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 OPENING 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
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 CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

CONSTITUTIONS, STATUTES AND RULES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

INTRODUCTION

This appeal concerns the City of Los Angeles' effort to rely on computer code, instead of time-tested analog regulation, to manage a growingly popular mode of personal transportation. Micromobility vehicles are the new vanguard in urban transit, offering an easy-to-use, lightweight alternative to traditional forms of transportation. These vehicles—typically dockless electronic bicycles or scooters—are offered as short-term rentals by private companies. By downloading a mobile phone application and registering an account, people can easily rent these personal vehicles and use them to traverse city streets.

Since its introduction in Southern California, dockless micromobility has steadily grown in popularity across the country, and not merely as a recreational novelty. Recent surveys show that dockless vehicles are increasingly popular as an alternative form of necessary transportation, taking passengers to and from work, school, errands, and leisure activities. They also increasingly connect riders with other forms of mass transit in cities, serving as the conduit to and from residences to public transit hubs. This is especially true in the City of Los Angeles, where distances and decades of car-centric transportation planning create significant challenges for those who cannot afford traditional modes of private transportation, like automobiles.

With the popularity of micromobility vehicles, cities have argued that they

need to regulate their distribution and use. However, instead of applying traditional forms of transit regulation, the City of Los Angeles' Department of Transportation ("LADOT") chose a method designed to collect as much sensitive and detailed location data about micromobility riders as possible. With its new regulations, Los Angeles now automatically ingests from micromobility providers the precise and granular real-time and historical location data of all riders within the City.

Justin Sanchez is one of these riders. He brought this action challenging LADOT's location surveillance as both unconstitutional under the Fourth Amendment and Article I, §13 of the California Constitution and violative of California's Electronic Communications Privacy Act ("CalECPA"), Penal Code section 1546 *et seq*. He alleged facts sufficient to support these claims. Yet the district court dismissed Mr. Sanchez's Complaint with prejudice, without argument, and without any opportunity to amend that initial pleading. In doing so, the district court failed to give appropriate weight to controlling law and Mr. Sanchez's well-pled facts concerning both how invasive LADOT's data collection scheme is and how LADOT failed to provide any reasonable justification for its expansive surveillance dragnet. The lower court also erroneously applied the third-party doctrine contrary to Supreme Court precedent and this Court's recent pronouncements. It further erred in dismissing Mr. Sanchez's CalECPA claim,

which provides a civil remedy to address LADOT's warrantless collection of electronic communications information. This Court should reverse.

JURISDICTIONAL STATEMENT

Mr. Sanchez invoked the district court's jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 1343, and 28 U.S.C. § 1367. On February 23, 2021, the district court entered judgment for Defendants. 1 Excerpt of Record ("ER") 1. Mr. Sanchez filed a timely notice of appeal. 3-ER-321–23; *see* Fed. R. App. P. 4(a)(1)(A). This Court has jurisdiction under 28 U.S.C. § 1291.

ISSUE PRESENTED

The issues presented in this appeal are as follows:

Whether the district court erred in ignoring Mr. Sanchez's allegations about the sensitivity of the precise location and movement information collected by LADOT, and LADOT's lack of operationally specific justification for this collection.

Whether the district court erred in summarily dismissing with prejudice Mr. Sanchez's Complaint without a hearing and without affording him any opportunity to amend the initial pleading.

Whether the district court erred in holding that LADOT's collection of real-time and historical GPS location data of every micromobility ride, on every vehicle, of every rider, and on every street in the City of Los Angeles violates Mr. Sanchez's rights to be free from an unreasonable search under the Fourth Amendment and the California Constitution.

Whether the district court erred in holding that California Penal Code section 1546.4(c), one of CalECPA's remedial provisions, does not provide Mr. Sanchez a civil cause of action when LADOT failed to seek court approval prior to collecting micromobility riders' sensitive location information.

STATEMENT OF THE CASE

I. FACTUAL SUMMARY[1]

A. LADOT created a dockless vehicle permitting program requiring operators to disclose their users' detailed location data.

Beginning in 2017, numerous private companies began deploying shared motorized scooters and electric bicycles on Los Angeles streets. These vehicles are "dockless" in that rides need not start from a fixed docking station, unlike certain municipal bicycle sharing programs. Instead, micromobility rides can begin and end anywhere, and individual customers can rent them via a smartphone application. The vehicles generally have rechargeable batteries, Global Positioning System ("GPS") trackers, and wireless connectivity to the internet. When users end the rental through the application, they are informed of its cost and charged accordingly.

Since launching in Los Angeles, micromobility vehicle use has surged. To regulate its growing use, on September 28, 2018, the Los Angeles City Council passed an ordinance compelling LADOT to implement a pilot program for operators of dockless bicycles, electric bicycles, and electric scooters to do business within the City. Under this pilot, the ordinance mandated that "an

[1] This section recounts the allegations made in Mr. Sanchez's Complaint. 3-ER-302–20. For any additional facts not originally alleged in the Complaint, a footnote with a citation is provided.

operator of a shared mobility device shall obtain a permit from the Department [of Transportation] and comply with all Department permit rules, regulations, indemnification, insurance and fee requirements."

LADOT responded to the City Council's mandate by requiring that micromobility operators seeking a permit to operate agree to implement an application programming interface ("API") called the Mobility Data Specification ("MDS").[2] Once an operator employs MDS, the API sends data collected by the operator's fleet of vehicles automatically to LADOT's servers, where the information is stored in perpetuity.

Through MDS, LADOT collects a wide variety of data directly from the micromobility providers without direct consent from riders. These include a unique device identifier for the vehicle, the type of vehicle, and each trip's location information. That location information includes the starting point of the trip, its starting time, its end point, its ending time, and the specific route taken by a user. The location data collected is maximally precise to within as little as a few

[2] An API is a segment of computer code "that acts as an intermediary between two other programs — or two components within a program — to exchange information." Dave Johnson, *A guide to APIs, software that helps different apps work together*, BUSINESS INSIDER, May 13, 2021, https://www.businessinsider.com/what-is-an-api. The purpose of an API is to standardize the exchange of information between these two other programs, and to make that exchange scalable. *Id*.

centimeters of the device's actual location.[3] Starting and ending locations are sent to LADOT in real-time, and the specific route information uploads after 24 hours.

B. Precise location information is easily identifiable and revelatory of sensitive private information, even when ostensibly anonymous.

While LADOT does not directly collect riders' names through MDS, the sensitivity of the location information gathered makes identification likely nonetheless. "Recent research has shown that, given only a few randomly selected points in mobility datasets, someone could identify and learn sensitive information about individuals."[4] For instance, it is possible to identify a rider by coupling their precise trip data with easily obtainable information from just one other dataset—for instance, public voting records from particular addresses, or even simple,

---

[3] Mobility devices convey their geolocation data via GPS coordinates out to seven decimal places, which corresponds to a level of accuracy within 1.11 centimeters at the equator. For reference, GPS coordinates are often expressed through decimal degrees, via longitude and latitude coordinates. The more decimal places a GPS coordinate is measured in, the more precise the location it reveals is. *See Decimal Degrees*, WIKIPEDIA, https://en.wikipedia.org/wiki/Decimal_degrees (last visited July 22, 2021).

[4] Rob Matheson, *The privacy risks of compiling mobility data: Merging different types of location-stamped data can make it easier to discern users' identities, even when the data is anonymized*, MIT News (Dec. 7, 2018), http://news.mit.edu/2018/privacy-risks-mobility-data-1207 (describing Daniel Kondor et al., *Towards matching user mobility traces in large-scale datasets*, IEEE Transactions on Big Data (Sep. 24, 2018), *available at* http://senseable.mit.edu/papers/pdf/20180927_Kondor-etal_TowardsMatching_IEEE-BigData.pdf)) (cited in Complaint at 3-ER-312 ¶ 28 n.3).

repeated physical observation of a rider. Sometimes, no other information is required to identify people based solely on a location dataset. In one study, researchers identified 50% of people from only two randomly chosen data points in a dataset that contained only time and location data, and they could identify 95% of people using just four spatio-temporal points.[5]

In addition, otherwise anonymous location information may reveal important information about the individual's residence, the identities of their employer and friends, along with their personal and professional activities. And when end points are sensitive locations—like therapists' offices, political demonstrations, or Planned Parenthood clinics—those routes may also reveal the sensitive and private *reason* they made that trip.[6]

---

[5] Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, 3 SCI. REP. 1376 (2013), http://www.nature.com/articles/srep01376 (cited in Complaint at 3-ER-311–12 ¶ 28 n.4).

[6] Based on these realities, shared vehicle operators in this space protested the deployment of MDS and its privacy implications. Micromobility providers have objected to MDS's real-time location tracking mandate. *See, e.g.*, Kia Kokalitcheva, *Inside Uber's privacy battle with Los Angeles*, AXIOS, Dec. 18, 2019, https://www.axios.com/uber-scooter-data-privacy-battle-los-angeles-962f2f01-7146-4f33-9ebc-7f5eabd271f2.html. Other players in this sector, like RideReport, a company that builds software to help cities manage mobility data, agrees that "MDS includes a lot of potential personally identifiable information, especially the full route information contained in trip data, so there are a lot of privacy matters to consider." Madeline Kernan, *What is Mobility Data Specification (MDS) and other common questions*, RIDEREPORT, June 26, 2020, https://www.ridereport.com/blog/what-is-mds-questions.

