No. 21-55285

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

JUSTIN SANCHEZ, *Plaintiff-Appellant*,

v.

LOS ANGELES DEPARTMENT OF TRANSPORTATION AND CITY OF LOS ANGELES, *Defendants-Appellees*.

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

APPELLANT'S REPLY BRIEF

Mohammad Tajsar
ACLU Foundation of Southern California
1313 West 8th Street
Los Angeles, CA 90017
Telephone: (213) 977-9500
Email: mtajsar@aclusocal.org

Jacob A. Snow
ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Email: jsnow@aclunc.org

Jennifer Lynch
Hannah Zhao
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 463-9333
Email: jlynch@eff.org
hzhao@eff.org

[Additional counsel on following page]

Douglas E. Mirell
Timothy J. Toohey
Greenberg Glusker Fields Claman & Machtinger LLP
2049 Century Park East,
Suite 2600
Los Angeles, California 90067
Telephone: (310) 553-3610
Email: DMirell@ggfirm.com
TToohey@ggfirm.com

Attorneys for Plaintiff-Appellant

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

FEDERAL CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

INTRODUCTION

This case concerns whether the City of Los Angeles and the Los Angeles Department of Transportation (together "LADOT") can lawfully develop an automated, city-wide data collection program that warrantlessly ingests the precise location data of every trip made by every rider of an increasingly popular mode of transportation. Rather than considering less intrusive alternatives or collecting a more limited set of data tailored to potentially legitimate planning needs, LADOT created a mass surveillance scheme with the vague purpose of "experimenting" with people's private geolocation information. In response to Justin Sanchez challenging the legality of this program, the district court erred in dismissing his lawsuit with prejudice, precluding any amendment to his complaint, and preventing any discovery into the contested program.

In its Opposition, LADOT invites this Court to repeat the errors of the decision below. First, it asks the Court to view contested, extra-record evidence in a light favorable to LADOT, effectively converting its motion to dismiss below into an attempt to improperly secure summary judgment. Second, it misapplies controlling Supreme Court precedent in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), effectively ignores *United States v. Jones*, 565 U.S. 400 (2012) and this Court's guidance in *United States v. Moalin*, 973 F.3d 977, 992 (9th Cir. 2020), and raises irrelevant and inapplicable doctrine to claim that LADOT's

program does not effectuate a search of riders—all without contesting the invasiveness of the indiscriminate dragnet it erected. Third, it defends the reasonableness of this data grab using an incorrect standard, and without accepting as true Mr. Sanchez's allegations calling into doubt LADOT's justification for collecting maximally precise trip data. Finally, it offers an erroneous interpretation of CalECPA that cannot be squared with either its text or its legislative purpose. This Court should reverse.

ARGUMENT

I. LADOT FAILS TO OFFER A MERITORIOUS DEFENSE OF THE DISTRICT COURT'S REFUSAL TO ACCEPT THE COMPLAINT'S ALLEGATIONS AND ITS DISMISSAL WITH PREJUDICE.

The district court erred by granting LADOT's motion to dismiss with prejudice without crediting Mr. Sanchez's plausibly pled facts and by depriving him of any opportunity to amend his complaint. LADOT's Opposition is as notable for what it does *not* say about Mr. Sanchez's allegations as what it does say. The agency never disputes Mr. Sanchez's principal allegation: that the private location data automatically collected by MDS is deeply invasive and can, with little effort, reveal sensitive and private information about micromobility riders. *See* 3 E.R. 317–19. While it offers various meritless legal arguments about why Mr. Sanchez nevertheless lacks a reasonable expectation of privacy, it does not defend the

district court's refusal to accept as true his allegations about the data's intrusiveness.

Conversely, LADOT does contest Mr. Sanchez's allegations that the maximally precise GPS coordinates are unnecessary to meet LADOT's planning purposes, but only by improperly relying upon evidence outside the four corners of the Complaint. Appellee's Brief in Opposition ("Opp'n") 56–57 (citing two extrinsic documents); *see United States v. Corinthian Colleges*, 655 F.3d 984, 998 (9th Cir. 2011) (generally, a district court "may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion"). The agency also contests Mr. Sanchez's interpretation of a statement made by its director concerning the MDS program. Opp'n 67 n.12. The important point here is that because the parties dispute LADOT's justifications for MDS's precise location collection, the district court's order rejecting allegations about the lack of any reasonable justification for MDS's location collection scheme should be reversed. *See* 3 E.R. 321–22; Brief of *Amicus Curiae* Kevin Webb at 14–23, ECF No. 25 (contesting justification for precise, individualized location collection),

Even if the Complaint were insufficient to meet Mr. Sanchez's burden on the pleadings, the district court erred by dismissing it and summarily concluding without explanation that leave to amend would be futile. Appellant's Opening Brief ("Br.") 24. LADOT does not defend this abuse of discretion.

