Case No. 21-55285

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN SANCHEZ

Plaintiff-Appellant

v.

LOS ANGELES DEPARTMENT OF TRANSPORTATION; CITY OF LOS ANGELES

Defendants-Appellees

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

BRIEF OF *AMICI CURIAE* SEVEN DATA PRIVACY AND URBAN PLANNING EXPERTS IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

Kendra K. Albert
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-998-1558
kalbert@law.harvard.edu

Mason A. Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845
mkortz@law.harvard.edu

Counsel for *Amici Curiae*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* John Clary, Greg P. Griffin, Joseph Lorenzo Hall, Jennifer King, Grant McKenzie, Arvind Narayanan, and Rebecca Williams each state that they are individuals and thus they do not have parent corporations, nor does any publicly held corporation own ten percent or more of their stock.

Dated: July 30, 2021

/s/ Kendra K. Albert

Kendra K. Albert

STATEMENT OF COMPLIANCE WITH RULE 29

Pursuant to Federal Rule of Appellate Procedure 29(a)(2), *amici curiae* certify that all parties have consented to the filing of this brief.

Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *amici curiae* certify that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief; and no person — other than the *amici curiae* or their counsel — contributed money that was intended to fund the preparation or submission of this brief.

Dated: July 30, 2021

/s/ Kendra K. Albert
Kendra K. Albert

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

RULES

STATEMENT OF INTEREST OF *AMICI CURIAE*

Amici curiae consist of seven individual technologists, urban planning experts, and geoprivacy researchers. Collectively, *amici* have deep experience with the Mobility Data Specification (MDS), location data privacy and de-anonymization, micromobility services like dockless scooters, and city transportation regulation. As such, *amici* have a significant interest in the factual claims dismissed by the district court on its Rule 12(b)(6) motion. Brief statements of the expertise of the *amici* follow.[1]

John Clary manages digital services for the City of Austin Transportation Department. He has worked with Mobility Data Specification data since its inception, and co-chaired the Open Mobility Foundation's Privacy, Security, and Transparency Committee from July 2019 to November 2020.

Dr. Greg P. Griffin is an assistant professor of urban and regional planning at The University of Texas at San Antonio. He holds a PhD from the University of Texas at Austin in Community and Regional Planning

[1] *Amici*'s institutional affiliations are provided only for purposes of identification.

and is a APA Certified Planner. Dr. Griffin's current research involves GPS accuracy for fitness tracking apps, and planning for a micromobility testbed with support from the National Science Foundation.

Dr. Joseph Lorenzo Hall is a senior vice president at the Internet Society, a non-profit organization dedicated to an open, secure, and trustworthy Internet. He was previously the chief technologist and director of the Internet architecture project at the Center for Democracy & Technology. Dr. Hall has served as a member of the Los Angeles County Registrar-Recorder/County Clerk's Open Technology Advisory Group.

Dr. Jennifer King is the Privacy and Data Policy fellow at the Stanford Institute for Human-Centered Artificial Intelligence at Stanford University. She is a scholar of information privacy, and her work focuses on consumer understandings and expectations of privacy online. Dr. King was a co-author of a report examining the use of municipally-owned surveillance cameras by the City of San Francisco.

Dr. Grant McKenzie is an assistant professor of spatial data science in the Department of Geography at McGill University. At McGill, he leads a lab at the intersection of information science and behavioral geography. Much of Dr. McKenzie's work examines applied aspects of geoprivacy and micro-mobility services as well as the broader role that geographic information science plays at the intersection of information technologies and society.

Dr. Arvind Narayanan is an associate professor of computer science at Princeton University. His doctoral research showed how algorithms can be used to re-identify seemingly anonymized data, for which he won the 2008 Privacy Enhancing Technologies Award and the 2019 Institute of Electrical and Electronics Engineers Security and Privacy "Test of Time" Award.

Rebecca Williams is an information policy researcher and expert in government data management. She served as a Fellow at Harvard Kennedy School's Technology and Public Purpose project where she studied the harmful effects of "smart city" surveillance systems on civil liberties. She previously served as a Digital Services Expert at the White House.

SUMMARY OF ARGUMENT

Dockless scooters have transformed urban transportation, raising novel challenges for city governments. The Los Angeles Department of Transportation ("LADOT") seeks to address these challenges by collecting granular data about scooter trips. LADOT requires scooter providers to submit the start and end location (in real time) and the route (within 24 hours) of every scooter trip in the city through the Mobility Data Specification system. Plaintiff Justin Sanchez sued, arguing that this requirement endangers individual privacy.[2]

The district court dismissed Sanchez's claims, holding that Sanchez has no reasonable expectation of privacy in MDS data—and that MDS is not a search—because multiple trips cannot be linked to individual riders. This holding rests on an incorrect understanding of the facts. In truth, a trip can be reidentified by pairing the observed time, location, and direction of a rider with MDS data. Even lacking that information, LADOT could easily reidentify a pattern of trips by a particular rider

[2] The other original plaintiff, Eric Alejo, voluntarily withdrew his appeal while the matter was pending. ECF 18-19. As such, the brief solely refers to Plaintiff Sanchez.

using freely available datasets, without relying on any special knowledge or equipment.