C. LADOT has rapidly exported MDS to other forms of transport and across the country without justifying its mass collection of location data.

Despite the granular and precise data collected through MDS, LADOT did not provide any operationally specific justification for this mass surveillance. Nor did it develop a data collection and retention program narrowly tailored to meet even the abstract use cases it did identify. To the contrary, LADOT leadership expressly identified the MDS pilot program as a mechanism to "experiment" with people's data.[7] LADOT offered no explanation for why it needs *all* riders' geolocation information at maximum precision. Even when the City Council instructed LADOT to articulate "specific regulatory purposes for the collection and use of each type of data required by MDS" by February 25, 2020, LADOT simply did not comply. At the time Mr. Sanchez initiated this action, and more than three months after that February deadline, LADOT still had not articulated those purposes in response to the request.

Despite these privacy concerns, LADOT plans to expand the use of MDS to "all kinds of future transportation forms—from ride-hailing and car-sharing to

---

[7] David Zipper, *Cities can see where you're taking that scooter*, SLATE, Apr. 2, 2019, https://slate.com/business/2019/04/scooter-data-cities-mds-uber-lyft-los-angeles.html (quoting LADOT General Manager Seleta Reynolds, "When bikes and scooters showed up, they gave us a pretty interesting sandbox to start experimenting.") (cited in Complaint at 3-ER-314 ¶ 35 n.8).

delivery drones and autonomous vehicles."[8] It has also exported its use to cities across the country and the globe.

II. PROCEDURAL HISTORY

On June 8, 2020, Plaintiffs Justin Sanchez and Eric Alejo,[9] both serial micromobility riders in the City of Los Angeles, filed this action against LADOT and the City of Los Angeles (collectively "LADOT") alleging that MDS's data collection scheme violates the Fourth Amendment of the United States Constitution; Article I, § 13 of the California Constitution (California's analog to the Fourth Amendment); and CalECPA, California Penal Code section 1546 *et seq*. Mr. Sanchez is a resident of Los Angeles, and a customer of the micromobility providers Lime, Bird, and Lyft. Since MDS has been in effect, he has ridden these vehicles to and from home, work, and commercial centers in a fashion that he alleges makes his trips and habits identifiable from MDS's data set.

LADOT moved to dismiss the lawsuit, arguing it had the regulatory authority to impose MDS's data collection scheme on the operators. 2-ER-94–96.

---

[8] Laura Bliss, *This City Was Sick of Tech Disruptors. So It Decided to Become One.*, BLOOMBERG CITYLAB, Feb. 21, 2021, https://www.citylab.com/transportation/2020/02/los-angeles-transportation-data-mobility-scooter-mds-uber/606178/ (cited in Complaint, 3-ER-317 ¶ 41 n.12).

[9] With this appeal pending, Plaintiff Eric Alejo successfully moved to voluntarily withdraw his appeal. ECF 18–19. Plaintiff Justin Sanchez is now the sole remaining Appellant.

LADOT also argued that MDS does not constitute a search because it does not violate any expectation of privacy, and is presumptively reasonable. 2-ER-97–103. It also argued that CalECPA applies only in the criminal context, 2-ER-103–05, and that, in any event, only the Attorney General could enforce the statute in a civil action, 2-ER-105–06.

On February 23, 2021, the district court granted LADOT's motion to dismiss without a hearing, with prejudice, and without opportunity to amend the Complaint. 1-ER-3–11. First, the district court held that MDS's collection of location data does not constitute a search. Despite stating that it accepted as true the allegation MDS data was easily identifiable, *see* 1-ER-6, the district court noted that "MDS data was anonymized" in an attempt to distinguish the current case from *Carpenter v. United States*, 138 S.Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012). 1-ER-6. The district court held that because MDS does not collect riders' names and because it cannot "identify and compile *all* the trips that Plaintiffs took on scooters, from all the various providers they allege to have used," their reasonable expectations of privacy have not been violated. 1-ER-7 (emphasis in original). The district court alternatively held that the third-party doctrine bars Mr. Sanchez's constitutional claims because riders provide the locations of their rides to the operators prior to LADOT's collection of that information. 1-ER-7–9. Characterizing *Carpenter*'s rejection of the third-party

doctrine as an "exception" only for "cell phone location data," the court applied the doctrine, claiming, *ipse dixit*, that cell site location data was more revelatory than GPS location data and that riding shared vehicles is not as necessary to "participation in modern society" as owning a cell phone. 1-ER-7–8 (quoting *Carpenter*, 138 S.Ct.. at 2220).

The district court went on to rule that even if MDS constituted a search, "it would pass the balancing test" for reasonableness. 1-ER-9. On the one hand, the district court described MDS's intrusion as "limited" because "it would be difficult to actually effectuate the intrusion," while, on the other hand, "the government's interests are legitimate and substantial." *Id*. Assuming "self-evident" the proposition that "smart, effective regulation of a completely novel industry requires robust data," the district court ruled that the information MDS collects "would help the City determine how and where to adjust the rules of the road to accommodate them" and "to regulate the public right-of-way." 1-ER-9–10.

Turning to the CalECPA claim, the district court ruled that Penal Code section 1546.4(c), the remedial subsection upon which Mr. Sanchez's claim rests, only enables a suit in an "issuing court" to void or modify a warrant, order, or process that resulted in the unlawful collection of his data. 1-ER-10. Although LADOT did not raise this argument in its Motion, the district court concluded that

it was not the "issuing court" and that Mr. Sanchez therefore lacked a private right of action.

Though the district court acknowledged concerns regarding "the unprecedented breadth and scope of the City's location data collection," it nevertheless granted LADOT's motion with prejudice. 1-ER-11. It summarily found, without explanation, "that amendment to add more facts would be futile." *Id*. It issued judgment for LADOT on February 23, 2021, and this appeal followed. 1-ER-1, 3-ER-321–23.

SUMMARY OF THE ARGUMENT

LADOT's automated collection of the precise GPS locations of every shared micromobility ride taken in the City of Los Angeles is unprecedented in both its invasiveness and its scope. Whereas traditional monitoring of vehicles on public streets once required manual resources to identify and "tail" an individual of interest, modern technologically-assisted surveillance has dramatically lowered the cost for government officials to follow every vehicle at all times, including micromobility devices. MDS expands this surveillance capacity exponentially. By automatically monitoring every shared micromobility vehicle within city limits, MDS records the locations and movements—down to a maximum precision of a few centimeters—on every city street, on every ride, made by every rider. LADOT collects this information and stores it in perpetuity without any warrant, suspicion, or reasonable regulatory justification.

As a threshold matter, the district court summarily granted LADOT's motion to dismiss with prejudice, preventing Mr. Sanchez from amending his pleading as the federal rules require. The court failed to credit many of his allegations about the invasiveness of MDS as true, and ignored his allegations about LADOT's lack of justification for the data collection mandate. Instead, the district court improperly substituted its own judgment about the propriety of MDS in place of Mr. Sanchez's allegations, then denied him the opportunity to cure defects the

district court found in his pleading. In so doing, the district court committed reversible error warranting this Court's correction.

On the merits, the district court contravened controlling Fourth Amendment principles by refusing to hold that MDS effectuates a search of Mr. Sanchez's movement and location information. Mr. Sanchez's allegations explain how sensitive location and movement information collected by MDS can reveal extraordinarily private information about his activities, habits, and life. Recent Supreme Court precedent establishes that the collection of GPS data of this sort invades reasonable expectations of privacy.

The district court also erred in applying the Fourth Amendment's third-party doctrine to MDS. As courts have made clear, the involuntary transmission to third parties of location data necessary for the proper functioning of a modern service does not automatically waive an individual's privacy interest.

The district court alternatively, and erroneously, ruled that LADOT's regulatory interests justify its micromobility surveillance dragnet. In so holding, the court ignored Mr. Sanchez's allegations that LADOT lacked a reasonable and specific justification for collecting granular location information of all micromobility riders. The district court also ignored LADOT's statement that the agency designed MDS to "experiment" with data collection, as opposed to addressing specific regulatory needs. At best what LADOT *actually* plans on doing

with this data is a mixed question of fact, foreclosing dismissal on the pleadings.

Finally, the district court misconstrued CalECPA's civil remedy when it held that Mr. Sanchez could not bring a Penal Code section 1546.4(c) civil claim because the district court had not "issued" a warrant for the collection of his electronic communications information. But the only reason that no such "issuing court" exists is precisely because LADOT violated CalECPA's requirements to secure a court order. The text and legislative intent of the statute confirms that a violation of CalECPA of this sort cannot immunize LADOT from civil liability.

STANDARD OF REVIEW

This Court reviews "de novo a district court's order granting a motion to dismiss under Rule 12(b)(6)." *Coal. to Defend Affirmative Action v. Brown*, 674 F.3d 1128, 1133 (9th Cir. 2012). "Dismissal without leave to amend is improper unless it is clear, upon de novo review, that the complaint could not be saved by any amendment." *Polich v. Burlington N., Inc.*, 942 F.2d 1467, 1472 (9th Cir. 1991). However, "[a] district court's failure to consider the relevant factors and articulate why dismissal should be with prejudice instead of without prejudice may constitute an abuse of discretion." *Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003).

