too easy for the government. A government need only compel location data from a third party to track both real-time and historic movement patterns and, absent legal constraints, can maintain such data *indefinitely*.

Collection of precise location data implicates significant and fundamental privacy interests, and courts have held that such data cannot be accessed by law enforcement without a warrant under the Fourth Amendment. Location information, including data about electronic scooter use, can be used to track an individual's movements and can easily reveal a comprehensive record of their

family, political, professional, religious and sexual associations. Even if such data is initially "anonymized" it is easily susceptible to re-identification by both the government and the public at large.

Constant warrantless tracking of private vehicles would unquestionably run afoul of the Fourth Amendment. Yet, the district court below dismissed Appellant Justin Sanchez' case challenging warrantless tracking at the motion to dismiss stage, without even the benefit of discovery and oral argument, because the tracking concerned use of electronic scooters instead of private cars. Such a decision runs the very real risk that the Fourth Amendment will become a luxury for those who can afford private vehicles, private residences, and high walls, while those who utilize smartphone applications to share micromobility devices, vehicle services such as Uber and Lyft, and lodging such as Airbnbs become second-class citizens under the United States Constitution. This is not, and should not be, the state of the law and this Court should reverse the district court's grant of Appellee City of Los Angeles and Los Angeles Department of Transportation's (collectively, the "City's") motion to dismiss and remand for further proceedings.

ARGUMENT

I. THE CITY'S MDS PROGRAM IMPLICATES FUNDAMENTAL PRIVACY INTERESTS THAT GENERALLY REQUIRE A WARRANT UNDER THE FOURTH AMENDMENT.

In cities such as Los Angeles, electric scooters and other dockless micromobility devices (collectively, "e-scooters") are popular with individuals who are looking for relief from traffic congestion and road rage, lack access to adequate public transportation systems, cannot afford an automobile, or who need to get to locations where automobiles are prohibited, such as beach boardwalks. E-scooters are generally outfitted with GPS trackers and wireless connectivity to the Internet to track rides for the provider to charge the user accordingly and to locate the e-scooter should it need to be moved or serviced.

As e-scooters began to rise in popularity and show up in various locations around the City of Los Angeles, the City developed the MDS,[2] which allows the City to not only access the current, real-time location of an e-scooter, but also a route history of that e-scooter's daily trips. *See* Alexander P. Carroll, *New Technology and the Right to Privacy: Do E-Scooters Implicate the Fourth*

[2] Although originally developed by the City, MDS is now being developed by the Open Mobility Foundation, https://www.openmobilityfoundation.org/about.

Amendment?, 40 J. Nat'l Ass'n Admin. L. Judiciary 27, 33 (2021).[3] The MDS accomplishes this through a set of Application Programming Interfaces, more commonly known as APIs, which standardize the government's ingestion of data from mobility companies such as Lyft, Bird, JUMP, and Lime. *See id.* These APIs interface directly with the mobility companies' databases and, as such, are invisible to the end user who may not be aware that the government is precisely tracking his or her e-scooter jaunt. The mobility companies are required to use MDS and provide information about their users to the city in order to operate within the City of Los Angeles; there is no opportunity to opt out. *See id.*

Ostensibly, the City's reasons for requiring that mobility companies use MDS and share individualized location data is to manage the equitable distribution of e-scooters throughout the City of Los Angeles, to decrease congestion and increase efficiency, and to promote safety. *See id.* at 33-34. Certainly, the citizenry's rising use of e-scooters provides challenges to a large city whose roads and sidewalks were not necessarily designed with such modes of transportation in mind. Yet the data collected by the MDS's APIs is both individualized and particularized—it records both real-time and historical data about every e-scooter

[3] *Available at* https://digitalcommons.pepperdine.edu/naalj/vol40/iss2/2/.

trip taken in the City of Los Angeles, including that e-scooter's start time, end time, and the route it took (or is taking) during the ride, even in situations where the e-scooter leaves the City of Los Angeles. *See* CDT, *Smart Enough Cities – Governments that Seek Mobility Data Must Respect Individual Privacy*, June 2020, at 4-5.[4] It is also extremely precise in that it captures the GPS coordinates broadcast by the e-scooters up to seven decimal places. In other words, the City's MDS system can track—in real time or historically—an individual e-scooter user from their home address to any point in—or outside—the City of Los Angeles within a few dozen feet of accuracy and maintain that information *indefinitely*. As a result, individuals who use e-scooters are unknowingly subject to the granular tracking of their every movement.