II. MR. SANCHEZ'S COMPLAINT PLAUSIBLY PLEADS A VIOLATION OF THE FOURTH AMENDMENT AND THE CALIFORNIA CONSTITUTION.

A. LADOT'S argument that MDS's precise location collection is not a search lacks merit.

Mr. Sanchez enjoys an expectation of privacy in his precise location and path of travel when riding a shared micromobility device, even in public spaces. *Carpenter*, 138 S. Ct. at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere."); Br. 25–34. LADOT contests the application of *Carpenter* by raising four flawed arguments.

1. *The collection of Mr. Sanchez's location information violates his expectation of privacy.*

LADOT disputes that Mr. Sanchez has a reasonable expectation of privacy in his precise location information by arguing that: (1) people lack such an expectation when in public; (2) the facts here are different from those in *Carpenter*; and (3) a series of pre-*Carpenter* lower court decisions should control this case. But *Carpenter* foreclosed LADOT's arguments about surveillance in public, its facts are not meaningfully distinguishable, and the earlier cases LADOT relies upon address more limited data collection far afield from the technologically-assisted dragnet the agency imposes on Mr. Sanchez here.

First, LADOT's proposition that riders lack an expectation of privacy in their locations on public roads directly conflicts with *Jones*—a case conspicuously

ignored by LADOT, and one that the Supreme Court affirmed in *Carpenter*. The relevant question is not whether the location data ingested by MDS corresponds to public spaces, but whether the collected information "partakes of many of the qualities of the GPS monitoring [the Supreme Court] considered in *Jones*," and is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216. The *Carpenter* majority drew upon the five concurring justices in *Jones* to conclude that warrantless location tracking in public invades reasonable expectations of privacy when the quantity and granularity of the data collected can reveal intimate details of a person's life. *Id.* at 2215. That rule applies here.[1]

[1] LADOT, referencing a nine-year old secondary source that predates *Carpenter*, *Riley*, and *Moalin*, raises a straw man argument that Mr. Sanchez is asking this Court to categorically adopt a legal doctrine called the "mosaic theory." Opp'n 26 (citing Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311, 313 (2012)). However, Mr. Sanchez only asks the Court to follow settled case law to hold that he has adequately alleged a reasonable expectation of privacy in his location data. *Carpenter* provides that support. 138 S. Ct. at 2217. *See also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J. of Law & Tech. 357, 373 (noting that *Carpenter* "in effect endorses the mosaic theory of privacy"). *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021), does not change this analysis, as it concerned pole cameras, not automated location tracking. *Id.* at 524 (pole cameras directed at Tuggle's home did not effectuate a search because they "exposed no details about where Tuggle traveled, what businesses he frequented, with whom he interacted in public, or whose homes he visited"). The proper analogue is the indiscriminate mass aerial surveillance program at issue in *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (en banc) ("*LBS*"), which, unlike "pole cameras" but like MDS, is a "citywide prolonged surveillance campaign." *Id.* at 345–46.

Second, LADOT attempts unsuccessfully to draw factual distinctions between its vehicle location dragnet and the tracking at issue in *Carpenter* and *Jones*. LADOT claims it only collects the location of scooters, not individuals, Opp'n 17, 25, but that belies the truth. Just like cell phones, scooters can only go where people take them. *Carpenter* and *Jones* make clear that the devices whose location the government tracks need not be physically connected to an individual for the information collected to be private. In *Jones*, the collected data originated from the defendant's wife's car, not from Jones himself, and included the locations of the car when parked and abandoned. 565 U.S. at 403. In *Carpenter*, the location data derived from the cell towers to which the mobile phones connected, not the telephones themselves. 138 S. Ct. at 2212. Whether the locations originate from the vehicle or directly from the rider is, therefore, a distinction without a difference.[2] The Fourth Amendment asks whether LADOT's data can reveal the whereabouts of Mr. Sanchez and, in turn, sensitive and private information about his life which he is entitled to protect from unreasonable acquisition. *See LBS*, 2 F.4th at 344 ("Whether those [location] points are obtained from a cell phone

[2] The location information MDS collects from micromobility providers may in fact be a hybrid that incorporates both device locations as well as GPS coordinates from riders' mobile phones, narrowing the distinction even further with *Carpenter*. *See* Brief of *Amici Curiae* Seven Data Privacy and Urban Planning Experts at 20–21, ECF No. 23.

pinging a cell tower or an airplane photographing a city makes no difference" because location data is so revealing).

LADOT also argues that *Carpenter* is inapplicable to dockless micromobility because people use scooters much less than mobile phones. Opp'n 38–39. However, the revelatory nature of the information—not how much raw data the government collects or the popularity of the technology—is the core of the search analysis. So long as Mr. Sanchez plausibly that alleges that private, revealing information about him can be easily gleaned by MDS data, *Carpenter* applies. 138 S. Ct. at 2217 ("*As with GPS information*, the time-stamped data provides an intimate window into a person's life," citing *Jones*) (emphasis added).[3] Notably, LADOT fails to say anything about the myriad ways MDS data is *more* revealing than either CSLI or *Jones*' GPS data. *See* Br. 30–33.