ARGUMENT

I. THE DISTRICT COURT ERRED IN DISMISSING THE COMPLAINT WITHOUT LEAVE TO AMEND AND WITHOUT A HEARING.

Federal notice pleading rules require that district courts liberally grant leave to amend pleadings that fail to state claims for relief. The district court's peremptory dismissal of Mr. Sanchez's initial complaint with prejudice and without a hearing constituted an abuse of discretion that alone justifies reversal and remand of the decision below.

A. The district court erred by ignoring plausible allegations about the invasiveness of MDS and the lack of justification for its precise data collection.

In deciding LADOT's motion to dismiss, the district court's task was "not to resolve any factual dispute," but to assume Mr. Sanchez's allegations as true and assess whether they stated claims for relief. *Dahlia v. Rodriguez*, 735 F.3d 1060, 1076 (9th Cir. 2013); *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010) ("We accept as true all well-pleaded allegations of material fact, and construe them in the light most favorable to the non-moving party"). The district court failed to do so in four critical respects.

First, the district court did not credit Mr. Sanchez's allegations regarding the sensitivity of the information collected by LADOT. In the Complaint, Mr. Sanchez alleged that MDS data is not functionally anonymous because the location

information could easily reveal his identity and other private information. *See* 3-ER-313–14 ¶ 31 (location datasets like MDS "cannot reasonably be considered 'anonymized' in any real sense when collected *en masse* and with the precision that MDS currently demands"). He alleged that the precision of the location information MDS ingests "makes it possible to identify individual riders anyway," that location datasets "are easily susceptible to identification," and that re-identification of his trips is therefore "likely." 3-ER-311–14 ¶¶ 26, 28, 32. Ignoring these assertions, the district court assumed that identification of MDS rides "would likely be an enormously resource- and/or time-intensive project." 1-ER-7 n.6. On this basis, the Court distinguished *Carpenter* and *Jones*, contrasting the "cheap and easy" GPS tracking discussed in those cases with what *it* claimed was the difficulty of using MDS to track Mr. Sanchez. *Id.* Yet his well-pled complaint alleged precisely the opposite.

At best, the question whether MDS data is susceptible to easy identification is one of fact, and potentially one requiring mathematical or technological expertise. *Cf. Siracusano v. Matrixx Initiatives, Inc.*, 585 F.3d 1167, 1179 (9th Cir. 2009), *aff'd*, 563 U.S. 27 (2011) ("statistical significance is a question of fact"); *see, e.g.*, *Garcia v. Country Wide Fin. Corp.*, No. 07-1161 VAP (JCRx), 2008 WL 7842104, at *6 (C.D. Cal. Jan. 17, 2008) (plaintiff "is not required at the pleading stage to produce statistical evidence proving a disparate impact"); *Turocy v. El*

Pollo Loco Holdings, Inc., No. 15-1343 DOC (KESx), 2017 WL 3328543, at *14 n.2 (C.D. Cal. Aug. 4, 2017) (statistical dispute concerning whether certain information was misleading in securities fraud action cannot be decided on motion to dismiss). The district court erred in substituting its own judgment in place of Mr. Sanchez's allegations.

Second, the district court also ignored Mr. Sanchez's plausible allegations concerning the revelatory nature of MDS's data collection scheme. He alleged, with scientific support, that location datasets like MDS can easily reveal not only an individual's identity and travel habits, but also "important information about the individual's residence, the identity of her employer, associates, or friends, the types of physicians she visits, or her favorite recreational activities." 3-ER-311 ¶ 26. When endpoints of trips are particularly sensitive—"like therapists' offices, marijuana dispensaries, or Planned Parenthood clinics—those routes may reveal *why* she made that trip." *Id.* The district court ignored these allegations, and the underlying research cited in support of these allegations, to conclude that MDS may reveal only "the places that Plaintiffs have traveled to on rental scooters in Los Angeles." 1-ER-9.

Third, the district court downplayed the importance of micromobility rides as an accessible form of transit to Mr. Sanchez (and other Los Angeles residents). The Court assumed not only that his rides could not be identified from MDS's

location dataset, but that he did not "use rental scooter services for transportation to the same degree as the Supreme Court imagined one uses a privately-owned car." 1-ER-7 n.5. This again contradicts Mr. Sanchez's allegation that his scooter rides can be easily identified, and indeed invents whole facts about Mr. Sanchez not present in the Complaint. Mr. Sanchez uses shared micromobility vehicles to take trips to where he lives, works, shops, and frequents. 3-ER-314 ¶ 32. It is precisely because he rides these vehicles as others may ride personal cars that makes his location and movement data so revealing.

Fourth, the court ignored Mr. Sanchez's allegations that LADOT lacks any reasonable interest in collecting GPS coordinates of every micromobility rider in the City. As explained in Part II.B below, rather than assuming as true his allegations that LADOT failed to provide to the City any reasonable and specific use case for collecting such precise location information, the district court relied upon its own wisdom for why MDS data collection is a reasonable exercise of LADOT's regulatory authority. Without any citation to the Complaint, any outside records, or even to LADOT's papers, the district court declared that "smart, effective regulation of a completely novel industry requires robust data." 1-ER-9. But Mr. Sanchez alleged precisely the opposite: that none of LADOT's potential use cases for invasive data collection "necessitated collecting all riders' granular and precise location information *en masse*," and that MDS collected data without

any justification and only to "experiment" with data analysis. 3-ER-314–16 ¶¶ 34–35, 38. He also explained how coarser data collection may satisfy regulatory interests without needing precise locations. *See, e.g.*, 3-ER-315 ¶ 37 (tracking *all* rides and *all* vehicles not required to monitor geographic distribution of vehicles). Rather than crediting these allegations, much less allowing for any discovery on the reasonableness of MDS and LADOT's regulatory scheme, the district court ignored them altogether and summarily dismissed Mr. Sanchez's well-pled allegations of unreasonableness. This it was not entitled to do.

B. The district court exacerbated its errors by dismissing the Complaint without allowing amendment.

The district court's dismissal of Mr. Sanchez's Complaint with prejudice violates this Court's instruction that pleadings be treated liberally, and parties be given leave to amend "freely" and "when justice so requires." *AmerisourceBergen Corp. v. Dialysist W., Inc.*, 465 F.3d 946, 951 (9th Cir. 2006). "Dismissal with prejudice and without leave to amend is not appropriate unless it is clear on de novo review that the complaint could not be saved by amendment." *Eminence Cap., LLC*, 316 F.3d at 1052.

Here, the district court failed to explain why Mr. Sanchez could not amend his Complaint to overcome the supposed deficiencies the court laid out in its order granting with prejudice LADOT's motion to dismiss. *Foman v. Davis*, 371 U.S. 178, 182 (1962) (while granting leave to amend is ordinarily left to the discretion

of a district court, recognizing that "outright refusal to grant the leave without any justifying reason appearing for the denial is not an exercise of discretion"); *Eminence Cap., LLC*, 316 F.3d at 1052 ("A district court's failure to consider the relevant factors and articulate why dismissal should be with prejudice instead of without prejudice may constitute an abuse of discretion"). Although a district court enjoys "particularly broad" discretion to deny leave to amend where "the plaintiff has previously been granted leave to amend," Mr. Sanchez had no such opportunity. *See Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009). And the district court did not explain why it believed he should not have that opportunity.

Far from a harmless error, opportunity to amend would have allowed Mr. Sanchez to further address the district court's assumptions, including that: (1) identification of MDS data requires a lot of time or resources; (2) the precision of MDS data collection is unlikely to allow for the easy identification of many, if not all, of his trips; (3) the only information revealed by MDS data is where he travels on his micromobility devices; (4) LADOT has proffered operationally specific use cases for MDS data; and (5) LADOT requires maximally precise location data of the type envisioned by MDS to meaningfully regulate shared micromobility vehicles, to name a few. The district court's failure to allow Mr. Sanchez the opportunity to amend his initial complaint constitutes reversible error independent

of the court's substantive legal errors.

II. MR. SANCHEZ ALLEGED FACTS SUFFICIENT TO SHOW LADOT VIOLATED HIS RIGHTS.

A. LADOT's location collection scheme constitutes a search under the Fourth Amendment.[10]

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). The district court's dismissal order misapplied this basic principle to hold that LADOT's mass location data collection program is not a search, and that, alternatively, any such search is presumptively reasonable as a matter of law.