The lower court also held that, even if riders have a reasonable expectation of privacy in MDS data, their privacy interests are minimal and the city's need for such granular data is substantial. However, LADOT's need for granular data is disputed. Discoverable facts would likely show that Sanchez's privacy interests are substantial and that the data required is ill-suited for LADOT's stated regulatory goals. As such, the district court should have allowed discovery before deciding whether LADOT's requirements constituted a reasonable search. At the very least, the lower court should have granted Sanchez leave to allege additional facts.

Amici urge this Court to reverse the dismissal of Plaintiff's claims and remand with instructions to proceed to discovery or, in the alternative, to grant Sanchez leave to file an amended complaint.

ARGUMENT

I. Sanchez's claim that MDS data is easily linkable to individual riders is more than merely plausible—it is true and correct.

The court below improperly dismissed Sanchez's suit under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. To survive a Rule 12(b)(6) motion to dismiss, a plaintiff is only required to allege facts sufficient to "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007). The court must accept all of the plaintiff's factual allegations as true. *Id.* at 555. If these "[f]actual allegations [are] enough to raise a right of relief above the speculative level," the court must deny the motion to dismiss. *Id.*

In many cases, discussion of the 12(b)(6) standard would be boilerplate. But here, Sanchez made factual allegations that MDS data can be linked to individuals. The lower court failed to accept these allegations as true. Instead, the lower court found that MDS data is "anonymous." 1-ER-005-15 (hereinafter "Opinion") at ER-008. The court acknowledged Sanchez's allegation that "location data can be readily de-anonymized," but went on to say that MDS data can be linked "only to the scooter . . . ." *Id.* However, Sanchez clearly alleged that MDS trip data is also easily linked to individual riders with minimal time and technical expertise. 3-ER-308-26 (hereinafter “Complaint”) ¶ 26. Sanchez further alleged that scooter rides are not fully disassociated from one another. *Id.* ¶ 26. Had the lower court properly accepted these allegations as true, they would raise Sanchez’s right to relief well above the speculative level.

Moreover, Sanchez’s allegations that MDS data for multiple trips can be linked to individual riders are not merely well-pleaded, they are also factually accurate. While it is true that MDS does not record direct identifiers, like names or user IDs, MDS data can nevertheless be connected to individuals. Trip start and end locations, route, time, and scooter brand data can be used to identify an individual either through physical observation or by combining it with additional datasets. Such reidentification can be done with minimal time and effort, and doesn’t require specialized technical expertise or equipment. The lower court’s findings regarding MDS data therefore are not just inappropriate at the motion to dismiss stage, they are incorrect as to the nature of MDS data and the realities of de-anonymization.

A. MDS data can be easily linked to individuals through simple physical observation.

Sanchez alleged that "even simple physical observation of a rider[] can likely identify the individual who took the trip." Complaint ¶ 26. *Amici* confirm that physical observation would be the easiest, cheapest, and most efficient way to reidentify a particular scooter rider from MDS data. An observer intent on reidentifying a scooter rider would simply need to note the time, location, and general direction a scooter was travelling.

Importantly, these observations do not need to be intentional. In the digital age, technology constantly captures unintended data that can later be mined for novel uses. In New York City, journalists scoured a database of "anonymous" taxicab trips released by the city, pairing the data with time-stamped paparazzi photos of celebrities exiting or entering cabs. The paparazzi photos were sufficient to identify which trips in the database various celebrities, including Bradley Cooper and Kourtney Kardashian, had taken. J.K. Trotter, *Public NYC Taxicab Database Lets You See How Celebrities Tip*, Gawker (Oct. 23, 2014).[3]

[3] https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546 [https://perma.cc/Y5L2-RWSY].

Time-stamped and geotagged images or video (for example, from a mobile phone, security camera, or smart home device) could supply similar information regarding individuals on scooters.

The existence of such images is common, even for non-celebrities. With one camera per 4.6 people, individuals in America are filmed by security cameras over 200 times a week. *How Many Times are Americans on Camera Every Week?*, Safety.com (Feb. 17, 2021).[4] Add to that all the personal photos and smart doorbell footage that makes its way to social media, and there is a high chance that some portion of a scooter ride will be captured. Moreover, the information captured is likely to be unique; even in highly trafficked areas, multiple riders are rarely at the same location, going the same direction, on the same brand of scooter, at the exact same moment. A single image or frame could be sufficient to reconstruct an individual's trip from MDS data.