Third, LADOT wrongly relies on pre-*Carpenter* cases that lack the hallmarks of the technologically assisted dragnet MDS enables here. The taxicab cases LADOT cites concern the diminished expectations of privacy of specially licensed taxi drivers "who choose to participate in a 'closely regulated industry.'"

[3] In any case, LADOT's reasoning that MDS is justified due to the "proliferation of electric scooters and bicycles" that are "overwhelm[ing] public places and infrastructure" undermines its position that micromobility vehicles are too uncommon to receive Fourth Amendment protection. *See* Opp'n 10.

Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 657 (1995); Opp'n 36–37.[4] GPS technology merely replaced, rather than "impermissibly enhance[d]," long-standing requirements that taxi drivers maintain written logs of rides' start and end locations. *LBS*, 2 F.4th at 341. LADOT, on the other hand, never collected—and never *could have* collected—the foot-by-foot granular data that MDS collects today. The lone case that also concerned taxi *passenger* rights involved locations only with reference to far less precise census tracts.[5] *Azam v. D.C. Taxicab Comm'n*, 46 F. Supp. 3d 38, 43 (D.D.C. 2014).

LADOT's citations to other pre-digital search cases are equally unavailing, as "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33–34 (2001); *see* Opp'n 35–36. *United States v. Weaver* concerned manual—not technologically assisted—

[4] *See El-Nahal v. Yassky*, 993 F. Supp. 2d 460, 465–66 (S.D.N.Y. 2014) (no reasonable expectation of privacy in trip data given long history of regulation of taxicab industry); *Buliga v. New York City Taxi Limousine Comm'n*, No. 07 CIV. 6507 (DLC), 2007 WL 4547738, at *2 (S.D.N.Y. Dec. 21, 2007) (discussing same); *Carniol v. New York City Taxi and Limousine Comm'n*, 975 N.Y.S.2d 842, 848 (N.Y. Sup. Ct. 2013) (same). For a helpful discussion of micromobility's contrasting lack of regulation, *see* Brief of Center for Democracy & Technology and Electronic Privacy Information Center as *Amicus Curiae* at 21–22, ECF No. 24.

[5] Census tracts are "roughly equivalent to a neighborhood" and contains 1000–8000 people. *See Finding Census Tract Data: About Census Tracts*, Michigan State University, https://libguides.lib.msu.edu/tracts.

surveillance conducted of an individual after he disembarked a public bus. 1996 WL 554746 (2d Cir. 1996) (unpublished); *see Carpenter*, 138 S. Ct. at 2217 (contrasting invasiveness of technologically-assisted location tracking with police monitoring "[p]rior to the digital age"). *United States v. Moffett* restated the non-controversial rule that the government does not conduct a search when it reads a non-private train manifest or other paper ticketing record. 84 F.3d 1291, 1293 (10th Cir. 1996). And *Patel v. City of Montclair* addressed an invasion of private property, not the invasion of an expectation of privacy. 798 F.3d 895, 899–900 (9th Cir. 2015) (regarding entry into public areas of a privately owned motel).

2. *Carpenter forecloses LADOT's argument that the third-party doctrine extinguishes Mr. Sanchez's expectation of privacy.*

LADOT's reliance on the third-party doctrine is also barred by *Carpenter* and its progeny. Opp'n 40–45. *Carpenter* established, and this Court in *Moalin* agreed, that individuals do not relinquish their reasonable expectations of privacy in their digital data simply because a third party collected the data initially. *Carpenter*, 138 S. Ct. at 2217 ("Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."); *Moalin*, 973 F.3d at 992 ("The assumption-of-risk rationale underlying the [third-party] doctrine is ill suited to the digital age, in which people reveal a great deal of

information about themselves to third parties in the course of carrying out mundane tasks.") (internal quotations omitted). The Supreme Court "decline[d] to extend *Smith* and *Miller* to cover these novel circumstances" presented by advancements in technology, noting its own history of "special solicitude for location information in the third-party context." *Carpenter*, 138 S. Ct. at 2217, 2219.

LADOT argues that *Carpenter* does not apply to micromobility riders who understand they will disclose their locations to a third party to pay for their vehicle rental. Opp'n 43. But the knowing disclosure of data to a third party is not the doctrine's lone touchstone. "The nature of the particular documents sought" matters too. *Carpenter*, 138 S. Ct. at 2219 ("*Smith* and *Miller,* after all, did not rely solely on the act of sharing."). In interpreting *Carpenter*, this Court in *Moalin* articulated four features of digital data collection that counsel against applying the third-party doctrine: (1) the revelatory nature of the data, as opposed to the "limited" sensitivity of pen register data, 973 F.3d at 991; (2) the duration of the data's collection and retention, which far exceeded the limited uses in *Smith* and *Miller*, *id.* at 991; (3) the large number of people captured by the collection scheme, *id.* at 992; and (4) the inevitability of third-party data collection in the digital age, which makes it nearly impossible to avoid the intermediaries with ownership of otherwise private data, *id.* All four features of that data collection are

present here. *See, e.g.*, *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000) (applying the third-party doctrine to motel guest registration records they did not reveal "highly personal information.") (cited in Opp'n 36).