1. Collecting precise locations and movements of a vehicle on public roads violates reasonable expectations of privacy.

Traditionally, the visual monitoring of a person or vehicle's location and movements in public raised no Fourth Amendment concern. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) ("a person travelling in an automobile on public

[10] The relevant search and seizure rules set by the Fourth Amendment and Article I, Section 13, of the California Constitution are functionally coterminous. *Sanchez v. County of San Diego,* 464 F.3d 916, 928–29 (9th Cir. 2006) ("[T]he right to be free from unreasonable searches under [Article I, Section 13] parallels the Fourth Amendment inquiry."). They are therefore addressed under the heading of the Fourth Amendment here.

thoroughfares has no reasonable expectation of privacy in his movements" because he has "voluntarily conveyed [that information] to anyone who wanted to look"). However, a plurality of the Supreme Court in *Jones* and a majority in *Carpenter* recognized that modern technology changes the calculation. Society has expected "that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement" of an individual, but practical constraints on such surveillance that may have existed in the past no longer exist today. *See Jones*, 565 U.S. at 430 (Alito, J., concurring); *id.* at 416, (Sotomayor, J., concurring) (GPS tracking "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility"; internal citations omitted).[11] To "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 138 S.Ct. at 2214 (*quoting Kyllo*, 533 U.S. at 34), the Constitution mandates restrictions on technologically-assisted location and movement surveillance of the type Mr. Sanchez challenges here. However, in holding that LADOT's tracking of micromobility vehicles does not constitute a search, the district court turned a blind eye to these recent Supreme Court cases

[11] Even in *Knotts*, the Supreme Court recognized that technologically-assisted "twenty-four hour surveillance" of public spaces could raise "different constitutional principles." *Knotts*, 460 U.S. at 283–84.

and ignored the fact that modern technology has upended historical reality.

The micromobility data collection regime challenged in this case raises many of the same privacy concerns as the GPS tracking at issue in *Jones* and the historical cell site location information at issue in *Carpenter.* As in *Jones*, LADOT mandates the disclosure of precise GPS coordinates for the starting and ending points of each ride in real time. And, as in *Carpenter*, the government has access to historical location data for every ride, "a category of information otherwise unknowable" without this technology. *Carpenter*, 138 S.Ct. at 2218.

In *Jones*, five Justices agreed that continuous real-time GPS monitoring of a vehicle violated the defendant's reasonable expectation of privacy and, on that ground, constituted a search under the Fourth Amendment. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring) (long-term collection of vehicle's GPS coordinates violates reasonable expectation of privacy). In reaching this conclusion, the concurring justices relied on three key characteristics of precise location data: the sensitivity of movement and location information; how inexpensive it is to collect; and the ease with which technology facilitates the collection of such data. Justice Sotomayor wrote that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 415 (Sotomayor, J., concurring). This type of movement and

vehicular location monitoring "chills associational and expressive freedom . . . by making available at relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track." *Id.* at 416.

Similarly, the Court held in *Carpenter* that the warrantless collection of historical cell site location information, or CSLI, violates an individual's reasonable expectation of privacy in their physical movements. *Carpenter*, 138 S.Ct. at 2217–19.[12] The Court explained that "[a]s with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). "And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 138 S.Ct. at 2217–18. Coupled with the ease of storing this data in perpetuity, the Court held that such cheap, easy, and invasive location collection invades reasonable expectations of privacy, even in public. As the *en banc* Fourth

[12] CSLI refers to the geographic segments created by the mesh of cellular radio antennas that provide cellular coverage in an area. *Carpenter*, 138 S.Ct. at 2211, 2219. When cellular phones connect to a network, the wireless carrier generates a time-stamped record of the location segment to which an individual cell phone connected. *Id.* These segments are much less precise than the GPS coordinates at issue here.

Circuit recently explained, "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns." *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 2021 WL 2584408, at *8 (4th Cir. June 24, 2021) (en banc) (*quoting Carpenter*, 138 S.Ct. at 2218). After *Carpenter*, it is clear that "[t]he latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." *Id.*

Carpenter and *Jones*, along with *Leaders of a Beautiful Struggle*, demonstrate how the district court here erred in concluding that LADOT's GPS collection program does not invade a reasonable expectation of privacy. As alleged in the Complaint, MDS works an even greater intrusion into settled privacy expectations than the forms of surveillance at issue in *Jones* and *Carpenter*, for three reasons.

First, the reasoning of the *Carpenter* and *Jones* decisions applies to MDS, since the Court discussed the harms of all forms of location and movement tracking, not merely CSLI collection or GPS tracking of privately-owned cars. *See, e.g.*, *Leaders of a Beautiful Struggle*, 2021 WL 2584408 at *12 (applying *Carpenter* to strike down a system of prolonged aerial surveillance using wide-angle cameras to track individuals' movements). Justice Alito in *Jones* expressed

concerns about the Fourth Amendment implications of not only persistent GPS tracking of vehicles but other forms of movement-based surveillance like cameras, toll roads, and on-board roadside assistance systems. *Jones*, 565 U.S. at 428. *Carpenter* similarly recognized that CSLI data enabled the government to learn information just as sensitive as what it could deduce from the GPS tracking in *Jones*, even though CSLI was less precise. *Carpenter*, 138 S.Ct. at 2216 ("like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortless compiled"); *id.* at 2217 (CSLI information, "[a]s with GPS information, . . . provides an intimate window into a person's life"); *id.* at 2217–18 ("like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient"); *Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *11 (explaining that "cell phone technology is ultimately incidental to the outcome in *Carpenter*," as "[i]t is precedents concerning privacy in 'physical location and movements' that control." (*quoting Carpenter*, 138 S.Ct. at 2215)). Here, MDS data—accurate to within as little as a few centimeters—is more precise than either the GPS data in *Jones* (15 to 30 meters) or the CSLI in *Carpenter* (50 meters).[13] It may therefore enable an even more invasive search. 3-ER-313 ¶ 30.

[13] For a discussion of the accuracy of GPS data, *see GPS Accuracy*, GPS.gov, http://www.gps.gov/systems/gps/performance/accuracy/ (last visited July 22, 2021).

Second, MDS allows LADOT to conduct invasive location tracking *en masse* and unsaddled by the limitations of physical GPS tracking in *Jones* or the targeting of particular cell phone towers in *Carpenter*. The placement of a physical GPS tracker required investigative time, resources, and targeting, while the collection of CSLI data required the government identify particular cell sites to target for investigation. MDS, on the other hand, contains no such practical limitations against population-wide intrusions on privacy. It only requires implementing some computer code and flicking a virtual switch to collect the locations of *every* rider, on *every* shared micromobility device, on *every* ride, on *every* street in the City, in a centralized database, forever. 3-ER-304–06 ¶¶ 3, 7, 3-ER-318 ¶ 46. This kind of dragnet would have been unimaginable to the Justices just ten years ago, let alone to the Founders centuries ago.

Recent circuit opinions bear out this distinction between a targeted, resource-intensive search, and a technologically-assisted dragnet. In *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020), this Court applied the Supreme Court's surveillance jurisprudence to another mass data collection scheme: the National Security Agency's bulk collection of telephone metadata. That program required telecommunications providers turn over details of all phone calls made within the United States, excluding the content of the calls. *Id.* at 989. In analyzing whether that program constituted a search, this Court distinguished targeted surveillance of

one individual for a matter of days from the telephony metadata program's dragnet monitoring of "millions" of callers "on an ongoing, daily basis for years." *Id.* at 991. This Court recognized that long-term, non-targeted surveillance, "made possible by new technology, upends conventional expectations of privacy." *Id.* at 991–92. As with MDS's collection of *every* ride, the "extremely large number of people" impacted by the NSA's metadata collection program rendered that program constitutionally suspect. *Id.* at 992. Its bulk character, along with "the ability to aggregate and analyze" the data, makes any individual's own data "considerably more revealing." *Id.* Sister appellate courts have also concluded that the bulk collection of location information exacerbates the magnitude of the constitutional violation that might otherwise be permissible if conducted on a targeted, individualized basis. *See, e.g.*, *Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *8 (mass surveillance of movement yields information "greater than the sum of the individual trips"); *United States v. Marquez*, 605 F.3d 604, 610 (8th Cir. 2010) ("wholesale surveillance" of large numbers of people using GPS devices raises especially troubling Fourth Amendment concerns); *United States v. Garcia*, 474 F.3d 994, 998–99 (7th Cir. 2007) (discussing concerns raised by "wholesale surveillance" and "mass surveillance" using GPS trackers).

Third, the surveillance enabled by MDS combines the real-time GPS tracking of *Jones* with the historical collection of CSLI in *Carpenter*, making it

potentially more invasive than either. With MDS, LADOT creates a bird's eye, real-time view of all micromobility rides. 3-ER-304–11, ¶¶ 3, 7, 25. It also serves as a time machine, capable of retrospective analysis of every trip ever taken on these vehicles. *Cf. Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *8 (explaining that the "photographic, retrospective location tracking [through the aerial surveillance program] in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. . . is enough to yield a wealth of detail, greater than the sum of the individual trips"; internal quotation marks omitted). The dangers of this kind of collection are self-evident: with MDS, an unscrupulous government official "need not even know in advance whether they want to follow a particular individual" because every trip is available to them. *Carpenter*, 138 S.Ct. at 2218.