It is true that pinning a single trip to an observation does not automatically reveal the identity of the scooter rider, since MDS data does not include personal identifiers. Unlike celebrities in New York,

[4] https://www.safety.com/digital/identity/average-american-filmed-by-an-estimated-238-security-cameras-a-week/ [https://perma.cc/G3AJ-WP98].

most people are not immediately recognizable from observing them on a scooter. But even riders who aren't famous can be reidentified from a single trip. As privacy researcher Yves-Alexandre de Montjoye, whose research was cited by the district court, explains, the ease of reidentification is due to a combination of "human behavior and the way we all move around." PAPIs.io, *ITV with Yves-Alexandre de Montjoye—Researcher at Imperial College London & MIT Media Lab,* YouTube (Aug. 17, 2017).[5] While there may be many people in the same place as you at this moment, only a small fraction of them will be in the same place as you five hours from now. An even smaller fraction of those will also be in the same place as you tomorrow morning. *Id.* Human mobility patterns are so distinctive that just two time-stamped locations (such as the start and end of a scooter trip) are sufficient to uniquely characterize more than 50 percent of individuals. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Sci. Rep. 1376, 2 (2013). Once four time-stamped location data points have been pinned to an individual, that person will be uniquely identifiable 95

[5] https://www.youtube.com/watch?v=DinBSlOF7yM [https://perma.cc/QUD5-SYPH].

percent of the time. *Id.* Thus, if an observer is able to match two trips from MDS data to the same individual, there is a 95 percent chance that those four time-stamped location data are sufficient to uniquely identify the scooter rider. Given how simple it is to link a uniquely identified rider to their personal information elsewhere on the web, even the Open Mobility Foundation, which oversees MDS, encourages cities to "treat MDS data as sensitive personal data . . . ." Open Mobility Foundation, *Privacy Guide for Cities: Mobility Data Specification* (Sept. 15, 2020).[6]

Reidentification of scooter trip data through physical observation is more than merely a hypothetical. Authorities in Austin, Texas used surveillance camera footage to identify the brand of scooter ridden by a bank robber making his escape. Once they had used the footage to identify the scooter provider, authorities were able to subpoena that particular scooter provider for the user's account information, capturing the suspect. Matthew Prendergast, *APD Identifies Bank Robbery Suspect Who Used E-Scooter for Getaway*, KXAN (Jan. 25, 2019).[7] Because

[6] https://github.com/openmobilityfoundation/governance/blob/main/documents/OMF-MDS-Privacy-Guide-for-Cities.pdf [https://perma.cc/G2EB-73UG].

[7] https://www.kxan.com/news/local/austin/apd-identifies-bank-robbery-suspect-who-used-e-scooter-for-getaway/ [https://perma.cc/PTE8-9M8H].

security camera footage had captured the suspect on a scooter, MDS data enabled law enforcement to determine which scooter was at the bank at the time of the robbery. From there, it was simple to subpoena the account information of the individual who had rented that particular scooter.

Domestic abuse and stalking present more troubling use cases. MDS data could enable abusers or stalkers to keep near-constant tabs on their victims' location with only occasional physical observation. Once an abuser or stalker knew a victim's typical movement patterns, MDS data would allow them to determine that person's location in near-real-time from a set of "anonymous" rides. Sanchez alleged instances where government-collected location data contributed to such stalking, pointing to a report of hundreds of instances of misuse of police databases by law enforcement officers. Complaint ¶ 29; *see Automated License Plate Recognition*, California State Auditor (Feb. 20, 2020) at 12-13.[8] In a chilling example from Illinois, a stalker subpoenaed the toll-road transponder records of his ex-spouse to circumvent a restraining order,

[8] https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [https://perma.cc/FSD6-CCSA].

using them to track her and her family's movements. Tony Arnold, *How Your Private Illinois Tollway Data is Shared with Cops and Divorce Lawyers,* WBEZ Chicago (Sept. 19, 2019).[9] When local governments collect fine-grained location data without adequate safeguards, they are setting up an environment ripe for misuse and substantial harm.

B. MDS data can be easily linked to individuals through comparison of multiple datasets.

Reidentifying scooter data can also be done without physical observation by combining widely available datasets with MDS data. As Sanchez alleged, "coupling a rider's precise trip data with information from just one other dataset[,] for instance, . . . public voting records from particular addresses[,] can likely identify the individual who took the trip." Complaint ¶ 26. Sanchez cited research demonstrating that someone with access to MDS data (legitimate or otherwise) "could potentially match users' trajectories in anonymized data from one dataset, with deanonymized data in another, to unmask the anonymized data." Complaint ¶ 28.

[9] https://www.wbez.org/stories/how-your-private-illinois-tollway-data-is-shared-with-cops-and-divorce-lawyers/cea68ea0-4b13-481a-80a1-50bf0e9db738 [https://perma.cc/N34L-MFYW].

One way to de-anonymize location data is to overlay multiple datasets in geographic information system (GIS) software and look for patterns. A GIS user could easily layer MDS trip data atop free, detailed datasets such as U.S. census block data, voting records, road networks, or building footprints. Morgan Herlocker, a mobility data privacy expert, demonstrated the severity of GIS-based de-anonymization when he combined MDS data with other public datasets to identify sensitive scooter trips, including a midday trip from a high school in a conservative area to a city block which included a Planned Parenthood clinic. Harry Campbell, *RSG113: Morgan Herlocker on Mobility Data and Privacy Concerns,* Ride Share Guy (Dec. 17, 2019).[10] This technique does not require deep expertise (modern GIS software enables visualization and pattern-matching on complex datasets with just a few lines of code) or special technology (GIS software is freely available online and can run on a personal laptop). As a result, de-anonymization can be accomplished by almost anyone with access to MDS data.