Furthermore, both the shared vehicles here and the cell towers at issue in *Carpenter* automatically disclose location information to their third-party providers. Opp'n 43; *Carpenter*, 138 S. Ct. at 2220 (CSLI is automatically generated by "dint of [a phone's] operation, without any affirmative act on the part of the user beyond powering up"). Neither a micromobility rider nor a cell phone user can decide whether a third party generates logs of their precise location information, nor can they prevent the government from collecting their locations without forfeiting access either to their shared vehicles or their cell phones. Under these circumstances, they cannot have voluntarily "assumed the risk" that their locations would wind up in the hands of the government. *Carpenter*, 138 S. Ct. at 2216 (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)). The third-party doctrine is therefore inapplicable to MDS.

3. *LADOT is wrong to argue that riders' reasonable expectations of privacy are defeated by rental contracts.*

LADOT's contract-based defenses of MDS's geolocation dragnet are equally unpersuasive. Setting aside LADOT's offensive assertion that only wealthy people are entitled to constitutional protections, *see* Opp'n 52 ("privacy has always been something that people could buy"), its distinction between vehicle owners

and vehicle renters conflicts sharply with the Supreme Court's admonition that "the entitlement to an expectation of privacy does not hinge on ownership." *Rakas v. Illinois*, 439 U.S. 128, 161 (1978). This applies equally to vehicles. *Byrd v. United States*, 138 S. Ct. 1518, 1528 (2018) (recognizing "no reason why the expectation of privacy that comes from lawful possession and control and the attendant right to exclude would differ depending on whether the car in question is rented or privately owned"); *United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2000), *as amended* (Mar. 5, 2001) (renter had expectation of privacy in a rental car during rental period). There is no constitutionally relevant distinction between the expectation of privacy from third-party tracking of a vehicle "someone else owns free and clear" versus a third party "maintain[ing] the ability to locate a car that it has a right to repossess in the event of default." Opp'n 49–50.[6] As a renter, Mr. Sanchez enjoys the right to maintain his privacy in the whole of his movements while in exclusive possession of a shared scooter.

LADOT also wrongly invokes contract law to try to undermine Mr. Sanchez's expectation of privacy, arguing that he agreed to dockless vehicle providers disclosing his precise geolocation information to the government. But whether or not Mr. Sanchez assented to some variant of device providers' terms of

[6] *Jones* itself concerned the expectation of privacy a driver in possession of, but without title to, a car. *Jones*, 565 U.S. at 402 (targeted car belonged to Jones' wife).

service, he would still enjoy an expectation of privacy in his precise location records *as against the government*. The reason for rejecting the third-party doctrine in digital location tracking cases is that the provision of such data to a private company lacks the traditional indicia of voluntariness that undergirds application of the doctrine. It is for that reason that the *Carpenter* majority, over the objections of a dissent, ignored a contract between Carpenter and his mobile phone provider to store—indeed, to *own*—Carpenter's locations. 138 S. Ct. at 2242 (Thomas, J. dissenting) ("Carpenter stipulated below that the cell-site records are the business records of Sprint and MetroPCS."); *see United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (contractual agreements allowing telephone companies to listen in on communications or email providers to access emails do not diminish expectations of privacy in either). This is likely the reason that the district court in *United States v. Diggs* did not rely upon the contract LADOT seeks judicial notice of: it was irrelevant to the analysis.[7] 385 F. Supp. 3d 648, 650 (N.D. Ill. 2019). In any event, that was an agreement between the seller and Diggs' *wife*, who also

[7] LADOT seeks judicial notice of two documents in support of its Opposition: the purchase contract in *Diggs*, and certain CalECPA legislative materials. *See* Request for Judicial Notice, ECF No. 40. Mr. Sanchez does not oppose judicial notice of the existence of the CalECPA bill analysis, but opposes notice of the *Diggs* contract. The contract is unauthenticated, contains vague and contested provisions, and is irrelevant here. *Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001) (court may not take "judicial notice of a fact that is subject to reasonable dispute").

drove the vehicle. *Id.* at 652. Whatever the buyer and seller intended vis-à-vis repossession of the car surely could not have extinguished Diggs' expectations of privacy. *Byrd*, 138 S. Ct. at 1529 (holding that provisions in rental car contracts "do not eliminate an expectation of privacy, all of which concern risk allocation between private parties").[8]

LADOT disclaims the *Byrd* holding's application here by suggesting that, while a renter maintains an expectation of privacy in the contents of their vehicle, they cannot maintain a similar expectation of privacy in the location of the vehicle itself. Opp'n 35. But this distinction between physically searching a vehicle and tracking it finds no support in the law, and LADOT cites none. Just as Mr. Jones had an expectation of privacy in the location of a vehicle he did not own, so too must renters of shared micromobility devices.