Both federal and state courts that have considered the relationship between real-time and historical data collection have concluded that both raise independent privacy risks that, when working together, compound the constitutional stakes. *See, e.g.*, *United States v. Diggs*, 385 F.Supp.3d 648, 652 (N.D. Ill. 2019) (noting that "'the retrospective quality of the data here' impinges even further on privacy concerns than did the live data in *Jones* because it 'gives police access to a category of information otherwise unknowable' by enabling the police to 'travel back in time to retrace [Diggs's] whereabouts, subject only to the[ir] retention

polic[i]es'") (quoting *Carpenter*, 138 S.Ct. at 2218); *United States v. Chavez*, No. 15-CR-00285-LHK, 2019 WL 1003357, at *11 (N.D. Cal. Mar. 1, 2019) (discussing real-time location tracking as opposed to historical data collection, noting "an individual has arguably an even greater expectation of privacy" in real-time CSLI); *Commonwealth v. Almonor*, 120 N.E.3d 1183, 1196–97 (Mass. 2019) (distinguishing a prior case involving historical location data from current case involving real-time location data); *Tracey v. State*, 152 So.3d 504, 518 (Fla. 2014) (explaining greater privacy risk associated with real-time collection).

2. MDS effectuates a search even without explicitly associating location data with any individual.

The district court erred in failing to credit Mr. Sanchez's well-pled allegation that MDS location data can be readily associated with a particular rider. 1-ER-6–7. Contrary to the district court's reasoning, the Fourth Amendment may constrain data collection even when the information seized by the government is not explicitly associated with a particular person. *Leaders of a Beautiful Struggle,* 2021 WL 2584408, at *1, 10–11 (despite individuals appearing as dots or blurs from data, a search requiring a warrant existed because government "can deduce an individual's identity from [aerial surveillance] data, other available information, and some deductive reasoning.").

On this point, the district court improperly exceeded the scope of Mr. Sanchez's pleadings to make several factual findings unsupported by the

allegations in the Complaint. The most problematic of these was the court's assumption that the location information LADOT collects "cannot even be connected to [a rider]." 1-ER-6. The lower court also assumed that LADOT could not identify all of Mr. Sanchez's trips. Not only did Mr. Sanchez repeatedly allege to the contrary (3-ER-314 ¶ 32), he also alleged that identifying riders' trips could be done "easily" (3-ER-311–12 ¶ 28, 314 ¶ 33), and that research has found that 95% of individuals in less revealing datasets could be identified (3-ER-312 ¶ 28 n.4). *See Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *10 & n.10 (crediting the same study).

The district court's factual assumption resulted in its making a grievous legal error: it concluded that Mr. Sanchez enjoys no expectation of privacy in de-identified location and movements because the government must possess *some additional information* to identify Mr. Sanchez in the MDS data set. This contravenes Supreme Court precedent, which rejects the proposition that "inference insulates a search." *Carpenter*, 138 S.Ct. at 2218 (quoting *Kyllo,* 533 U.S. at 36); *id.* at 37 n.4 (rejecting argument that because "the technologically enhanced emanations had to be the basis of inferences before anything inside the house could be known, the use of the emanations could not be a search").

In *Carpenter*, the government unsuccessfully argued that Carpenter did not have a reasonable expectation of privacy in his CSLI because the police could not

rely on the CSLI on its own to explicitly identify him. *See* Brief for Petitioner, at 24, *Carpenter*, 138 S.Ct. 2206 (No. 16-402), *available at* https://www.scotusblog.com/wp-content/uploads/2017/09/16-402-bs-US.pdf. The Supreme Court held to the contrary: the government effectuated a search when it collected the CSLI even if "the location records did not on their own suffice to place Carpenter at the crime scene." 138 S.Ct. at 2218 (internal quotation marks omitted). In fact, a search occurs even where the identity of an individual within the dataset is entirely unknown, so long as the seized data might eventually result in identification. *Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *9–11; *Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1104 (Mass. 2020) (anonymized licensed plates from automated reader could, "[w]ith enough cameras in enough locations, . . . invade a reasonable expectation of privacy and would constitute a search for constitutional purposes."). Therefore, because the "Government could, *in combination with other information*, deduce a detailed log" of Mr. Sanchez's movements, the data collection violates expectations of privacy. *Carpenter*, 138 S.Ct. at 2218 (emphasis added).

MDS works a search even though Mr. Sanchez alleges only some—but not all—of his trips are identifiable. 1-ER-7 (district court order proposing that MDS would be a search if it "identif[ied] and compile[d] *all* the trips that Plaintiffs took"). Simply because the government cannot extract *all* information about *all*

riders' movements, personal lives, and activities does not render the collection of *some* information about their sensitive movements, personal lives, and activities undeserving of Fourth Amendment scrutiny. *Leaders of a Beautiful Struggle*, 2021 WL 2584408, at *8 (concluding a search occurred even though "[w]e do not suggest that the AIR program allows perfect tracking of all individuals it captures across all the time it covers.").

3. The third-party doctrine does not insulate MDS from constitutional scrutiny.

By applying the Fourth Amendment's third-party doctrine to this case, contrary to *Carpenter* and this Court's decision *Moalin*, the district court also erred. The third-party doctrine traditionally provides that, in certain contexts, individuals lack an expectation of privacy in information they willingly and voluntarily provide to a third party. *Smith v. Maryland*, 442 U.S. 735 (1979) (government collection of telephone numbers dialed); *United States v. Miller*, 425 U.S. 435 (1976) (financial records provided to bank).

Carpenter marked a shift from that rule by explicitly declining to apply the third-party doctrine to location tracking because of the sensitivity of location information and the fact that cell phones necessarily (and thus involuntarily) reveal location information to their wireless carriers. 138 S.Ct. at 2219–20.[14] This Court

[14] Even the Justices in dissent recognized that the third-party doctrine does not apply to all data shared with third parties. *See Carpenter*, 138 S.Ct. at 2230

in turn recognized that "numerous commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities." *Moalin*, 973 F.3d at 992. "Advances in technology since 1979 have enabled the government to collect and analyze information about its citizens on an unprecedented scale." *Id.* at 990. The district court failed to recognize, as this Court did in *Moalin*, that "there are strong reasons to doubt" that the third-party doctrine applies to LADOT's program, which amasses "on an unprecedented scale . . . information whose collection was enabled by new technology." *Id.* at 990.

Here, Mr. Sanchez alleged that LADOT collects precise GPS coordinates of all his shared micromobility rides without his agreement. 3-ER-314 ¶ 32. He also alleged that the vehicles he rides necessarily transmit his GPS coordinates to their micromobility providers, since that transmission allows the operators to charge riders based on the length of the trip taken. 3-ER-308 ¶¶ 17–18. LADOT exploits

---

(Kennedy, J., dissenting) (case law permitting warrantless access to records "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."); *id*. at 2262 (Gorsuch, J., dissenting) ("Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." (citing *Smith*, 442 U.S. 735 and *Miller*, 425 U.S. 435)).

this transmission, and demands that all micromobility providers turn over, in real-time, these precise coordinates. In this way, "[a]pplying the third-party doctrine to the GPS data here would require essentially the same extension of the doctrine that the Court rejected in *Carpenter*." *Diggs*, 385 F.Supp.3d at 653. The district court therefore failed to show the "special solicitude for location information in the third-party context" that the Supreme Court demands. *Carpenter*, 138 S.Ct. at 2219.

In addition, the district court also erroneously concluded as a matter of law that "[r]iding a one-time rental scooter is not indispensable to modern life." 1-ER-8. The indispensability of a mode of transport bears no relationship to whether the collection of location data is "knowing" or "voluntary." For one, the question of how communities use shared dockless vehicles is one of fact (*i.e.*, how reliant is Mr. Sanchez *himself* on this particular form of transit, as opposed to ones that the government does not surveil as closely) that cannot be properly assessed on the pleadings.[15] In any event, the district court's own conclusions about the necessity

[15] Recent research on the topic shows that people use micromobility as a replacement for traditional forms of transport, not merely for recreation. *See, e.g.*, Rebecca L. Sanders, et al., *To scoot or not to scoot: Findings from a recent survey about the benefits and barriers of using E-scooters for riders and non-riders*, 139 TRANSPORTATION RESEARCH PART A: POLICY AND PRACTICE 217 (Sep. 2020), https://www.sciencedirect.com/science/article/pii/S0965856420306522 (surveying shared scooters and finding that they "fill an important transportation niche and may contribute to transportation equity, and that efforts to address barriers could

of certain modes of transit would force individuals to eschew technology altogether to enjoy a surveillance-free mode of transit. The Constitution imposes no such mandates on free people.

The district court also justified the application of the third-party doctrine because it made the unwarranted factual assumption that location tracking in micromobility, unlike in mobile phones, is necessary by design. 1-ER-8. This is wrong both on the facts and on the law. Mobile phones require collection of location information, a fact the Supreme Court acknowledged while still rejecting the application of the third-party doctrine. *Carpenter*, 138 S.Ct. at 2220 (noting "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of a user beyond powering up"). And just like CSLI, there is "no way to avoid leaving behind a trail of location data" while using micromobility vehicles. *Id.* The district court's logic would not only force riders off shared micromobility devices to avoid constant governmental surveillance, but also off *any other form of transit* subject to similar state data collection programs. Under

---

further enhance that contribution," and that 72% of all trips were for transportation purposes like traveling to and from work, school, errands, and socializing/associating with others); *2018 E-Scooter Findings Report*, PORTLAND BUREAU OF TRANSPORTATION (PBOT), https://www.portlandoregon.gov/transportation/article/709719 (finding that 71% of survey respondents used the micromobility devices for transportation as opposed to recreation or exercise).

the district court's reasoning, were LADOT to mandate the collection of GPS data from all rental cars, neither the federal nor state constitutions would have anything to say because individuals could, theoretically, abandon renting cars altogether. The federal and state constitutions are supposed to protect against the government's unreasonable searches and seizures, not to give that same government free reign to limit how people can live their lives free from its gaze.