The government could not obtain such detailed location information without a warrant if the individual were using their own automobile. *See United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J. concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its

---

[4] *Available at* https://cdt.org/insights/report-smart-enough-cities-governments-that-seek-mobility-data-must-respect-individual-privacy/. The particular data fields captured by MDS' APIs include "device_id", "vehicle_id" (the type of e-scooter), "trip_id," "route", "start_time", and "end_time".

unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"); *id.* at 430 (Alito, J. concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."). The result should be no different if the individual is using an e-scooter instead of a car. The Fourth Amendment does not justify that distinction and neither do the stated goals of the City, which supposedly seeks only to regulate the public byways and encourage the equitable distribution of e-scooters across the City of Los Angeles.

A. E-Scooter Users Have a Privacy Interest in the Compelled Disclosure of Their Location Information Even if Initially Anonymized.

The particularized and precise nature of the information collected by MDS has the potential to reveal "a wealth of detail about [the person's] familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring). Such data can reveal, for example, an e-scooter user's visit to a high school, abortion clinic, church or mosque, marijuana dispensary, organized protest, and/or psychiatrist's office. *See People v. Weaver*, 12 N.Y.3d 433, 441-42 (2009). The government's "unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Jones*, 565 U.S. at 416

(Sotomayor, J. concurring). In the information age, that abuse can come not only from the government itself, but also from third-party hackers and data miners who would seek to exploit such data (and the government's poor track record in protecting such data) for their own ends.

MDS supposedly anonymizes the extensive data it requires from e-scooter companies by not collecting the end user's personally identifying information ("PII"), such as name and credit card information. But location data is, by its very nature, easily susceptible to re-identification. In one study, researchers were able to re-identify 95% of the 1.5 million people represented in anonymized mobile phone location data (which is far less precise than the GPS data MDS captures) from just four data points. *See* Yves-Alexandre de Montjoye, *et al.*, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature (2013).[5] With just two data points, the researchers were able to re-identify more than 50% of the people in the dataset. *Id.*

In 2014, data collected by the New York City Taxi and Limousine Commission that tracked taxi pickup and drop-off times, locations, fare and tip amounts, and anonymized versions of the taxis' license and medallion numbers,

---

[5] *Available at* https://www.nature.com/articles/srep01376.

was obtained by a Freedom of Information Law ("FOIL") request and released online. *See* Anthony Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, Neustar (Sept. 15, 2014).[6] Not only were the anonymized versions of the taxis' license and medallion numbers quickly de-anonymized, but even some passengers were re-identified by cross referencing their trip data to other publicly available data. *See id.*

Several of the cities who employ MDS have recognized that individualized trip data can be re-identified and, therefore, that substantial privacy interests exist in the data. At least three cities have refused to release the individualized and precise data they collect through the MDS system to the public in response to FOIL requests: San Diego, San Francisco, and Seattle. San Francisco and Seattle release the data but aggregate it to minimize the risk of reidentification.[7] San Diego does not appear to release the information at all. Indeed, in a privacy study

---

[6] *Available at* https://agkn.wordpress.com/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

[7] *See* SFMTA, *Powered Scooter Share Permit Program: Appendix 4 Data Reporting Guidelines and Requirements* at 1, *available at* https://www.sfmta.com/sites/ default/files/reports-and-documents/2021/03/ appendix_4_-_data_reporting_guidelines_and_ requirements_2021.pdf; City of Seattle, *Mobility Data Privacy and Handling Guidelines* (Dec. 30, 2019), *available at* http://www.seattle.gov/Documents/Departments/SDOT/NewMobilityProgram/ Mobility_Data_Guidelines_01142020.pdf.

performed by the law firm Kutak Rock LLP and commissioned by the San Diego Association of Governments ("SANDAG"), Kutak Rock opined that "[d]esignating Mobility Data as confidential PII will protect it from public disclosure, thereby reducing the risk that it will be re-identified and linked with individual riders." Kutak Rock LLP, *Privacy Impact Assessment for Micromobility Data* (August 2020).[8] Thus, even the very municipalities that employ MDS recognize its power to turn a so-called "smart city" into a surveillance state that is inimical to the Fourth Amendment.