[8] At the district court, LADOT unsuccessfully sought judicial notice of the contents of three privacy policies, without any evidence that any of them applied to Mr. Sanchez himself. 2 E.R. 112–4; *see* 1 E.R. 9 n.7 (denying judicial notice require because the "privacy policies are not incorporated by reference in the Complaint and their authenticity is subject to dispute"). Now, LADOT asks this Court to consider additional extra-record documents, again without evidence that Mr. Sanchez assented to these *particular* agreements. *See, e.g.*, Opp'n 42. In the absence of any incorporation or reliance by Mr. Sanchez in his Complaint, they cannot be considered in this appeal of a Rule 12(b)(6) motion that did not address them.

4. *Mr. Sanchez has standing to challenge LADOT's collection of precise location information, even if the agency has not yet analyzed it.*

LADOT's final attack on Mr. Sanchez's constitutional claims addresses standing. LADOT erroneously argues that because Mr. Sanchez does not allege that the agency ever analyzed its MDS data to identify sensitive information about him, he does not enjoy standing to challenge its collection. Opp'n 32–34. This is wrong.

It is well established that the collection and analysis of private data are separate Fourth Amendment events. *See Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 618 (1989) (the "collection and subsequent analysis of . . . biological samples must be deemed [separate] Fourth Amendment searches."). *Carpenter*, for instance, passed on the government's data *collection*, not just on its later analysis. 138 S. Ct. at 2209, 2212, 2217; *see id.* at 2220 ("The Government's *acquisition* of the cell-site records was a search . . . .") (emphasis added). The Court required a warrant as a precursor to collecting CSLI, even though the government would need to analyze it later to place Mr. Carpenter at the scene of the crime. *Id.* at 2218. Similarly, it is a search to conduct an invasive blood test that "places in the hands of law enforcement authorities a sample that can be preserved and from which it is *possible* to extract information," even without an allegation of

actual analysis. *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2178 (2016) (emphasis added).

The same possibility of future analysis led this Circuit to hold that the National Security Agency's mass collection of private telephone metadata was a search. *Moalin*, 973 F.3d at 992 (recognizing "the collection of millions of other people's telephony metadata, and the ability to aggregate and analyze it, makes the collection of Moalin's *own* metadata considerably more revealing," even without evidence of actual analysis) (emphasis in original); *see also ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (rejecting argument that injuries depend "on the government's *reviewing* the information collected," holding that "appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them") (emphasis in original); *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 526 (7th Cir. 2018) (finding automated collection of electricity smart-meter data to be a search even though "observers of smart-meter data must make some inferences to conclude, for instance, that an occupant is showering, or eating, or sleeping"); *LBS*, 2 F.4th at 344–45 (because analysis of aerial surveillance data "is what enables deductions from the whole of individuals' movements, the Fourth Amendment bars BPD from warrantless access to engage in that labor-intensive process" in the future).

Kyllo undermines, rather than supports, LADOT's "analysis only" theory. Opp'n 30–31. There, the Supreme Court held that capturing information available in a public setting (the heat emanating from a home) is a search because that information could enable inferences about private conduct within the home. 533 U.S. at 34. The prohibition was on the warrantless collection itself, and did not turn on the good graces of the government not to mine it for the privacies it would reveal. *See Kyllo*, 533 U.S. at 38 (noting that "one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful"). The collection alone of Mr. Sanchez's information is therefore a search.

LADOT confuses matters by conflating Fourth Amendment standing with Article III's case-or-controversy requirement. Opp'n 33. There is a strong argument that Fourth Amendment "standing" no longer exists as a separate doctrine. In *Rakas*, the Supreme Court held that standing arguments are "more properly subsumed under substantive Fourth Amendment doctrine." 439 U.S. at 139 ("[W]e think the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing."). Regardless, Mr. Sanchez alleges, and LADOT does not dispute, that the surveillance program LADOT implemented *in fact* collected his precise location

information, unlike in *Laird v. Tatum*, 408 U.S. 1 (1972). Further, Mr. Sanchez plausibly alleges both past injury (prior collection of his location information) as well as the prospect of future injury (that he is a frequent micromobility rider who will have his trip information collected by MDS in the future). This makes this case very different from *Clapper v. Amnesty International USA*, 568 U.S. 398, 411 (2013), where the plaintiffs had difficulty alleging that the government would target them at all. *See Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1118 (9th Cir. 2017) (describing the case as unlike *Clapper* because "both the challenged conduct and the attendant injury have already occurred"). And since MDS is ongoing, Mr. Sanchez enjoys standing to challenge it prospectively. *See Melendres v. Arpaio*, 695 F.3d 990, 998 (9th Cir. 2012) (defendants' express policy of stopping people based on suspected unlawful presence established a likelihood that plaintiffs—who had been stopped only once in the past—would be stopped again in the future).