Further, if there is a question at all whether the third-party doctrine applies here, the district court's order dismissing the case with prejudice precludes even minimal discovery to allow Mr. Sanchez to collect evidence to show otherwise. Nowhere in his pleading does Mr. Sanchez allege that shared dockless vehicles require that their operators store his location and ride information in perpetuity. It may well be that micromobility companies do not store (or need to store) granular location data of the type LADOT requires them to disclose via MDS. Retaining such information forever may therefore be LADOT's policy choice, forced upon Mr. Sanchez and the operators by fiat. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) ("[T]he [Fourth] Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government."); *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527 (7th Cir. 2018) (A "choice to share data imposed by fiat is no choice at all."). Without the benefit of a complete record, the district court was not in a position to make the

factual assumptions it relied upon to apply the third-party doctrine.

4. The rental character of shared micromobility does not lessen Mr. Sanchez's privacy interests.

The district court erred by assuming that riders enjoy a lesser right to privacy in rental vehicles than in vehicles they own. 1-ER-7 n.5. The Supreme Court expressly rejected this narrow—and classist—conception of the Fourth Amendment:

> The Court sees 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 by someone other than the person in current possession of it, much as it did not seem to matter whether the friend of the defendant in *Jones* owned or leased the apartment he permitted the defendant to use in his absence.

Byrd v. United States, 138 S.Ct. 1518, 1528 (2018); *see United States v. Thomas*, 447 F.3d 1191, 1199 (9th Cir. 2006) ("an unauthorized driver who received permission to use a rental car and has joint authority over the car may challenge the search to the same extent as the authorized renter"). The linchpin to the Fourth Amendment's reasonable expectation of privacy inquiry is not ownership over that which is searched, but possession. *Rakas v. Illinois*, 439 U.S. 128, 161 (1978) ("We have concluded on numerous occasions that the entitlement to an expectation of privacy does not hinge on ownership.").

Further, the privacy policies and terms of service applicable to Mr.

Sanchez's rental of micromobility vehicles do not limit his Fourth Amendment rights against unlawful government searches. *See* 1-ER-7 n.7. Privacy policies and terms of service do not make enforceable contracts without a proper consent mechanism, and cannot waive Fourth Amendment rights. For one, they are rarely read or understood by consumers. *United States v. Nosal*, 676 F.3d 854, 861 (9th Cir. 2012) (*en banc*) ("Our access to . . . remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands"). Even if a privacy policy or a term of service can be considered an enforceable contract between the service provider and the user, such agreements cannot serve as basis for waiving constitutional protections. *Byrd*, 138 S.Ct. at 1529 (drivers maintain a reasonable expectation of privacy in a rental car even if they violate the rental agreement, because the agreement concerns risk allocation among private parties); *see also Thomas*, 447 F.3d at 1198 (similar). Allowing private notices or contracts to waive Fourth Amendment rights would "make a crazy quilt of the Fourth Amendment" in a fashion the Supreme Court cautioned against. *Smith*, 442 U.S. at 745.

B. The district court erred in holding that LADOT's collection of real-time and historical GPS locations of micromobility riders was reasonable.

Compounding its failure to appreciate the intrusive nature of MDS's collection of Mr. Sanchez's precise GPS coordinates, the district court alternatively

held that the collection was reasonable and necessary to regulate dockless vehicles. In reaching this conclusion, the court again made numerous unwarranted factual assumptions and failed to credit Mr. Sanchez's allegations that LADOT lacked any legitimate public interest for deploying MDS.

1. Mr. Sanchez alleged that LADOT failed to advance a compelling interest that supports the invasive collection of his sensitive location information.

An administrative search scheme "is only valid if the search serves a narrow but compelling administrative objective, and the intrusion is as limited as is consistent with satisfaction of the administrative need that justifies it." *United States v. Bulacan*, 156 F.3d 963, 968 (9th Cir. 1998) (cleaned up). Whether LADOT's warrantless collection of precise GPS data is reasonable rests on a balancing of: (1) "the nature of the privacy interest allegedly compromised" by the search; (2) "the character of the intrusion imposed" by the government; and (3) "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 v. Earls*, 536 U.S. 822, 830–34 (2002). Notably, these factors involve factual questions that the district court refused to credit in Mr. Sanchez's favor.

On one side of the ledger, Mr. Sanchez alleged that MDS works a deeply invasive search of his private movement and location information. He alleged that MDS allows the government to "easily" reveal sensitive information him—

including where he lives, works, and travels, and with whom and how he associates with others. 3-ER-314 ¶ 32. The district court simply ignored these allegations, finding that "the nature and character of the privacy intrusion would be, at the absolute most, knowledge of the places that Plaintiffs have traveled to on rental scooters." 1-ER-9. Mr. Sanchez also pled that MDS is a highly invasive search into his protected movements and locations. *See* Part II.A, *supra*. The district court downplayed this privacy intrusion by engaging in its own fact-finding. Instead of crediting his allegations that all his rides could be identified (3-ER-314 ¶ 32), that identifying riders' trips could be done "easily" (3-ER-311–14 ¶¶ 28, 33), and that this type of mass re-identification has proven successful (3-ER-311–12 ¶ 28 n.4), the district court stated that "it would be difficult to actually effectuate" the intrusion Mr. Sanchez complains of. 1-ER-9. The district court also concluded that Mr. Sanchez voluntarily and knowingly provided his GPS coordinates, *id.*, despite the allegation that he did not agree to share his location data with LADOT. 3-ER-314 ¶ 32.

On the other side of the ledger, the district court discounted Mr. Sanchez's allegation that LADOT lacked any reasonable government purpose in collecting his ride data. LADOT ignored City Council requests to offer a specific, legitimate regulatory interest to support MDS's sweeping data collection program. 3-ER-314–16 ¶¶ 33, 36–39. Instead, it publicly stated that its purpose in advancing MDS

was "to experiment" with data collection, not to resolve any pressing or legitimate transportation planning need. 3-ER-314–15 ¶ 35. The allegations regarding the government's failure to articulate an interest are questions of fact that must be credited at the motion to dismiss stage. *Ker v. State of Cal.*, 374 U.S. 23, 33 (1963) ("Each case is to be decided on its own facts and circumstances."). Yet the district court rejected these allegations by characterizing them not as factual assertions, but as legal argument. *See* 1-ER-9 ("Plaintiffs *argue* that the City fails to articulate why its regulatory interests necessitate collecting such precise route data"; emphasis added"). Instead of assuming their truth, the district court substituted its own judgment in place of well-pled allegations. *See, e.g.*, *id.* ("And smart, effective regulation of a completely novel industry requires robust data.").

The district court also improperly presumed facts outside of the Complaint in announcing that "understanding where scooters tend to transit and park," and "knowing what streets they typically take, at what hours, and at what destinations" is necessary "for municipal authorities attempting to regulate the public right-of-way." 1-ER-9–10. This assumption is neither found in the Complaint nor in LADOT's motion papers. Whatever its ultimate truth, there can be no doubt that this assumption must be tested by discovery into the motivations, purposes, and practices of LADOT in creating and implementing MDS. What the record reveals will ultimately determine whether LADOT's scheme is "limited and no more

intrusive than necessary to protect against the danger to be avoided." *McMorris v. Alioto*, 567 F.2d 897, 899 (9th Cir. 1978); *Bulacan*, 156 F.3d at 968 (an administrative search is "only valid if the search serves a narrow but compelling administrative objective, and the intrusion is as limited as is consistent with satisfaction of the administrative need that justifies it.").

Finally, the sheer scale of the data collection here cuts sharply against any claims that LADOT's program is "reasonable." That MDS indiscriminately collects location information about all riders and rides in perpetuity dramatically intensifies its privacy harms and raises the burden on LADOT to demonstrate regulatory necessity for such information. *Airbnb, Inc. v. City of New York*, 373 F.Supp.3d 467, 490 (S.D.N.Y. 2019) (characterizing "the scale of the [data] production" required by a municipal ordinance targeting all short-term housing providers in New York City as "breathtaking" and weighing against a finding of reasonableness).

2. The Fourth Amendment also requires LADOT provide some pre-collection process to gather geolocation data.

Deepening its errors, the district court refused to require that individual riders be afforded some process to review or challenge LADOT's data collection program. *See City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015). The Fourth Amendment's reasonableness analysis accounts not only for the scope of a search or seizure, but also the "manner of [its] execution." *United States v. Grey*, 959 F.3d

1166, 1182 (9th Cir. 2020). It was the manner of the collection—and the process afforded to the subjects of that collection—that animated the Supreme Court's striking down of a municipal requirement that hotels maintain detailed logs about each guest, including the individual's name, their times of arrival and departure, and rates charged. *Patel*, 576 U.S. at 412–13. "The Court has held that absent consent, exigent circumstances, or 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." *Id.* at 420.