[10] https://therideshareguy.com/rsg113-morgan-herlocker-on-mobility-data-and-privacy-concerns/ [https://perma.cc/9X92-F2G6].

C. Multiple scooter rides can easily be associated with each other using MDS data.

The district court held that the city would only violate a reasonable expectation of privacy if it "identif[ied] and compile[d] *all* the trips that [Sanchez] took on scooters" from MDS data. Opinion at ER-009. In holding that this was not possible, the court made two factual findings: (1) that "[e]ach ride is disassociated from other rides the user may have purchased," and (2) that "de-anonymizing one location data point would . . . reveal only a sole trip . . . ." *Id.* Again, these findings mischaracterize the process of de-anonymization.

While human mobility patterns are unique, they are also highly regular—that is, predictable and repetitive, since "individuals tend to do the same things over and over . . . ." Adrian Colyer, *Trajectory Recovery from Ash: User Privacy is NOT Preserved in Aggregated Mobility Data*, The Morning Paper (May 15, 2017).[11] People tend to stay close to their homes, workplaces, and other important locations. Some human mobility models are premised on the assumption that movement between

[11] https://blog.acolyer.org/2017/05/15/trajectory-recovery-from-ash-user-privacy-is-not-preserved-in-aggregated-mobility-data/ [https://perma.cc/6C8S-CBWA].

neighborhoods is exponentially less common than movement within neighborhoods. Laura Alessandretti et al., *The Scales of Human Mobility,* 587 Nature 402, 406 (2020). Other models demonstrate how destinations with a specialized function, such as medical clinics, are visited at a lower frequency and attract visitors from a much wider radius than more generic locations. Markus Schläpfer et al., *The Universal Visitation Law of Human Mobility*, 593 Nature 522, 526 (2021). This means scooter trips to sensitive locations are especially identifiable, since repeated trips could be more easily identified and linked together. Researchers have used machine learning to combine bikeshare data with Google Maps, inferring how students use public bikes in their daily lives and revealing their recreation and commuting habits. Jie Bao et al., *Exploring Bikesharing Travel Patterns and Trip Purposes Using Smart Card Data and Online Point of Interests*, 17 Network & Spatial Econ. 1231, 1233 (2017).

Sanchez plausibly alleged that MDS data could be de-anonymized to reveal "a pattern of repeated trips." Complaint ¶ 26. The lower court should have accepted this well-pleaded allegation as true—which it is, since multiple trips *can* be linked to each other.[12] Therefore, dismissal of Sanchez's claims based on factual disputes about the reidentifiability of MDS data was inappropriate.

II. The lower court should have allowed discovery instead of holding that LADOT's use of MDS is a reasonable search.

The lower court held that, even if MDS implicated a reasonable expectation of privacy, it is a reasonable search. Opinion at ER-011. It applied the test for administrative searches, which balances the "nature" and "character" of the privacy intrusion against the "nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 829, 832, 834 (2002). All of these factors depend on "the particular circumstances" of the case, making it deeply fact-specific. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 529 (7th Cir. 2018).

[12] The district court found in a footnote that "even if it were possible to create such a comprehensive record of an individual's movements from the MDS data, it would likely be an enormously resource- and/or time-intensive project" and suggested that Sanchez agreed. Opinion at ER-009 n.6. But Sanchez clearly (and correctly) alleged that "a *simple* analysis of MDS data will likely identify the precise trips taken by Plaintiff[] . . . ." Complaint ¶ 32 (emphasis added).

In the context of data, the nature of the intrusion and strength of the government's concerns depend heavily on how the data is collected and used. Some cities deploy MDS with additional data protections, such as collecting less granular data to preserve the privacy of individual riders or limiting sharing with law enforcement. These protections can be outcome-determinative. In *Naperville Smart Meter Awareness v. City of Naperville,* which the lower court cited as precedent, the court assessed whether the city's collection of data from digital electricity meters was a reasonable administrative search. The court's balancing hinged on two specific data protection practices: low-granularity collection and restrictions on law enforcement access. 900 F.3d at 528-29. The court relied on the city's "Smart Grid Consumer Bill of Rights," which "clarifie[d] that the city's public utility will not provide customer data to third parties, including law enforcement, without a warrant or court order." *Id.* at 528. The court ultimately held that the searches were reasonable but warned that, "[w]ere a city to collect the data at shorter intervals, our conclusion could change. Likewise, our conclusion might change if the data was more accessible to law enforcement or other city officials outside the utility." *Id.* at 529.