B. LADOT's contested justifications for collecting Mr. Sanchez's location information are disputed and cannot be credited on a motion to dismiss.

The district court improperly concluded MDS's precise location collection is a reasonable exercise of LADOT's regulatory authority by failing to accept as true Mr. Sanchez's allegations and by applying the wrong legal standard to uphold it. In its Opposition, LADOT offers no compelling defense of this error.

At bottom, this case concerns whether LADOT requires the *precise*, as opposed to coarse, location data of *every* micromobility rider in the City, and whether storing this sensitive data in perpetuity reasonably relates to the agency's transportation planning goals. Mr. Sanchez alleges that it does not. Whatever the goals set out by LADOT for regulating micromobility devices, this collection is far too invasive to meet those goals, and other less privacy-intrusive methods of regulation are available to the agency. *See* 3 E.R. 321–22; *see, e.g.*, Brief of Center for Democracy & Technology and Electronic Privacy Information Center at 24–31, ECF No. 24 (discussing aggregation, sampling, and differential privacy as alternatives to individual data collection); Brief of *Amici Curiae* Seven Data Privacy and Urban Planning Experts at 28, ECF No. 23 (discussing data binning, *k*-anonymity, and tessellation as additional alternatives). In fact, the collection of individual trip data is likely altogether irrelevant since transportation planning relies principally on statistically significant aggregated data over individualized trip data. *See* Brief of *Amicus Curiae* Kevin Webb at 14–15, ECF No. 25 (explaining that transportation "planning does not occur by anecdote, but rather by understanding behavior in the aggregate").

Nevertheless, the district court erred when it ignored Mr. Sanchez's allegations about the utility and importance of the collected data to LADOT's regulatory agenda, and denying him the opportunity to prove these allegations in

discovery. Br. 44–47. Short of discovery, the district court could not have properly appraised the factual dispute about whether MDS's data collection is "limited in its intrusiveness as is consistent with satisfaction of the administrative need that justifies it." *United States v. Grey*, 959 F.3d 1166, 1183 (9th Cir. 2020) (quoting with approval *United States v. Bulacan*, 156 F.3d 963, 967 (9th Cir. 1998)).[9]

To win dismissal outright based on its own contested justifications for MDS, LADOT relies on *Naperville* to argue that MDS is unintrusive by directing this Court to extra-record evidence beyond the scope of the Complaint to claim the agency limits third-party access to the agency's data. Opp'n 56 (citing "Data Protection Principles") & 57 (citing "On-Demand Mobility Rules and Guidelines 2021"). Given Mr. Sanchez's lack of opportunity to dispute the contents of these documents, or to introduce additional evidence in support of his position, this Court should not affirm the district court's premature dismissal of this action. In any event, the search at issue in *Naperville* regarded smart utility meters, not the type of location data collection that *Jones* and *Carpenter* recognized invades expectations of privacy. *Naperville Smart Meter Awareness*, 900 F.3d at 529

[9] Contrary to LADOT's suggestion, the test first set out in *United States v. Davis*, 482 F.2d 893, 910 (9th Cir. 1973) and quoted in *Bulacan* remains good law, and was cited by this Court just last year in *Grey*, 959 F.3d at 1183—18 years after the Supreme Court's decision in *Board of Education of Independent Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 837 (2002). The Supreme Court has not overruled this Court's administrative search cases, and no court has concluded that it has.

(cautioning that its holding "depends on the particular circumstances of this case," and may have been different if a city "collect[ed] the data at shorter intervals.").

Nor is it enough to say, as LADOT does here, that Mr. Sanchez can simply elect not to ride a dockless vehicle if he wishes to safeguard his privacy. *See* Opp'n 59 (citing *Davis*, 156 F.3d at 910–911). LADOT creates this false choice from language in *Davis* that is no longer good law. More than 40 years after *Davis*, this Court explained that the reasonableness of airport searches does not depend on explicit or implied consent, overruling the basis for the suggestion that individuals can merely forego riding airplanes to save themselves from government searches. *United States v. Aukai*, 497 F.3d 955, 960 (9th Cir. 2007).[10]

Finally, as explained in Mr. Sanchez's principal brief, the administrative search scheme here requires either a warrant or other mechanism for neutral review pre-search. Br. 47–48. LADOT concedes that *City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015) applies to *some* administrative searches, Opp'n 59, even though *Patel* unequivocally stated that "absent consent, exigent circumstances, or

[10] The endorsement of MDS by its proprietor the Open Mobility Foundation fails to meet this standard. *See* Brief of Open Mobility Foundation at 25–32, ECF No. 44. Although the Foundation purports to offer examples of why precise location collection is necessary to regulate micromobility, *id.* at 22, it does not explain how any of the accomplishments it cites could *not* have been achieved without precise trip data, nor whether they could have been achieved through coarse data collection. *See, e.g.*, *id.* at 27–28 (discussing MDS use to increase access and equity without explaining how less intrusive alternatives are insufficient).

the like, in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker." *Patel*, 576 at 409. Importantly, *Patel* does not prescribe the form of review, requiring only "an opportunity to obtain" such a neutral review. *Id.* at 420.[11] If LADOT does not wish to provide such a mechanism to mitigate the intrusiveness of its dragnet, it could simply resort to consent or to a warrant—that or halt its data collection program altogether. *Id.* at 423.