Given these weighty privacy concerns, the district court below should have permitted Sanchez to fully explore the scope, aggregation, and alleged anonymity of the City's MDS data collection on private citizens and then examine information through the lens of the Supreme Court's Fourth Amendment jurisprudence. The Framers' intent, after all, in authoring the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Instead, the district court dismissed Sanchez's contentions without any discovery at all and without even the benefit of oral

[8] *Available at* https://www.sandag.org/uploads/publicationid/publicationid_4724_28377.pdf.

argument, effectively substituting its own judgment about Sanchez's arguments at the earliest possible stage of the litigation. This was reversible error.

B. E-Scooter Location Information Implicates Fourth Amendment Privacy Interests and Requires a Warrant Under Carpenter and its Progeny.

The purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Ct. of City and Cty. of San Francisco*, 387 U.S. 523, 528 (1967). The Fourth Amendment "protects people, not places[,]" *Katz v. United States*, 389 U.S. 347, 351 (1967), and given rapidly evolving and increasingly sophisticated technology, not only are people more mobile than ever, they are also more capable of having their precise location tracked, surveilled, and/or logged by government authorities. "[I]ndividuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). As technology enhances the government's "capacity to encroach upon areas normally guarded from inquisitive eyes," *id.* at 2214, it is incumbent upon the courts to assure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

The Supreme Court has already held—unanimously—that the warrantless tracking of an individual's movement through a GPS attached to a *vehicle* was

impermissible under the Fourth Amendment. *Jones,* 565 U.S. 400. In so holding, the Justices highlighted the particular sensitivity of location data: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 415 (Sotomayor, J. concurring). Much like the MDS data, the GPS data available in *Jones* was accurate to within 50-100 feet. *Id.* at 403. The Supreme Court has also held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements" as captured through CSLI. *Carpenter,* 138 S. Ct. at 2217. In so holding, the Supreme Court found that CSLI was "like GPS tracking of a vehicle" in that the location information "is detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216.

Of additional concern to the Court in *Carpenter* was the historical quality of the location data, which permitted the government to "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers." *Id.* at 2218. In the case of CSLI, wireless carriers maintained records for up to five years, *id.*, whereas in the case of the City, it is possible for the MDS system to retain the records indefinitely. Discovery in the case below, which the lower court erred in cutting off prematurely, would have permitted inquiry into how long the City intends to maintain the sensitive and individualized location data harvested from e-scooter users. *See Jones*, 565 U.S. at 415 (Sotomayor, J.

concurring) ("The government can store such records and efficiently mine them for information years into the future."). The longer such records are maintained in their individualized form, the greater the risk of re-identification.

The Court in *Carpenter* also made clear that location records that, "in combination with other information, deduce a detailed log of [a person's] movements" implicate the Fourth Amendment. *Id.* at 2218. In the case of *Carpenter*, other information was necessary because the CSLI was only accurate to within one-eighth to four square miles. *Id.* at 2218. Here, GPS technology is much more accurate than CSLI. And while "other information" may be necessary to re-identify an individual's movements, the constitutional precept is the same—both cases involve individually identifiable location records that should be protected under the Fourth Amendment.

Another particularly relevant example is *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330 (4th Cir. 2021), wherein an *en banc* panel of the Fourth Circuit considered the Aerial Investigation Research ("AIR") program, an aerial surveillance program of the Baltimore Police Department that utilized aerial photography to track historic movements related to serious crimes. *Id.* at

3.[9] The AIR program planes tracked around 90% of the City of Baltimore each day for twelve hours, weather permitting, and then maintained that data for 45 days. *Id.* Photographic resolution of images captured by the AIR program was limited to one pixel per person or vehicle, meaning that individuals could be made visible "but only as blurred dots or blobs." *Id.* Analysts on the ground would then analyze the AIR program data after serious crimes happened to determine whether the AIR program images could be utilized to track persons of interest related to those crimes. *Id.*