Here, the district court erred by failing to apply *Patel* to MDS, concluding instead that *Patel* applies only to "individual, targeted search[es]" that are not "programmatic and uniform in application." 1-ER-10 n.8. *Patel*, however, is not so limited. It involved a neutral, programmatic, and uniform data collection scheme that subjected hotel owners "to mandatory record inspections under the ordinance without consent or a warrant." 576 U.S. at 413–14. *Patel* draws no distinction between "individual, targeted" searches or "programmatic" searches, as the district court did. *Airbnb, Inc.*, 373 F. Supp. 3d at 491–93 (same, in applying *Patel*). LADOT does not target users or micromobility operators by discretion; it employs software code to gather information about *every* user, on *every* ride, at *every* location, by *every* provider. It cannot be the case that *less* process is owed to Mr. Sanchez because LADOT chooses to collect *more* information, as the district court

suggested. 1-ER-10 n.8.[16]

III. CALECPA ENTITLES MR. SANCHEZ TO PETITION FOR RELIEF WHEN HIS INFORMATION IS UNLAWFULLY COLLECTED BY THE GOVERNMENT.

The district court granted LADOT's motion to dismiss Mr. Sanchez's CalECPA claim based on a cursory and mistaken interpretation of the statute, relying on arguments that LADOT did not make, and without allowing Mr. Sanchez to be heard. In dismissing Mr. Sanchez's CalECPA claim, the district court disregarded the core purpose of CalECPA—the unambiguous requirement that the government *get a warrant* or other legal process—and risked putting in place a regime in which victims of violations of the statute would be left without a remedy. The court also failed to recognize that, properly construed, CalECPA provides Mr. Sanchez a petition remedy in Los Angeles Superior Court. Through supplemental jurisdiction, that remedy also exists in the district court. This Court should correct those errors and direct that the district court allow Mr. Sanchez's CalECPA claims to proceed.

[16] Mr. Sanchez does not demand at this stage that LADOT provide him (or the micromobility providers) any particular form of process. *Patel*, 576 U.S. at 421 (Fourth Amendment requires "only . . . an opportunity to have a neutral decisionmaker review" a search). Whatever review may ultimately be required, the LADOT fails to provide any.

A. CalECPA provides strong, clear digital privacy rules for government, companies, and the public.

California has a long tradition of providing more robust privacy protections than federal law. *See, e.g.*, Cal. Const., art. I, § 1. CalECPA continues that tradition. Before CalECPA, both federal and state law only offered weak safeguards for modern electronic communication information, notwithstanding the rapid spread of new information and communication technologies.[17]

CalECPA prohibits the government from compelling access to electronic communications and location information without a warrant or other legal process. CalECPA governs "electronic communication," which it defines as "the transfer of signs, signals, . . . , data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system," Cal. Penal Code § 1456(c), and "electronic communication information," which it defines as including "the location of the sender or recipients" of electronic communications, Cal. Penal Code § 1546(d). GPS location data collected by MDS is therefore covered by CalECPA and subject to its restrictions.

[17] A core goal of CalECPA was to update the statutory framework for electronic privacy to take modern technology into account. As this Court observed in *Konop v. Hawaiian Airlines* 302 F.3d 868, 874 (9th Cir. 2002), because the Stored Communications Act "was written prior to the advent of the Internet and the World Wide Web . . . the . . . statutory framework is ill-suited to address modern forms of communication," and hence courts "have struggled to analyze problems involving modern technology within the confines of this statutory framework."

Specifically, CalECPA begins by forbidding: (1) compelling the production of electronic communication information from a service provider, Cal. Penal Code § 1546.1(a)(1); (2) compelling the production of electronic device information from anyone other than the authorized possessor of the device, *id.* at § 1546.1(a)(2); or (3) accessing electronic device information by means of physical interaction or electronic communication with the device, *id.* at § 1546.1(a)(3). The statute then carves out exceptions, permitting them only when the proper procedures—laid out in Penal Code sections 1546.1(b)–(k)—are followed.

These strict mandates of legal process, accompanied by judicial review, are CalECPA's hallmark feature. CalECPA's legislative history makes this abundantly clear: *every* committee analysis highlighted—in the first sentence of the bill summary, no less—the requirement that the government get a warrant or other comparable process before compelling production of electronic communications and location information.[18]

[18] *See* SB 178 (Leno) Committee Analysis, Senate Committee on Public Safety, March 23, 2015, p. 1 ("The purpose of this bill is to require a search warrant or wiretap order for access to all aspects of electronic communications . . . ."); SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations, April 27, 2015, p. 1 ("SB 178 would create the Electronic Communications Privacy Act, which would require a search warrant or wiretap order for access to all aspects of electronic communications . . . ."); SB 178 (Leno) Committee Analysis, Senate Committee on Appropriations, May 28, 2015, p. 1 ("SB 178 would create the Electronic Communications Privacy Act, which would require a search warrant or wiretap order for access to all aspects of

CalECPA also provides for robust and clear enforcement in court, by both individuals affected by unlawful collection of information and the Attorney General. CalECPA specifies three avenues of enforcement. First, any individual may move to suppress information collected in violation of the statute. Cal. Penal Code § 1546.4(a). That remedy is powerful but limited to when the unlawfully collected information is offered as evidence in a trial, hearing, or proceeding.

Second, the Attorney General has broad authority to "commence a civil action to compel any government entity to comply" with CalECPA. Cal. Penal Code § 1546.4(b). The Attorney General's authority to bring suit to enforce CalECPA is the most expansive of the three remedies. However, even though CalECPA has been in effect for over five years, the Attorney General has yet to bring a single enforcement action.

---

electronic communications . . . ."); SB 178 (Leno) Committee Analysis, Senate Rules Committee, June 2, 2015, p. 1 ("This bill requires a search warrant or wiretap order . . ."); SB 178 (Leno) Committee Analysis, Assembly Committee on Privacy and Consumer Protection, June 19, 2015, p. 1 ("Creates the California Electronic Communications Privacy Act (CalECPA), which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider."); SB 178 (Leno) Committee Analysis, Assembly Committee on Public Safety, July 13, 2015, p. 1 ("[This bill] prohibits government entities from compelling the production of, or access to, electronic communication information or electronic device information without a search warrant or wiretap order . . . ."). Full committee analyses available at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178.

The third and final remedy under CalECPA provides that an "individual whose information is targeted by a warrant, order, or other legal process . . . may petition the issuing court" to void or modify the process or order the unlawfully collected information to be destroyed. Cal. Pen. Code § 1546.4(c). This remedy is the only available means for people whose information is swept up in an unlawful government collection to protect themselves from further privacy intrusions.

B. CalECPA must be construed according to the Legislature's intent.

Questions of California's statutory construction are reviewed de novo. *John v. Superior Court*, 63 Cal.4th 91, 95 (2016). This Court's primary task in interpreting a state statute is to determine the California Legislature's intent, giving effect to the law's purpose, considering first the words of a statute as the most reliable indicator of legislative intent. *Id.* at 95–96 (citing *Tuolumne Jobs & Small Business Alliance v. Superior Court*, 59 Cal.4th 1029, 1037 (2014)). The language of the statute should be construed in context and harmonized to avoid absurd results. *Id.* at 96. When statutory language is ambiguous or subject to more than one interpretation, the Court may look to extrinsic aids, including legislative history or purpose. *Id.*

If a statute's "literal interpretation would result in absurd consequences the Legislature did not intend," courts should turn to extrinsic aids such as "the statute's purpose, legislative history, and public policy" to determine a term's

proper meaning. *See Coal. of Concerned Communities, Inc. v. City of L.A.*, 34 Cal.4th 733, 737 (2004); *Simpson Strong-Tie Co. v. Gore*, 49 Cal.4th 12, 27 (2010) ("…our fundamental task is to determine the Legislature's intent so as to effectuate the law's purpose. … we may reject a literal construction that is contrary to the legislative intent apparent in the statute or that would lead to absurd results"). In sum, courts should not resort to an overly rigid "dictionary school of jurisprudence" when construing a statute. *People v. Clayburg*, 211 Cal.App.4th 86, 91 (2012).

As this Court interprets CalECPA, two additional rules of construction apply. First, all provisions of the California Penal Code, including CalECPA, "are to be construed according to the fair import of their terms, with a view to effect its objects and to promote justice." Cal. Penal Code § 4. And second, as a remedial statute CalECPA "must be liberally construed to effectuate the object and purpose of the statute and to suppress the mischief at which it is directed." *Clayburg*, 211 Cal.App.4th at 91.

C. The district court's elimination of a remedy for large-scale CalECPA violations is contrary to its text and the Legislature's intent.

The district court gave two reasons for granting LADOT's motion to dismiss Mr. Sanchez's CalECPA claim. First, that under CalECPA, the phrase "issuing court" limits relief to challenging the violation of law "before the same court *in the*

same proceeding." 1-ER-11 (emphasis in original). And second, that Section 1546.4(c) deprives Mr. Sanchez of a remedy here because the district court in this case was not the "issuing court." 1-ER-10–11. The district court was mistaken on both counts and should be reversed.

1. The phrase "issuing court" refers to courts with the authority to issue legal process under CalECPA.

In Section 1546.4(c), CalECPA provides the following remedy for individuals whose information is unlawfully targeted by the government:

> An individual whose information is targeted . . . may petition the issuing court to . . . order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.

Cal. Penal Code § 1546.4(c). The question on appeal is whether to interpret the phrase "issuing court" as the district court did—to foreclose relief to individuals when a court has not (or has not yet) actually issued the legally required process that CalECPA mandates.

CalECPA does not include a definition of "issuing court."[19] Under standard rules of construction, the term refers not to a court that *has in fact issued* legal process (as the district court found), but rather to a court that *has the authority to*

[19] *See* Cal. Penal Code Section 1546 (definitions).

issue the required legal process. Interpreting "issuing court" as the district court did severely limits the ability of individuals to remedy large-scale and willful violations, and cuts against the Legislature's intent.

The two possible interpretations of the phrase "issuing court" have familiar analogues in non-legal English when verbs ending in "-ing" modify nouns. The phrase "running child," for example, describes, in the present tense, a child that is running. A "swimming pool," by contrast, refers not to a pool that is swimming, but to a pool that is *used for* swimming.[20] In the same way, an "issuing court" must be interpreted as a court "with authority to issue" a warrant, not a court "currently in the process of issuing" a warrant. The latter reading makes little sense in the context of Section 1546.4(c), which describes a petition remedy available to an individual (when the government complies with the process mandate) after the issuance has already concluded.[21]

This reading is consistent with other statutes and regulations under federal

---

[20] In this example, "running" functions as a "participial" adjective, specifying a participial (here, a present participial) verb functioning as an adjective, as opposed to a "descriptive" adjective which identifies a characteristic or purpose of the modified noun. *See* BRYAN A. GARNER, THE CHICAGO GUIDE TO GRAMMAR, USAGE, AND PUNCTUATION 405 (2016).

[21] When the government follows the most basic instruction of CalECPA and secures a warrant or other process, the court that in fact issues the warrant and the court with authority to issue the warrant will be one and the same. It is only because LADOT has not made any effort to comply with CalECPA that the two senses of "issuing court" make any practical difference.

law that define "issuing" entities as entities with the *authority* to issue. Under 18 U.S.C. § 1028, for example, which addresses fraud and counterfeiting of identification documents, an "issuing authority" is defined as a governmental entity that is *authorized* to issue identification documents or other anti-counterfeiting measures. 18 U.S.C. § 1028(d)(6). Federal law does not define "issuing authority" as the entity that *has in fact issued* a particular means of identification. *See also* 21 C.F.R. § 830.3 (under FDA regulations, "issuing agency" is an organization *accredited* to issue unique device identifiers, not the agency that in fact issued a particular unique device identifier).

The district court therefore incorrectly interpreted "issuing" to limit relief to cases where a court had *in fact* issued the required legal process. This cramped interpretation is inconsistent with the purpose of CalECPA, contravenes the requirement that remedial statutes be construed liberally, and would undermine the cause of justice that guides the interpretation of the Penal Code. *See* Cal. Pen. Code § 4.

2. Through supplemental jurisdiction, the district court below can be considered the "issuing court" for purposes of enforcing CalECPA.

Properly understood, CalECPA's reference to "issuing court" therefore includes, depending on specific facts and circumstances of the process sought, the state Superior Court for the county where the government entity is located. And

since federal courts have supplemental jurisdiction to hear state law claims that are part of the same case or controversy, *see* 28 U.S.C. § 1367(a), Mr. Sanchez's CalECPA claim may proceed in the district court below. Neither LADOT nor the district court ever called into question the validity of exercising supplemental jurisdiction over his state law claims. This claim—which could have been brought in Los Angeles Superior Court—is therefore properly within the district court's supplemental jurisdiction, and the district court was therefore the presumptive "issuing court" for the purposes of providing relief to him.

3. The district court's interpretation deprives the public of a remedy for the most egregious violations of CalECPA.

In this case, Mr. Sanchez challenges LADOT's compelled production of electronic communication and device information from micromobility providers in the City of Los Angeles. In order to comply with CalECPA, LADOT must acquire one of the legal processes listed in Section 1546.1(b): a warrant, a wiretap order, an electronic reader records order, a subpoena, or an order for a pen register or trap and trace device. *See* Cal. Pen. Code § 1546.1(b)(1)–(5). LADOT obtained none of these.

Simply disregarding the statute's requirements, as Mr. Sanchez alleges LADOT has done here, is an egregious violation of CalECPA. And it would result in no court having "issued" the required process, because LADOT never sought it. The district court's interpretation would therefore eliminate all judicial oversight

for any similar, large-scale violations of the law, contrary to the law's purposes.

The district court's holding also creates a loophole that other government entities can readily exploit. Agencies can compel production in ways other than seeking a warrant (as LADOT does) to deprive targeted individuals of the remedy CalECPA provided to them. This Court should avoid creating a perverse incentive that encourages the government to circumvent judicial review, especially when CalECPA's reason for existence is to impose it.

Instead, CalECPA relies on *courts* to serve as gatekeepers and enforcers of government legal process that reaches people's most private information. That judicial review of warrants, orders, and subpoenas is not hortatory or aspirational; it is mandatory under California law, and it is the precise mechanism through which the government can legitimately obtain extraordinary access to people's information. As CalECPA's author wrote, "[l]aw enforcement is increasingly taking advantage of outdated privacy laws to turn mobile phones into tracking devices and to access emails, digital documents, and text messages without proper judicial oversight." Bill Analysis, Assembly Committee on Public Safety 12, SB 178 (July 14, 2015) (quoting CalECPA's author, Senator Mark Leno).

Furthermore, CalECPA's protections against government access to electronic device information—which apply even when the government is not *compelling* production of information—would be left without remedies under the

district court's interpretation. Section 1546.1(a)(3) prohibits a government entity from accessing electronic device information by means of physical interaction or electronic communication with a device, unless the entity complies with Section 1546.1(c). The limits on device access protect, for example, students whose mobile devices might be accessed by public-school officials or the police without their full, specific consent. They also protect people whose mobile-phone location information could be captured by a cell-site simulator without their knowledge.[22] In both instances, the remedy for the affected individuals, who may have no connection to the underlying government purpose of collecting the information, is to file a Section 1546.4(c) petition to modify the relevant process or to delete their information. Without that relief, they will be left hoping (likely to no avail) that the Attorney General might intervene. The ability for people to remedy the government's access of their electronic data without the required process is a cornerstone of CalECPA's enforcement regime that the district court's holding would read out of the statute.

[22] *See, e.g.,* Ali Winston, *Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out*, THE NEW YORK TIMES, Jan. 15, 2019, https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html; Fruzsina Eördögh, *Evidence of "stingray" phone surveillance by police mounts in Chicago*, CHRISTIAN SCIENCE MONITOR, Dec. 22, 2014, https://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago.

D. The district court's attempt to distinguish 1546.4(b) from 1546.4(c) ignores robust "petition" rights under California law.

Finally, the district court erred in relying on the difference in language between the Attorney General's "civil action" remedy in Section 1546.4(b) and the private "petition" remedy in 1546.4(c). *See* 1-ER-11. The distinction between the two is meaningful, but it does not justify eliminating private remedies for egregious violations by the government, as the district court did.

Under California law, rights to "petition" a court often offer discrete and individualized remedies that may be filed as a separate civil action in pursuit of the provided relief. For example, persons included in state gang databases may petition the court to have themselves removed, *Lona v. City of Fullerton Police Dep't*, 268 Cal.Rptr.3d 248, 251 (Ct. App. 2020) (unpublished) ("To address legitimate concerns that the shared gang databases are sometimes inaccurate or overinclusive, the Legislature enacted sections 186.34 and 186.35, which allows persons to seek removal from such databases if they are no longer active gang members, affiliates, or associates."), or petition a court for injunctive relief to restrain conduct that violates California's auctioneering laws, *see Holyfield v. Julien Entertainment.com, Inc.*, No. CV 12-9388 CAS FFMX, 2012 WL 5878380, at *3 (C.D. Cal. Nov. 21, 2012) (granting a temporary restraining order based in part on violations of California auctioneering laws).

The difference in language used in CalECPA Sections 1546.4(b) and

1546.4(c) is no basis for denying relief to Mr. Sanchez. Quite the contrary, the establishment of petition rights under CalECPA indicates that the Legislature intended that affected individuals seek relief in actions like this one.

CONCLUSION

For the foregoing reasons, Appellant Justin Sanchez requests that this Court reverse the district court's grant of LADOT's Motion to Dismiss with prejudice, and remand for further proceedings.

Dated: July 23, 2021

Respectfully submitted,

/s/ Mohammad Tajsar
Mohammad Tajsar

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
Telephone: (415) 463-9333
Email: jlynch@eff.org
hzhao@eff.org

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

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 12,128 **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** July 23, 2021

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

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