III. CALECPA OFFERS MR. SANCHEZ A PETITION REMEDY TO ADDRESS THE UNLAWFUL COLLECTION OF HIS PERSONAL INFORMATION.

LADOT's attempt to nullify CalECPA's statutory remedy is inconsistent with its text, the intention of the Legislature, and the law of statutory construction in California. CalECPA requires that the government get a warrant, subpoena, or other specified process before compelling the production of information from service providers like the micromobility companies here. LADOT failed to obtain any of those legal processes, and now seeks to eliminate California's statutory right to challenge the unlawful collection of that information by the government. But riders have a petition right—enumerated explicitly in CalECPA—to address

[11] In that way, *Patel* does not require a "dial-a-judge" for every micromobility rider or every micromobility operator, as suggested by LADOT, so long as the agency establishes some neutral administrative process. Opp'n 58.

LADOT's unlawful collection. If endorsed by this Court, LADOT's argument would encourage extra-judicial accumulation of personal information and deprive people of petition rights guaranteed under the law.

A. LADOT's reading of CalECPA eviscerates important statutory petition remedies that are afforded under California law.

LADOT's argument that CalECPA offers "no private right of action" is belied by the statute's provision of a petition remedy to individuals whose information is targeted by unlawful data collection. Penal Code § 1546.4(c). LADOT chooses not to call that petition remedy a "private right of action," but the label is irrelevant. What matters is that Mr. Sanchez can seek relief in court—including in a federal district court, as he did here—to seek redress from LADOT's violation of his privacy.

In enacting CalECPA, the Legislature enumerated an explicit petition right for individuals affected by unlawful government collection of their information. Cal. Penal Code § 1546.4(c). LADOT argues that the presence of a "private right of action" in federal ECPA indicates that such a right is absent in CalECPA. Opp'n 64. But this argument is based on a false premise: that CalECPA is silent on whether relief is available. *See id.* ("CalECPA lacks an analogous provision."). In fact, CalECPA provides an explicit petition right for people to modify the relevant process or delete their information. Cal. Penal Code § 1546.4(c).

If the Legislature intended to deprive Californians of a private remedy here, it would have done so explicitly, as it has under numerous other statutes. *See, e.g.*, Cal. Pub. Con. Code § 2205(e) ("This act does not create, nor authorize, a private right of action or enforcement of the penalties provided for in this act."); Cal. Bus. & Prof. Code § 22948.23(a) ("This chapter shall not be deemed to create a private right of action, or limit any existing private right of action."); Cal. Civil Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.").

LADOT's misguided assertion that it is accountable for CalECPA violations to only the California Attorney General disregards these petition rights. The legislative history demonstrates unambiguously the Legislature's intent to allow *both* the Attorney General *and* affected individuals to enforce CalECPA.[12] In addition to misinterpreting CalECPA, LADOT's reading—that "petitions" cannot be part of a separate civil action—would eviscerate other statutory petition rights commonly found in California law. *See, e.g.*, Cal. Penal Code § 18150 (individual petition right to enjoin gun possession when a person poses a danger); *id.* at

[12] Assembly Committee on Privacy and Consumer Protection, SB 178 (Leno) Committee Analysis , at p. 8 (June 19, 2015) (noting that CalECPA "provides authorization to affected entities and the Attorney General to take action to uphold these requirements."), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178.

§ 186.35(a) (individual petition right for persons to remove themselves from a shared gang database); Cal. Civil Code § 1798.201 (individual petition right to designate personal information as impersonated in cases of identity theft); Cal. Civil Code § 8480 (individual petition right for property owner to seek court order releasing property lien).

Statutory petition rights are flexible under California law and allow for people to vindicate their rights as efficiently as possible. The distinguishing characteristic of "petitions," unlike "civil actions," is that they can be, but need not be, separate free-standing civil suits. For example, the California Attorney General's guidance associated with Penal Code Section 18150 (governing gun-violence restraining orders) indicates that, under the petition right, a "family member, household member, or law enforcement officer can request that a civil court in their jurisdiction issue a [Gun Violence Restraining Order] based on facts they present through a formal, written application, and/or at a hearing before a judge."[13] Similarly, a CalECPA petition under Section 1546.4(c) can be filed in a criminal case where the warrant resulted from the challenged collection of

[13] California Department of Justice, Information Bulletin: Gun Violence Restraining Order Process, No. 2019-BOF-02 (January 30, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/firearms/infobuls/2019-bof-02.pdf. A form produced by the Judicial Council of California to assist people in filing petitions in Superior Court is available at https://www.courts.ca.gov/documents/gv100.pdf.

information or, if no related action is already underway, as a separate civil action as Mr. Sanchez has brought here. *See* Br. 61 (citing cases in which a petition is the basis for a civil claim).