In holding that the AIR program likely constituted a warrantless search in violation of the Fourth Amendment, the Fourth Circuit found that the AIR program essentially permitted the government to access a "detailed, encyclopedic" record of where everyone came and went within the City of Baltimore over a month-and-a-half. *Id.* at 8. Although the AIR program was anonymized in that the persons of interest showed up as single pixels on the aerial photographs, the Court found that the pixels could easily be re-identified by governmental authorities using publicly available information, government data systems, and deductive reasoning. *Id.* at 9-10. In closing, the Fourth Circuit warned that the "Fourth Amendment must

---

[9] Because this case is not yet paginated, the page references are to the Westlaw printout of the case.

remain a bastion of liberty in a digitizing world" and that as technological advances in the name of advancing public safety arise, "the role of the warrant requirement remains unchanged[.]" *Id.* at 12.

C. The City's MDS Program is Part of a Broader Surveillance Trend by Cities to Collect Granular Data on Individuals' Daily Activities and Movements.

Although created by the City, MDS is now being adopted broadly—by 130 cities and public agencies so far. *Who is Using MDS?*, Open Mobility Foundation.[10] These cities and public agencies are located in the United States, Canada, and South America, meaning that an individual is now compelled—potentially, without his or her knowledge or agreement—to disclose his or her granular and particularized location information on a real-time (and historical) basis with multiple state and local governments every time that person rents an e-scooter, whether at home or abroad. This granular and particularized tracking of individuals has become so attractive to governments that cities and public agencies are looking to use MDS to also track users of ride-share companies such as Uber

[10] *Available at* https://www.openmobilityfoundation.org/mds-users/#cities-using-mds.

and Lyft. *See* CDT, *CDT Letter to Los Angeles World Airports Regarding Compelled Disclosure of Airport Visitor Information*, Dec. 16, 2020, at 1.[11]

For example, in a January 17, 2020 letter to the Los Angeles City Council, Los Angeles World Airports ("LAWA"), which operates LAX, stated that it was working with a consultant to "leverage MDS and LADOT's technology solution to facilitate the collection, tracking, and analysis" of Uber and Lyft operations around LAX "*in real-time* and to *an accuracy level* that allows LAWA to effectively manage and provide for more efficient ground transportation operations at LAX." 1/17/2020 Letter to Hon. Mike Bonin from LAWA. At 6-7 (emphasis in original).[12] LAWA also stated that it would steadfastly oppose any legislation that would hinder or limit its "data collection ability" and support any legislation that "strengthen[ed] the sharing of location data, trip origination and destination[.]". *Id.* at 7. By expanding MDS to other types of ride and vehicle sharing, the City is making it so that the Fourth Amendment is a luxury available only to those who can afford to purchase or lease, park, and fuel their own private vehicles.

---

[11] *Available at* https://cdt.org/insights/cdt-letter-to-los-angeles-world-airports-regarding-compelled-disclosure-of-airport-visitor-information/.

[12] *Available at* https://clkrep.lacity.org/onlinedocs/2018/18-0449_rpt_LAWA_01-17-2020.pdf.

The compelled disclosure of individualized and precise location information at the heart of this case is a facet of the larger effort by many cities to reimagine themselves as "smart cities," using data from connected devices to address every day, generalized problems like crowded streets, energy distribution, air quality, and trash collection. But increased compelled disclosure of citizens' data can erode their privacy such that these "smart cities" become "surveillance cities" and, in the name of so-called equitable distribution of mobility assets, the cities surveil those who may not be able to afford private vehicles free from the kind of individualized location monitoring that is the subject of this appeal. The Court below should have fully evaluated, with the benefit of discovery, whether MDS passed the point of privacy erosion that violated the Fourth Amendment. Because it did not, reversal is warranted.

II. THE CITY'S MDS PROGRAM DOES NOT MEET ANY RECOGNIZED EXCEPTION TO THE FOURTH AMENDMENT.

Contrary to the district court's view, the detailed, precise, pervasive, cheap, and efficient tracking of millions of Americans in previously impossible ways does not fall within an exception to the Fourth Amendment.

A. Courts Apply Exceptions to the Warrant Requirement Narrowly When Considering the Government's Use of Rapidly Developing Technology.

In the absence of a warrant, "a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley v. California*, 573 U.S. 373,

382 (2014). Generally, warrantless searches of location information that reveal an individual's presence in homes, offices, houses of worship, medical facilities, and other spaces that receive the highest protection under the Fourth Amendment is forbidden. *See, e.g.*, *Kyllo*, 533 U.S. at 40; *United States v. Karo*, 468 U.S. 705, 716 (1984). Further, "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. Put another way, courts are "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." *Id.* at 2223 (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting)).

For example, in *Kyllo*, the Court examined whether law enforcement's use of a new infrared technology, not generally available to the public, that detected heat emanating from a house (and thus the likely presence of heat lamps utilized to grow marijuana within) constituted a search within the meaning of the Fourth Amendment. 533 U.S. 27. The Court found that there were limits "upon this power of technology to shrink the realm of guaranteed privacy" and resisted "mechanical interpretation of the Fourth Amendment" that would leave an individual "at the mercy of advancing technology." *Id.* at 34-35. The Court also noted that the infrared technology it was dealing with in *Kyllo* was "relatively

crude" but the Court's Fourth Amendment jurisprudence "must take account of more sophisticated systems that are already in use or in development." *Id.* at 36.

In *Carpenter*, the Court dealt with CSLI, the precision of which was rapidly increasing on account of advances in the technology and the growth in the number of cell phone towers. In rejecting a mechanical application of the "third-party doctrine," which finds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), the Court found that it should show a "special solicitude for location information in the third-party context." *Carpenter*, 138 S. Ct. at 2219. In particular, given the "unique" ability of CSLI to record, store, and later provide to the government "a detailed and comprehensive record of [a] person's movements," the Court held that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 2217. This was true even though telecommunications companies collect CSLI for commercial purposes, just as mobility providers collect MDS data for commercial purposes, finding "that distinction does not negate [a person's] anticipation of privacy in his physical location." *Id.*

B. The District Court Erred in its Application of the Administrative Search Doctrine to Individualized E-Scooter Location Information Because MDS Does Not Meet the Exception's Narrow Requirements.

1. The Administrative Search Doctrine Applies Only to Industries More Closely Regulated than E-Scooters.

In addition to improperly holding, at the motion to dismiss stage without the benefit of any discovery at all, that compelled disclosure of information under the MDS standard was not a "search" under the Fourth Amendment, the district court also improperly held in the alternative that MDS was a permissible administrative search. First, administrative searches are only permissible where there is "such a history of government oversight that no reasonable expectation of privacy . . . could exist for a proprietor over the stock of such an enterprise." *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 313 (1978); *see also Camara v. Mun. Ct. of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967) (noting that this exception to the warrant requirement is narrowly defined). Such enterprises are limited to "pervasively regulated business[es]," *United States v. Biswell,* 406 U.S. 311, 316, (1972), or "closely regulated" industries "long subject to close supervision and inspection." *Colonnade Catering Corp. v. United States,* 397 U.S. 72, 74, 77 (1970). The mobility industry is neither.

In *City of Los Angeles v. Patel*, the Court held that hotels were not so "pervasively regulated" as to come within the administrative search exception to

the warrant requirement. 576 U.S. 409, 426 (2015). In so holding, the Court noted that it had identified only four industries that had such a history of government oversight that no reasonable expectation of privacy could be formed for an administrative search of such: liquor sales, firearms dealing, mining, and running an automobile junkyard. The Court reaffirmed that the "clear import of our cases is that the closely regulated industry . . . is the exception." *Id.* at 424 (internal quotation marks omitted).

In comparison to the City of Los Angeles hotel regulations the Court considered in *Patel*, e-scooters are far less regulated. Hotel purveyors must follow guidelines that regulate such aspects as workers' compensation, health and sanitation, and hotel service charges, and hotel guests must provide a significant amount of information to hotels depending on whether they have a reservation, are utilizing cash for payment, are checking into their room with a person or an automated system, and the length of their stay.

Yet, the *singular* universal requirement for e-scooter riders in the City of Los Angeles is that the riders must possess a valid driver's license. *See* Cal. Veh. Code § 21235. As for e-scooter providers, they are required to obtain a permit (as every business in the City is required to do), carry general commercial insurance, and utilize adequate methods to convey to users that they must follow traffic and parking laws. *See* Cal. Civ. Code § 2505; LAMC §§ 21.03(a), 21.09(a); City of

Los Angeles, *On-Demand Mobility Rules and Guidelines* (2021).[13] Put simply, this is not the level of government oversight that subjects an entire industry to the administrative search exception to the Fourth Amendment and the district court erred on this ground.

2. Mass Compelled Disclosure of Individualized Scooter Location Information is Not Necessary to Advance the Generalized Needs the City Identified.

Further, assuming *arguendo* that the rental of e-scooters was somehow on par with the likes of firearm and liquor sales, the City did not sustain its burden below to justify application of the administrative search exception. To warrant application of this exception to the Fourth Amendment, the government must satisfy three additional criteria: (1) there must be a "'substantial' government interest that informs the regulatory scheme pursuant to which the inspection is made;" (2) the "warrantless inspections must be 'necessary' to further [the] regulatory scheme;" and (3) the "statute's inspection program, in terms of the certainty and regularity of its application, [must] provid[e] a constitutionally adequate substitute for a warrant." *Patel*, 576 U.S. at 426 (quoting *New York v. Burger*, 482 U.S. 691, 702-703 (1987)).

---

[13] *Available at* https://ladot.lacity.org/sites/default/files/documents/on-demand-mobility-rules-and-guidelines-2021.pdf.

Here, the MDS program's compelled disclosure of precise, individualized location data is unnecessary because, as shown below, the City's stated goals in creating MDS would be adequately served by data aggregation, differential privacy, and/or sampling. Because less invasive means of data collection would meet the goals of the City's regulatory scheme, it cannot—at this stage of the litigation—meet their burden to demonstrate that the administrative search exception applies.

The needs identified by the City below in the MDS system are exceptionally *general* in nature. In the City's motion to dismiss, it identified a stated interest in "actively" managing "private mobility providers and the public rights of way" and "promot[ing] a transportation system free from discrimination." (Case No. 2:20-cv-0544-DMG-AFM, Docket No. 18 at 9-10.). The City did not—and could not—identify a policy goal for MDS that would require the granular and individualized location data it is currently acquiring from e-scooter users.[14] Addressing the broad,

[14] To be fair, the City did not spend any time briefing the administrative search exception before the district court other than a singular line in its reply brief, which stated that "despite the narrowness of the 'closely regulated industry' exception, this new micro-mobility platform, a cousin and precursor to autonomous vehicles, surely falls within the ambit of the exception." (Case No. 2:20-cv-0544-DMG-AFM, Docket No. 25 at 18.). The City cited no legal support for this proposition below.

generalized concerns put forth by the City at this stage of the litigation, they quite simply do not need individualized trip data to manage crowded streets or cluttered sidewalks or to ensure that mobility providers are serving disparate socioeconomic areas of the City of Los Angeles in a non-discriminatory fashion. Aggregated location data and sample sets would meet the stated goals of improving safety, efficiency, and equity of distribution in e-scooters in a far narrower fashion and in a manner that does not infringe on individuals' right to privacy in their real-time and historical location data.

3. The City's Data Needs Could be Met With Use of Privacy-Preserving Techniques Such as Aggregation, Sampling, and/or Differential Privacy.

Even were we to assume some specific policy goals that the City did not put before the district court, aggregate data, sample sets, and/or differential privacy are more than sufficient to address them. For example, the City may be interested in finding out how many e-scooters travel along a particular street between certain hours, what the high-frequency travel streets are for e-scooters, the average speeds at which e-scooters travel on a street, where inactive e-scooters are potentially clogging sidewalks, and if mobility companies are making e-scooters available to all communities on an equitable basis. However, these policy concerns do not require individual riders' mobility data, such as precise and individualized route information, to meet these imagined policy goals.

The City should not be able to collect a treasure trove of real-time and historical individualized location data without providing an individualized reason for why they need to collect such data. The administrative search exception to the Fourth Amendment is *only* available where "[l]arge interests are at stake, and inspection is a crucial part of the regulatory scheme[.]" *Biswell*, 406 U.S. at 315 (discussing federal regulation of the interstate traffic in firearms). Here, particularized location data inspection is not a crucial part of the regulatory scheme because the City's policy goals are easily met by generalized inspections that rely on aggregating data, sampling data, and differential privacy.

Aggregating data significantly decreases the chance that any one individual e-scooter user could be identified, without negatively impacting the usefulness of the data to the City. Aggregation could easily be accomplished by inserting a third-party intermediary between the information feed captured through MDS and cities such that the third-party intermediary keeps individual route data in an isolated (and highly secure) environment and then feeds the cities aggregated data relevant to that city's particular transportation and equity interests. Such intermediaries' collection, use, and disclosure of shared information would need to be closely regulated.

There are at least two companies that already act as intermediaries for MDS data—Remix and Populus. Remix "takes information about individual trips and

combines them together into data that allows cities to answer important questions without revealing any single person's activity." Jascha Franklin-Hodge, *Aggregating Mobility Data to Protect Privacy*, Remix (May 28, 2019).[15] Similarly, Populus "processes route data for individual trips into insights about the most common routes that people take on scooters without revealing the exact traces of individual trips." *A Practical Guide to Mobility Data Sharing and Cities*, Populus, at 14 (May 2020).[16] As Populus notes, holding "individual-level, sensitive information can be more difficult or expensive for cities that may not have the data management protocols to protect this data and to limit access to it." *Id.*

Unlike the City, most other MDS users are interested in this level of protection for individualized location data, with Populus noting that 80% of those cities that utilize the MDS system use a third-party data platform, such as Populus, to manage their data. *Id.* Were the City utilizing either Remix or Populus, it would still be able to answer the questions of whether mobility providers were equitably distributing e-scooters in low-income neighborhoods and where the

---

[15] *Available at* https://www.remix.com/blog/aggregating-mobility-data-to-protect-privacy.

[16] *Available at* https://www.populus.ai/white-papers/mobility-data.

majority of e-scooter trips were taking place on city streets without individually surveilling its citizenry on a daily basis and cataloguing their movements in violation of the Fourth Amendment. *See* Dr. Regina Clewlow, *A Practical Guide To Mobility Data Sharing,* Forbes (Aug. 28, 2019, 10:37 AM).[17]

Likewise, the City could use sampling to accomplish their goals. For example, if the goal is to determine whether e-scooters are adequately serving a particular part of the City of Los Angeles, the City could request data about e-scooter use in that part of the City for a specific period of time only. If the City receives a complaint that e-scooters are clogging a particular city street during the afternoon rush hour, it can request data about scooter use during that time and on that particular thoroughfare. Instead of this more targeted approach, the City demands a broad, on-going disclosure of individualized e-scooter location information that is far more intrusive than is necessary to meet its policy goals.

In a similar vein, the City could utilize differential privacy to meet its stated policy goals without subjecting e-scooter users to the risk that their anonymized location data would be re-identified. Differential privacy is a "rigorous mathematical definition of privacy" that seeks to ensure that the outcome of any

---

[17] *Available at* https://www.forbes.com/sites/reginaclewlow/2019/08/28/a-practical-guide-to-mobility-data-sharing/?sh=3737340199c9.

statistical analysis is not linked to any of the individual data included in the original dataset. *Differential Privacy*, Harvard University Privacy Tools Project (July 22, 2021).[18] Differential privacy promises data subjects that they "will not be affected, adversely or otherwise, by allowing [their] data to be used in any study or analysis, no matter what other studies, data sets, or information sources are available." Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy* 5 (2014).[19] Differential privacy accomplishes this goal by introducing into the data set "a controlled quantity of noise" that preserves statistical calculations while also "provid[ing] robust and measurable guarantees of confidentiality." Jae June Lee & Cara Brumfield, *Differential Privacy in the 2020 Census* 1-2 (Nov. 2019).[20]

Differential privacy is used because even aggregated data can unintentionally reveal information about individuals in a given data set. For example, a research article coauthored by researchers from Tsinghua University in China, Stanford University in California, and the University of Göttingen in

---

[18] *Available at* https://privacytools.seas.harvard.edu/differential-privacy.

[19] *Available at* https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf.

[20] *Available at* https://www.georgetownpoverty.org/wp-content/uploads/2019/11/GCPI-ESOI-Differential-Privacy-in-the-2020-Census-20191107.pdf.

Germany demonstrated that aggregated mobility data could be re-identified and linked to particular individuals. Fengli Xu et al., *Trajectory Recovery From Ash: User Privacy is NOT Preserved in Aggregated Mobility Data*, IW3C2 (April 3-7, 2017).[21] The researchers found this was so because "aggregating mobility records does not preserve users' privacy, since a user's mobility pattern is regular while different from others." *Id.* at 1243. Another study offered differential privacy as a solution after determining that, given the unique nature of mobility records, the researchers could recover individual mobility trajectories with 73 to 91 percent accuracy. Zhili Chen et al., *Differentially Private Aggregated Mobility Data Publication Using Moving Characteristics*, Cornell's arXiv Service (Aug. 10, 2019).[22]

There are many examples of differential privacy applied to aggregated mobility data that both successfully prevent the disclosure of individualized location information and generate useful data. For example, researchers who wanted to create a mapping program for commuting patterns within the United States used synthetic data generation and differential privacy techniques to

---

[21] *Available at* http://papers.www2017.com.au.s3-website-ap-southeast-2.amazonaws.com/proceedings/p1241.pdf.

[22] *Available at* https://arxiv.org/pdf/1908.03715.pdf.

preserve the commuters' privacy while achieving an accurate result. *See* Ashwin Machanavajjhala et al, *Privacy: Theory Meets Practice on the Map,* Dep'ts of Computer Science and Labor Economics, Cornell Univ. (July 22, 2021).[23] As another example, in working with several European institutions to "minimize traffic congestion, speed up journeys, improve safety, and reduce the amount of money spent on infrastructure," Google shared aggregated historical traffic data with differential privacy applied, to "intentionally [add] 'noise' to the data in a way that maintains both users' privacy and the data's accuracy." *Tracking Urban Mobility with Technology*, Google Europe Blog (Nov. 18, 2015).[24]

Following the recommendations of research scientists, Caroline O. Buckee et al., *Aggregated Mobility Data Could Help Fight COVID-19*, Science (Mar. 23, 2020),[25] companies have also been using differential privacy before releasing COVID mobility data. *See* Google, *COVID-19 Community Mobility Reports* (2021);[26] *see also* Paige Maas et al., *Facebook Disaster Maps: Aggregate Insights*

---

[23] *Available at* http://www.cse.psu.edu/~duk17/papers/PrivacyOnTheMap.pdf.

[24] *Available at* https://europe.googleblog.com/2015/11/tackling-urban-mobility-with-technology.html.

[25] *Available at* https://science.sciencemag.org/content/sci/early/2020/03/20/science.abb8021.full.pdf.

[26] *Available at* https://www.google.com/covid19/mobility/.

for Crisis Response & Recovery, Facebook (May 2019) (aggregated mobility data for natural disaster relief released with "add[ed] random noise and dropp[ed] small counts," i.e., differential privacy).[27] Thus, the City has numerous options available to it that help it meet the generalized regulatory goals of right of way management and equitable distribution of transportation, but which respects individuals' "reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 138 S. Ct. at 2217. The City has not met its burden to prove that the administrative search exception to the Fourth Amendment applies (to the extent that it should be analyzed *at all* in this context) and thus reversal is warranted.

[27] *Available at* https://research.fb.com/wp-content/uploads/2019/04/iscram19_camera_ready.pdf.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to reverse the district court's grant of the City's motion to dismiss below and remand the case for further proceedings not inconsistent with this opinion.

Date: July 30, 2021

WAYMAKER LLP

/s/ Brian E. Klein
Brian E. Klein
Melissa A. Meister

Attorneys for Amici Curiae
Center for Democracy and Technology and
Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 6530 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: */s/ Melissa A. Meister* **Date:** July 30, 2021