In the present case, the lower court correctly declined to take judicial notice of the contents of the city's Data Protection Principles, since the city's actual adherence to them was disputed. As such, many facts about the city's MDS data protection practices are unsettled. Without sufficient factual information to meaningfully conduct the balancing test, the lower court should have refrained from ruling on the reasonableness of the search until the parties had taken discovery. However, it chose to proceed with the balancing test under the motion to dismiss standard. Under this standard, the court should have accepted all of Sanchez's factual assertions as true *and* drawn all reasonable inferences in Sanchez's favor. Instead, it relied on an incorrect understanding of MDS data and unsupported "common sense" findings to draw inferences against Sanchez on both prongs of the administrative search test.

A. The nature and character of the privacy intrusion are more serious than mere places Sanchez travels.

In assessing the first prong of the balancing test, the lower court found that the nature and character of privacy intrusions from MDS data would be minimal. The court stated that "at the absolute most," the privacy intrusion would be "knowledge of the places that Plaintiff[has] traveled to on rental scooters . . . ." Opinion at ER-011. This assertion directly and improperly contradicts well-pleaded factual allegations by Sanchez.[13] Moreover, it is factually inaccurate, as there are substantial privacy interests in MDS data.

i. MDS may incorporate data from riders' mobile phones, increasing the invasiveness of the search.

In dismissing Sanchez's claims, the lower court assumed that GPS data is "all the information that MDS collects." Opinion at ER-012. This may not be true. To circumvent problems with GPS inaccuracy, scooter providers regularly combine location data collected from the vehicles themselves with location data collected from users' mobile phones, using both GPS data and cell site location information, in a process called "multi-source verification":

[13] Sanchez alleged that MDS data "may reveal important information about the individual's residence, the identity of her employer, associates, or friends, the type of physicians she visits, or her favorite recreational activities." Complaint ¶ 26. Additionally, "when end points are sensitive locations—like therapists' offices, marijuana dispensaries, or Planned Parenthood clinics—those routes may reveal *why* she made that trip." *Id.* Sanchez also alleged that "identification of location data poses grave risks to individuals," evidenced by recent cases of domestic abuse facilitated by automatic license plate reader information in California. *Id.* ¶ 29.

> Diverging from the data collection of [car] ride share companies, scooters are able to collect the perfect cocktail of user data, gathering multi-source verified information through both scooters and apps [installed on user's mobile phones] . . . . Beginning when users open the app to search for a scooter, these apps can track where individuals ride, possibly revealing users' living arrangements, employment, social connections, and consumer behavior. On the off chance users disable location tracking on their phone after unlocking a scooter, each scooter has location tracking capabilities built in through GPS chips and 4G data connections. When pairing scooter location data with that from a [user's] phone, each data set can be corroborated, providing an exceptionally accurate portrait of a [user's] location and trip routes. Over time, these trip routes can paint a clear picture of a [user's] lifestyle and preferences. This multi-source verification also makes scooter surveillance more concerning than [car] ride sharing services and poses significant risks to users.

Andrew Boyles Peterson, *Scoot over Smart Devices: The Invisible Costs of Rental Scooters*, 17 Surveillance & Soc'y. 191, 194 (2019).

Because of the lack of discovery, it is unknown whether any scooter providers in Los Angeles use multi-source verification. If they do, though, MDS hews much closer to the cell site location information at issue in *Carpenter v. United States*. 138 S. Ct. 2206, 2217 (2018). Moreover, while the lower court found that location tracking was an "obvious, core design feature" of scooter rental services, Opinion at ER-010, multisource verification is not. Most riders likely do not realize that companies combine cell phone location data with scooter GPS data to pinpoint their locations. *See Carpenter*, 138 S. Ct. at 2220 (holding that automatic cell phone data sharing does not constitute "voluntary exposure" of location information).

Both the relevance of *Carpenter* and the reasonableness of MDS as an administrative search could turn on whether the data demanded by LADOT incorporates location information from users' mobile phones. The lawsuit was incorrectly dismissed before Sanchez could determine whether scooter providers in Los Angeles use multi-source verification.

ii. Reidentified location data carries significant legal and reputational consequences for individuals.

The lower court also took too narrow a view of the significance of location data. To establish the reasonableness of a privacy expectation, courts "consider not only the raw data, but what that data can reveal" when combined with "other available information[] and some deductive reasoning." *Leaders of a Beautiful Struggle v. Baltimore Police Dep't.*, No. 20-1495, 2021 WL 2584408, at *10 (4th Cir. June 24, 2021). Location data, when combined with additional datasets, can paint a detailed picture of an individual's life, leading to significant legal and reputational consequences. Scooter data in particular has been leveraged by both law enforcement and private attorneys in legal proceedings. For example, scooter providers in Indianapolis and St. Louis indicated they were "fully cooperating with local authorities" to investigate robberies where scooters were used as getaway vehicles. Evan Koslof, *Dockless Scooters as Getaway Vehicles? Welcome to 2019*, WUSA 9 (May 23, 2019);[14] Crystal Muguerza, *Indiana Burglar Robs Man in His Home, Uses Bird Scooter to Get Away*, ABC News (Sept. 22, 2018).[15] In Chicago, personal injury lawyers subpoenaed the city's scooter location database in order to solve a hit-and-run accident. Dara Kerr, *Scooter Hit-and-Run Triggers Battle Over Rider Location Data*, CNET (July 8, 2019).[16]

Of course, privacy interests in location data go beyond legal proceedings. Purportedly anonymous taxi data, paired with paparazzi photos, has revealed the tipping habits of celebrities, leading some to defend their reputations against tabloid reporters. Trotter, *supra.* Researchers used "anonymized" data from Strava, a fitness app, to de-

[14] https://www.wusa9.com/article/news/crime/dockless-scooters-as-getaway-vehicles-welcome-to-2019/65-1b6bdac7-99f7-4035-a718-c92416fb087a [https://perma.cc/U79X-L499].

[15] https://abcnews.go.com/US/indiana-burglar-robs-man-home-bird-scooter/story?id=57987946 [https://perma.cc/EV7M-KNG6].

[16] https://www.cnet.com/news/scooter-hit-and-run-triggers-battle-over-rider-location-data/ [https://perma.cc/RDG6-HF7U].

anonymize the names and running routes of dozens of U.S. military members and, alarmingly, reveal the layouts of secret military installations. Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, Wired (Jan. 29, 2018);[17] Matt Burgess, *Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases*, Wired (Jan. 30, 2018).[18] And when the New York Times received huge databases of "anonymous" cell site location information, reporters were able to reidentify hundreds of mobile phone users, including a member of the Secret Service, based solely on publicly available datasets. Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019).[19]

Here, the district court disregarded the seriousness of the privacy harms because "it would be difficult to actually effectuate the intrusion . . . ." Opinion at ER-011. In doing so, the court relied on its own unsupported assessment that reidentifying all of Sanchez's trips would

[17] https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ [https://perma.cc/6E5A-NEGT].

[18] https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military [https://perma.cc/PSW8-QGGC].

[19] *See* https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/C98C-SB6K].

be "enormously resource- and/or time-intensive." Opinion at ER-009 n.6. But as explained earlier, the court's conclusion is based on a misunderstanding of how reidentification works—any geolocated point of data, such as a photo or credit card transaction, would be sufficient for someone with access to MDS data to associate a rider with a trip, triggering the privacy concerns described above. Even if reidentifying *all* of Sanchez's trips would be resource- or time-intensive, "the Fourth Amendment bans [the government] from warrantless access to engage in that labor-intensive process." *Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *11.

B. MDS data is ill-suited to serve the city's stated regulatory goals.

The lower court also erred in applying the second prong of the balancing test, asserting that the "the government's interests are legitimate and substantial." Opinion at ER-011. The court cited to *Naperville* for the proposition that "smart, effective regulation of a completely novel industry requires robust data." *Id.* (citing 900 F.3d at 528-29). However, the court in *Naperville* recognized that the reasonableness of the search depends on whether data is collected at a level that is tailored to meet the city's regulatory needs. *See* 900 F.3d at

529 ("[W]ere a city to collect the data at shorter intervals, our conclusion [that the search was reasonable] could change."). Sanchez plausibly alleged facts sufficient to show, beyond mere speculation, that the data currently collected through MDS is ill-suited to address the city's stated regulatory goals. Yet the lower court ignored these allegations, finding it "self-evident" that the MDS data as gathered would be useful for scooter regulation. Opinion at ER-011. Unfortunately, the court's intuition, in addition to being an impermissible inference drawn against the non-moving party, is factually incorrect.

The lower court acknowledged that "the City fails to articulate why its regulatory interests necessitate collecting such precise route data" but found it "self-evident that understanding where scooters tend to transit and park would help the city determine how and where to adjust the rules of the road." *Id.* The court elaborated, saying that, while "[t]here is no need to know the identity of the riders . . . knowing what streets they typically take, at what hours, and at what destinations they tend to stop would all be immensely useful for municipal authorities attempting to regulate the public right-of-way." Opinion at ER-011-12.

In reality, MDS data is more granular than necessary for many of the city's stated regulatory use cases and may not be granular enough for the others. Sanchez has thus plausibly alleged that "[e]ach of the articulated use cases LADOT has offered for its desire to collect *en masse* individual vehicle location data fails under scrutiny." Complaint ¶ 37. By drawing inferences against Sanchez and in favor of LADOT's position, the court erred as a matter of law in applying the Rule 12(b)(6) standard.

In any event, the court erred in finding that MDS data is tailored to LADOT's stated regulatory purposes. First, the detailed trip data that MDS collects is unnecessary for many of the city's regulatory needs. The court asserts that knowing where "scooters *tend* to transit and park," "what streets they *typically* take, at what *hours*, and at what destinations they *tend* to stop" is self-evidently useful data for the city's regulatory purposes. Opinion at ER-011-12 (emphasis added). These assumptions imply that scooter data is most useful when has been aggregated into geographic and temporal groups and analyzed for patterns. Conversely, raw MDS data, with the detail required by LADOT, is not needed for most of the city's regulatory goals.

The city could, therefore, request or retain only the aggregated data it needs for legitimate regulatory purposes. Techniques like data binning, *k*-anonymity, and tessellation can be used to do this aggregation, often with the added benefit of anonymizing individuals' data. Data binning involves sorting related values into bins to categorize otherwise messy data, often increasing the usefulness of models. Oracle, *Data Mining User's Guide: Binning* (May 2017).[20] Privacy-protective *k*-anonymity requires that multiple data points are combined before being viewable, making it harder to reidentify individual data points. Apu Kapadia et al., *Anonysense: Opportunistic and Privacy-Preserving Context Collection*, Dartmouth Scholarship 2 (2018).[21] Similarly, tessellation "partitions [a] geographic area into tiles large enough to preserve the users' privacy." *Id.* at 3. Once aggregation techniques have been applied to raw data, trends and tendencies can be discovered and the descriptor "typical" becomes meaningful, all while preserving individual privacy.

[20] https://docs.oracle.com/database/121/DMPRG/GUID-17270F04-C69B-4B5A-9B54-A8F1B9BF0531.htm#DMPRG377 [https://perma.cc/ZRJ9-RG2L].

[21] https://digitalcommons.dartmouth.edu/cgi/viewcontent.cgi?article=4305&context=facoa [https://perma.cc/B578-URAJ].

Aggregated scooter data is sufficient for the regulatory purposes articulated by LADOT, a point Sanchez raised in the complaint.[22] Even the Open Mobility Foundation, the non-profit currently responsible for maintaining and improving MDS, recognizes that aggregated data is sufficient for policy enforcement. To this end, MDS is testing a feature called "Geography-Driven Events" that allows agencies to "perform complete policy compliance monitoring without precise location data." Open Mobility Foundation, *Mobility Data Specification—General Information: Geography-Driven Events*, GitHub (Mar. 29, 2021).[23] "Rather than receiving the exact location of a vehicle, Agencies receive information about the vehicle's current geographic region." *Id.* Agencies can define the size and shape of each region, so the "data shared using Geography-Driven Events is matched to an Agency's particular regulatory needs." *Id.*

[22] For example, Sanchez alleged that the city's goal of "addressing equity in regional distribution of vehicles" could be achieved by "collecting a vehicle's neighborhood-level locations at regular but disparate, time intervals (*e.g.*, every two hours) . . . without collecting individuals' trip data." Complaint ¶ 37.

[23] https://github.com/openmobilityfoundation/mobility-data-specification/blob/main/general-information.md#geography-driven-events [https://perma.cc/XW9F-ULZH].

Other cities' deployments of MDS confirm that real-time, granular trip data is not necessary for scooter regulation. Most cities configure MDS in a "provider-side" setup, meaning scooter providers like Uber and Lime store their own data. Cities then query providers' data through custom interfaces. For additional privacy, these queries can be processed through an intermediary data analytics service. For example, Ride Report, which provides location data analytics to over 70 cities, provides mobility data dashboards, alerts, reports, and real-time vehicle monitoring by "process[ing], anonymiz[ing], and aggregat[ing] micromobility data in real-time, without compromising rider or operator privacy." *Ride Report*.[24] Because ride data is already being aggregated as part of the company's analysis workflow, there is no need for the city to collect and retain granular trip data.

LADOT, on the other hand, is unique among city governments in that has configured MDS as "agency-side," meaning scooter providers must supply trip data to the city in real-time. In this configuration, the city retains all data in its raw, granular form and can query that data without using a provider or third-party interface. LADOT, *Mobility Data*

[24] https://www.ridereport.com/ [https://perma.cc/6KD2-G5UH].

Specification: Information Briefing 1 (Oct. 31, 2018).[25] The agency-side configuration is rarely used, in part "[d]ue to significant privacy concerns, such as its requirement of real-time telemetry provided at the start and end of every trip . . . ." Madeline Kernan, *What Is Mobility Data Specification (MDS) and Other Common Questions*, Ride Report (June 26, 2020).[26] *Amici* see no reason to believe that Los Angeles, alone among cities, has special regulatory needs that demand the use of this more invasive configuration.

As for the few situations LADOT claims require precision, the relevant portion of the MDS data is simply not granular enough. As Sanchez alleged, "current physical limitations on the accuracy of GPS broadcasts from vehicles make their coordinates too imprecise to determine whether scooters are appropriately parked adjacent to a curb versus inappropriately parked in the middle of a sidewalk a couple of feet away, another purpose LADOT has offered for why it needs individual users' trip information." Complaint ¶ 38. This is an inherent technical

[25] https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf [https://perma.cc/R4A2-NKUZ].

[26] https://www.ridereport.com/blog/what-is-mds-questions [https://perma.cc/T4SD-Q9WF].

limitation on the accuracy of GPS within urban centers. The U.S. Space Force, which oversees the network of GPS satellites, indicates that GPS-enabled devices are usually accurate to within 16 feet under ideal conditions—already wider than most sidewalks. *GPS Accuracy*, GPS.gov.[27] In typical real-world settings, GPS readings are accurate to within a 40-foot range. Krista Merry & Pete Bettinger, *Smartphone GPS Accuracy Study in an Urban Environment*, 14 PLOS One 1 (2019). [28] But crowded downtowns with tall buildings create "urban canyons" where GPS signals may be blocked or distorted, lowering accuracy to the radius of an entire city block. Zhiyong Tan et al., *Vision: Cloud and Crowd Assistance for GPS Urban Canyons* 1 (2014).[29] On its own, GPS data collected from scooters is insufficiently detailed for the purpose of ensuring that the public right-of-way is free from incorrectly parked scooters.[30]

[27] https://www.gps.gov/systems/gps/performance/accuracy/#problems [https://perma.cc/H5EA-943M].

[28] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0219890 [https://perma.cc/JM47-GARH].

[29] https://synergylabs.org/MCS2014/tan_mcs2014.pdf [https://perma.cc/FMB4-BFV6].

[30] LADOT may attempt to circumvent this limitation by using data with multisource verification, as discussed above in Section A. But if it does

These details are significant. In *Naperville*, the court found that the granularity of data collection was material to the reasonableness of the search: if data was collected in more detail than necessary, the search was less likely to be reasonable. 900 F.3d at 529. Here, granular ride data is unnecessary for most of LADOT's proposed use cases and specific scooter location is ineffective for the remaining few. Thus, the lower court erred when it concluded that such data is "self-evident[ly]" useful for LADOT's purposes. Opinion at ER-011. The lower court should instead have made the reasonable inference that the invasiveness of the search outweighed the usefulness of the data and denied the motion to dismiss. If, after discovery, Sanchez's factual allegations proved to be incorrect, the court could revisit the reasonableness of MDS as an administrative search at that time.

III. At the very least, Sanchez should be granted leave to amend to support his allegations with these additional facts.

In addition to dismissing Sanchez's claims, the lower court also denied Sanchez the opportunity to plead additional facts, holding that

so, that shifts the analysis with regards to the granularity of the data, and thus the reasonableness of the search.

"amendment to add more facts would be futile." Opinion at ER-013. The court cited *Albrecht v. Lund,* which allows denial of leave to amend if "the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency . . . ." 845 F.2d 193, 195 (9th Cir. 1988). However, the district court itself identified allegations that could support Sanchez's claims—for example, conceding that MDS would be a search under the Fourth Amendment if "the City [were] able to not only de-anonymize one trip, but identify and compile *all* the trips that Plaintiff[] took on scooters . . . ." Opinion at ER-009. As such, denial of leave to amend was an abuse of discretion.

CONCLUSION

As alleged in the Complaint, MDS data is linkable to individuals and multiple trips are linkable to each other another, making the privacy interests in MDS data substantial. Moreover, the MDS data required by LADOT is ill-suited for the city's regulatory needs. These allegations are not merely plausible. They are true. Because the lower court ignored these allegations, drew inferences against Sanchez, and identified facts which, if pled, would sustain Sanchez's claims, dismissal of the complaint without leave to amend was incorrect.

For these reasons, *amici* respectfully request that this Court reverse the decision of the district court and remand with instructions to proceed to discovery or, in the alternative, to allow Sanchez to file an amended complaint.

Dated: July 30, 2021

Respectfully submitted,

/s/ Kendra K. Albert

Kendra K. Albert
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-998-1558
kalbert@law.harvard.edu

Mason Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845
mkortz@law.harvard.edu

Counsel for *Amici Curiae*[*]

[*] *Amici curiae* would like to thank Cyberlaw Clinic Summer Intern Abby Lemert, who served as a primary author on the brief, as well as Cyberlaw Clinic Summer Intern Navya Dasari, who cite-checked it, and Cyberlaw Clinic Spring 2021 Student Yihan Zhuang, who provided research assistance.

CERTIFICATE OF COMPLIANCE

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

This brief complies with the type volume limitations of Fed. R. App. P. 29(a)(5) and 32(a)(7)(b) and Ninth Circuit Rule 32-1(a) because it contains 6339 words as calculated by the word count feature of Microsoft Word for Mac, exclusive of the sections exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirement of Fed. R. App. P. 32(a)(5)(A) and (a)(6) because it uses 14-point proportionally spaced Century Schoolbook font.

Dated: July 30, 2021

/s/ Kendra K. Albert

Kendra K. Albert
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-998-1558
kalbert@law.harvard.edu

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing Brief of *Amici Curiae* John Clary, Greg P. Griffin, Joseph Lorenzo Hall, Jennifer King, Grant McKenzie, Arvind Narayanan, and Rebecca Williams in Support of Plaintiff-Appellant and Reversal with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on July 30, 2021. I certify that all participants in this case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECC system.

Dated: July 30, 2021

/s/ Kendra K. Albert

Kendra K. Albert
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-998-1558

kalbert@law.harvard.edu