B. The text of CalECPA entitles Mr. Sanchez to relief in court, notwithstanding LADOT's failure to seek pre-enforcement judicial review of MDS.

Contrary to LADOT's assertion, CalECPA's statutory text fully supports Mr. Sanchez's claim here. The statute provides a broad petition right to "an individual whose information is targeted" by a governmental legal process. Cal. Penal Code § 1546.4(c). Because Mr. Sanchez's information is targeted and eventually captured by LADOT every time he rides, 3 E.R. 31, he can file a CalECPA petition in a court that possesses the authority to issue the required legal process, notwithstanding LADOT's failure to comply with its obligations. And Mr. Sanchez exercised this right by filing this action over which the district court has supplemental jurisdiction. *See* 28 U.S.C. § 1367(a).

LADOT's primary argument appears to be that the phrase "issuing court" eliminates the possibility of filing a Section 1546.4(c) petition when no court previously issued the legal process required by CalECPA. That argument fails, for three reasons.

First, LADOT's would eliminate petition rights—and the ability for people to protect their privacy—when a government entity ignores CalECPA's

requirements entirely, as LADOT has done here. The reason no court has issued the required process is that LADOT implemented its mass surveillance program without seeking any manner of judicial approval. This Court should not indulge any interpretation that allows for the flagrant disregard of the statute's direct mandate to seek judicial review *before* collecting personal information. Br. 53–54, 58–60.

Second, LADOT's attempt to narrow CalECPA's petition rights by demanding that a court must have *already* issued the process is contrary to how "issuing" is often used, and not supported by CalECPA's statutory scheme. The phrase "issuing court" refers to the court *with the authority* to issue the required process. Br. 55–57. Here, the Superior Court of the State of California qualifies as the issuing court, and the district court could exercise supplemental jurisdiction over the claim. As federal regulations indicate, "issuing" can sensibly refer to the authority to issue rather than the fact of prior issuance. *Id.* at 56–57.[14]

Third, the inclusion of a deletion remedy in Section 1546.4(c) indicates that remedies under CalECPA are available even when a court is not yet involved. LADOT incorrectly claims that the language "void or modify" presupposes the

[14] LADOT attempts to distinguish these regulations based on their subject matter. Opp'n 63. But it concedes that 18 U.S.C. § 1028 does define "issuing" in the way that is "akin to how Sanchez would define 'issuing court' in CalECPA." *Id.* The fact that regulations define "issuing" in a way that would fulfill the statutory purpose of CalECPA is strong support for Mr. Sanchez's interpretation.

existence of an order. Opp'n 62–63. But under the statute, any "legal process" can be voided or modified, not just court orders. Cal. Penal Code § 1546.4(c) (referring to "a warrant, order, or other legal process"). Moreover, an individual's ability to seek a court order directing the government to delete personal information is a protection entirely disconnected from the nature of the process used to capture the data. The deletion remedy provides vital relief, for example, for people whose devices are accessed warrantlessly by law enforcement in violation of Penal Code Section 1546.1(a)(3), or for people attending a protest where unlawful cell-site simulator surveillance was deployed. These remedies are available, critically, regardless of whether the government complies with the mandate to obtain court approval.

C. California law on statutory construction does not permit LADOT's restrictive reading of CalECPA.

LADOT's brief is silent on the rules of statutory construction in California, likely because its reading of CalECPA is inconsistent with them. Stripping individuals of their petition rights for CalECPA violations does not construe the Penal Code "according to the fair import of [its] terms, with a view to effect its objects and to promote justice." Cal. Penal Code § 4. Nor does it interpret CalECPA, a remedial statute, "to effectuate the object and purpose of the statute and to suppress the mischief at which it is directed." *People v. Clayburg*, 211 Cal. App. 4th 86, 91 (2012).

LADOT claims that even if MDS violates CalECPA and unlawfully collects the personal information of thousands of riders in Los Angeles, those riders have no means by which to challenge LADOT's invasion of their privacy. Opp'n 65. This argument plainly conflicts with *Clayburg* and encourages, rather than suppresses, the large-scale unlawful collection of Californians' private information at which CalECPA is directed. It therefore cannot be squared with California law and must be rejected.

CONCLUSION

Mr. Sanchez respectfully requests this Court reverse and remand the decision below for further proceedings.

Dated: December 20, 2021

Respectfully submitted,

/s/ Mohammad Tajsar
Mohammad Tajsar
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA

Attorneys for Plaintiff-Appellant

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 21-55285

I am the attorney or self-represented party.

This brief contains 6,970 **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.
- ( ) 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/ Mohammad Tajsar **Date** 12/20/2021

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov