

No. 21-55285

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

JUSTIN SANCHEZ,
Plaintiff and Appellant,

v.

LOS ANGELES DEPARTMENT OF TRANSPORTATION, et al.,
Defendants and Appellees.

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

ANSWERING BRIEF

MICHAEL N. FEUER, City Attorney (SBN 111529)
KATHLEEN A. KENEALY, Chief Deputy City Attorney (SBN 212289)
SCOTT MARCUS, Chief Assistant City Attorney (SBN 184980)
BLITHE S. BOCK, Managing Assistant City Attorney (SBN 163567)
JONATHAN H. EISENMAN, Deputy City Attorney (SBN 279291)
JEFFREY L. GOSS, Deputy City Attorney (SBN 178597)
200 North Spring Street, City Hall 14th Floor
Los Angeles, California 90012
(213) 978-2212 | Jonathan.Eisenman@lacity.org

Attorneys for Defendants and Appellees

**LOS ANGELES DEPARTMENT OF TRANSPORTATION
and the CITY OF LOS ANGELES**

TABLE OF CONTENTS

TABLE OF CONTENTS	2
TABLE OF AUTHORITIES	4
INTRODUCTION.....	10
JURISDICTIONAL STATEMENT	14
ISSUES ON APPEAL	15
STATEMENT OF THE CASE	16
SUMMARY OF ARGUMENT	21
ARGUMENT	23
I. The district court properly dismissed Sanchez’s constitutional claims.....	23
A. Review of the dismissal of Sanchez’s constitutional claims is de novo.....	23
B. There can be no Fourth Amendment search unless the Department violated Sanchez’s reasonable expectation of privacy.....	24
C. Sanchez has no reasonable expectation of privacy in the whereabouts of a third party’s device on public rights-of- way.....	25
1. Sanchez doesn’t have a reasonable expectation of privacy in the results of a hypothetical analysis of location data if he lacks a reasonable expectation of privacy in the data itself.....	25
2. In any event, Sanchez lacks Article III standing to sue over an allegedly privacy-invading analysis that has never taken place.....	32

3.	Nor does Sanchez have a reasonable expectation of privacy in the underlying location data itself.	34
D.	Even if Sanchez had an expectation of privacy in the location data generated while he rides a scooter, by willingly providing that data to the device’s owner, he cannot reasonably expect it to remain private.	40
E.	And even if the collection of a third party’s data about the location of its device amounts to a search of Sanchez, the search is a reasonable one.	53
II.	The district court properly dismissed Sanchez’s California Electronic Communications Privacy Act claim.	60
A.	Review of the dismissal of Sanchez’s CalECPA claim is also de novo.	60
B.	Remedies under CalECPA are prescribed by the statute, and a private right of action against a government entity is not one of the enumerated remedies.	60
III.	No amendment can revive Sanchez’s claims. The district court correctly dismissed them with prejudice.	65
	CONCLUSION	68
	CERTIFICATE OF COMPLIANCE	69
	ADDENDUM (Los Angeles Ordinance 186,955).....	70

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Airbnb, Inc. v. City of N.Y.</i> , 373 F. Supp. 3d 467 (S.D.N.Y. 2019).....	46
<i>Azam v. D.C. Taxicab Comm’n</i> , 46 F. Supp. 3d 38 (D.D.C. 2014)	22, 36
<i>Bassett v. ABM Parking Servs.</i> , 883 F.3d 776 (9th Cir. 2018).....	24, 36, 37
<i>Bd. of Educ. v. Earls</i> , 536 U.S. 822 (2002).....	22, 53, 58
<i>Bond v. United States</i> , 529 U.S. 334 (2000).....	24, 35
<i>Byrd v. United States</i> , 138 S. Ct. 1518 (2018).....	<i>passim</i>
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	<i>passim</i>
<i>City of L.A. v. Patel</i> , 576 U.S. 409 (2015).....	59
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	33
<i>First Fed. Sav. Bank v. Key Markets, Inc.</i> , 559 N.E.2d 600 (Ind. 1990).....	49
<i>Freeman v. DirecTV, Inc.</i> , 457 F.3d 1001 (9th Cir. 2006).....	60, 64

Gikas v. Zolin,
863 P.2d 745 (Cal. 1993)..... 65

Gould v. Bowyer,
11 F.3d 82 (7th Cir. 1993)..... 48

Herrera v. Zumiez, Inc.,
953 F.3d 1063 (9th Cir. 2020)..... 63

Katz v. United States,
389 U.S. 347 (1967)..... 52

Kilgore v. City of S. El Monte,
3 F.4th 1186 (9th Cir. 2021) 23

Kroessler v. CVS Health Corp.,
977 F.3d 803 (9th Cir. 2020)..... 65

Kyllo v. United States,
533 U.S. 27 (2001)..... 21, 29, 30, 31, 54

Laird v. Tatum,
408 U.S. 1 (1972)..... 33

Larkin v. Workers’ Comp. Appeals Bd.,
358 P.3d 552 (Cal. 2015)..... 63

Leaders of a Beautiful Struggle v. Baltimore Police Department,
2 F.4th 330 (4th Cir. 2021) (en banc) 39, 40

Lyall v. City of Los Angeles,
807 F.3d 1178 (9th Cir. 2015)..... 26

Meland v. Weber,
2 F.4th 838 (9th Cir. 2021) 60

Mich. Dep’t of State Police v. Sitz,
496 U.S. 444 (1990)..... 59

Miller v. Gammie,
335 F.3d 889 (9th Cir. 2003) (en banc)..... 58

Naperville Smart Meter Awareness v. City of Naperville,
 900 F.3d 521 (7th Cir. 2018)..... 54, 55, 56, 67

Nichols v. Brown,
 859 F. Supp. 2d 1118 (C.D. Cal. 2012) 20

Norcia v. Samsung Telecomms. Am., LLC,
 845 F.3d 1279 (9th Cir. 2017) 50

Patel v. City of Montclair,
 798 F.3d 895 (9th Cir. 2015)..... 36

Riley v. California,
 573 U.S. 373 (2014)..... 28, 38, 39, 44, 45

S.F. Herring Ass’n v. U.S. Dep’t of the Interior,
 946 F.3d 564 (9th Cir. 2019)..... 65

Smith v. Maryland,
 442 U.S. 735 (1979)..... 22, 41, 45, 46, 47

Sonner v. Premier Nutrition Corp.,
 971 F.3d 834 (9th Cir. 2020)..... 23

Spokeo, Inc. v. Robins,
 136 S. Ct. 1540 (2016)..... 32, 33

Summers v. Earth Island Inst.,
 555 U.S. 488 (2009)..... 32

United States v. Bulacan,
 156 F.3d 963 (9th Cir. 1998)..... 58

United States v. Cormier,
 220 F.3d 1103 (9th Cir. 2000)..... 36

United States v. Davis,
 482 F.2d 893 (9th Cir. 1973)..... 58, 59

United States v. Diggs,
 385 F. Supp. 3d 648 (N.D. Ill. 2019)..... 47, 48, 50

United States v. Jones,
565 U.S. 400 (2012)..... 24, 27

United States v. Karo,
468 U.S. 705 (1984)..... 21, 33

United States v. Knotts,
460 U.S. 276 (1983)..... 35

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010) 26

United States v. Miller,
425 U.S. 435 (1976)..... 41, 45

United States v. Moalin,
973 F.3d 977 (9th Cir. 2020)..... 34

United States v. Moffett,
84 F.3d 1291 (10th Cir. 1996)..... 36

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) (en banc)..... 50, 51

United States v. Perea,
986 F.2d 633 (2d Cir. 1993) 37

United States v. Ritchie,
342 F.3d 903 (9th Cir. 2003)..... 42

United States v. Tuggle,
4 F.4th 505 (7th Cir. 2021) 27, 36

United States v. Weaver,
No. 96-1068, 1996 U.S. App. LEXIS 25708 (2d Cir. 1996)..... 35

United States v. Wise,
877 F.3d 209 (5th Cir. 2017)..... 52

United States v. Yang,
958 F.3d 851 (9th Cir. 2020)..... 46, 50

United States v. Young,
573 F.3d 711 (9th Cir. 2009)..... 36

Statutes, Rules, and Ordinances

18 U.S.C. § 1028 63, 64
 18 U.S.C. § 1030 51
 18 U.S.C. § 2520 64
 28 U.S.C. § 1291 14
 28 U.S.C. § 1343 14
 28 U.S.C. § 1367 14
 42 U.S.C. § 1983 14, 20
 Fed. R. App. P. 4..... 14
 Fed. R. Civ. P. 12..... 60
 Cal. Penal Code § 1546.1..... 60
 Cal. Penal Code § 1546.4..... 61, 65
 L.A. Ord. 186,955 16

Other Authorities

On-Demand Mobility Rules and Guidelines
<https://ladot.lacity.org/sites/default/files/documents/on-demand-mobility-rules-and-guidelines-2021.pdf> 16, 57

Orin S. Kerr, *Implementing Carpenter*
 (USC Law Legal Studies Paper No. 18-29, 2018),
<http://ssrn.com/abstract=3301257> 38

Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*,
111 Mich. L. Rev. 311, 331–32 (2012) 26, 27

Ryan Fonseca, *When People Rage Against The Scooter Machines, This
LA Instagram Shares The Destruction*, LAist (Jun. 13, 2019),
<https://laist.com/news/bird-graveyard-scooter-instagram-q-and-a....> 39

INTRODUCTION

It is hard to imagine that anyone who lived in a city over the last few years missed the proliferation of electric scooters and bicycles on its streets and sidewalks. The companies that own those dockless mobility devices leave them in public places. People who want to use them locate and rent them with a smartphone app, get on, and ride away. When they reach their destinations, the users hop off, leave the devices wherever they stopped—there’s no “dock” for them—and then end their trips with the same smartphone app. Riders are charged for the distance that they travel between unlocking and locking the devices.

This business model presents at least two problems. First, as experience demonstrates, it overwhelms public places and infrastructure with scooters and bicycles. (This is probably true for several reasons, but it’s enough to say that a company can achieve an advantage over its competitors by ensuring that more of its devices are available to potential riders.) Second, the companies that own the devices need to know where they’re located for billing purposes. Or to maintain them. Or to recover them from places that they shouldn’t be.

One way to overcome both of these problems is for companies to put tracking devices on their scooters and bicycles—so they know where the devices are—and then to make the data that they collect available to municipalities—so the municipalities know, and can limit, things like how many devices are in a given place at a time.

The question in this appeal is whether that kind of regulatory framework violates the privacy rights of every person who borrows and rides one of the devices.

Justin Sanchez sued the City of Los Angeles and the Los Angeles Department of Transportation, alleging that by requiring dockless mobility providers to tell the Department where their devices are, the Department is collecting data that could then be analyzed to determine who is riding those devices—and why. Sanchez, who uses the devices regularly, claimed the Department's requirement thereby violated his privacy rights under (1) the Fourth Amendment to the United States Constitution; (2) article I, section 13 of the California Constitution; and (3) California's Electronic Communications Privacy Act, Cal. Penal Code §§ 1546–1546.4.

The district court properly dismissed Sanchez’s claims without leave to amend, for several reasons.

It doesn’t matter that the Department could determine who was riding a scooter (for example) by analyzing the location data that it collects *about the scooter* from the company that owns it. A rider has no reasonable expectation of privacy in a business’s data about where its scooter is located, and the process of analyzing that data—assuming that someone does analyze it—is not a search as a matter of law. (Indeed, with no allegation that anyone has crunched the data even to identify Sanchez, let alone to track him, it’s unclear that he has suffered any injury at all over which to sue the City or Department.)

But assume for argument’s sake that the location of third parties’ devices is information in which their riders have some kind of privacy interest. The riders relinquish that interest to the devices’ owners both as a matter of contract and a matter of practicality. Unlike, e.g., cell phones, the devices aren’t always tethered to a person and tracked incidentally while providing other services. People might be surprised to learn that a phone—a tool meant, quaint as it seems, to make phone calls—is constantly keeping track of their whereabouts. It blinks

reality to say that someone who rents a dockless mobility device would be surprised to learn that the device generates location data and transmits it to the company that owns the device. That is both inherent in the devices' use and obvious to riders who themselves must access the devices' location data, via the third-party device owners' smartphone apps, to find and unlock a device to ride.

Bereft of an expectation of privacy in the device location data, riders like Sanchez can't claim to have been searched when the Department collects it. Even if the Department's collection of location data *did* amount to a search, though, it's a search that is reasonable as a matter of law. The example cited by the district court to support this proposition is a good one: The Seventh Circuit held that a program by which a municipal electric utility attached "smart" meters to houses, allowing it to monitor residents' electricity use with enough precision to know what people were doing in their own homes, was a search for constitutional purposes. It was a constitutionally reasonable search, though, given the municipality's protection of the collected data and the non-law-enforcement use to which it was being put. If a program that requires people to accept the placement of monitoring devices on their

own homes—or else to give up electricity—amounts to a reasonable search, then it’s hard to see how a program that tracks the whereabouts of rental devices strewn all over public rights-of-way is an unreasonable search. (If it’s a search at all.)

Lastly, there’s Sanchez’s California Electronic Communications Privacy Act claim. That statute contains an exclusive list of remedies, and the list does not include a private right of action against the City.

There is no amending around any of these problems. This Court should affirm the district court’s judgment of dismissal.

JURISDICTIONAL STATEMENT

Sanchez alleged a violation of the Fourth Amendment under 42 U.S.C. § 1983. (3-ER-14–15.) The district court had subject-matter jurisdiction pursuant to 28 U.S.C. § 1343(a). Sanchez also alleged violations of California state law (3-ER-15–17), which the district court had subject-matter jurisdiction to hear under 28 U.S.C. § 1367(a). The district court dismissed Sanchez’s complaint, with prejudice, on February 23, 2021. (1-ER-13.) Sanchez appealed (3-ER-327–33) on March 24. Fed. R. App. P. 4(a)(1)(A). This Court has subject-matter jurisdiction over the appeal pursuant to 28 U.S.C. § 1291.

ISSUES ON APPEAL

1. If a person lacks a reasonable expectation of privacy in data about a dockless mobility device, can he claim a Fourth Amendment violation on the assumption that analyzing the data would allow the government to deduce private facts about him?

2. Assuming that an analysis of device data would allow the government to deduce private facts about the device's rider, has the rider suffered an injury-in-fact without even an allegation that the analysis has been performed?

3. Does someone who rents a dockless mobility device have a reasonable expectation of privacy in the device's whereabouts?

4. If someone who rents a dockless mobility device could have a reasonable expectation of privacy in its whereabouts, would the third-party doctrine forfeit that expectation?

5. If collecting data from dockless mobility devices constitutes a Fourth Amendment search, is the search reasonable when the data is used for transportation planning and management purposes?

6. Does the California Electronic Communications Privacy Act create a private right of action against a government entity?

STATEMENT OF THE CASE

The relevant facts are straightforward: Faced with “a near-overnight invasion of motorized electric scooters,” that “cluttered city sidewalks, lacked safety features, and interfered with disabled access to city streets,” the City of Los Angeles took measures to protect its residents and the public spaces it holds in their trust. (2-ER-117, 3-ER-310.) Rather than banning the mobility devices outright, the City opted to regulate them to “ensure safe and equitable access, maintenance and operations.” (2-ER-117.) The City Council enacted the “Shared Mobility Pilot Program,” authorizing the Los Angeles Department of Transportation “to issue permits to an operator of shared mobility devices, and to enforce rules and regulations developed by the Department regarding the use of the devices on City public rights-of-way.” (2-ER-118.)¹

¹ The City Council has since replaced the pilot program with a permanent program. L.A. Ord. 186,955 (Apr. 6, 2021). The Department has also since updated its *On-Demand Mobility Rules and Guidelines*, <https://ladot.lacity.org/sites/default/files/documents/on-demand-mobility-rules-and-guidelines-2021.pdf>.

Part of regulating the use of devices in the public right-of-way is knowing whether and where those devices are in the public right-of-way. The companies that own the devices already collect data about where the devices are located: The owners use “precise GPS coordinates” in order “to track rides and charge customers accordingly.” (3-ER-314.) The Department requires device owners to provide that data as a condition of receiving a permit to place the devices in the City.

When someone uses a device, the Department receives the device’s starting location and the time at which it departed that location, and the location and time at which the device is left for the next user. (3-ER-317.) After 24 hours, the Department receives the route that the device took between the beginning and end of a trip. (*Id.*) The data is transmitted to the Department through an open-source tool called the Mobility Data Specification, which is managed by the Open Mobility Foundation (3-ER-316)—a non-profit organization comprising municipalities around the world and various private entities (including Bird, the owner of a fleet of scooters).

All of this is information about the device itself; none of it is information about the person using the device. (3-ER-317.)

Still, Justin Sanchez—who uses dockless mobility devices and “intends to continue riding these dockless vehicles within Los Angeles in the future”—claimed that “a simple analysis” of data about the devices “will likely identify the precise trips” he has taken, and that he “never agreed to share” that data with the Department. (3-ER-313, 320.)²

Sanchez sued the City and the Department, alleging that collecting device location data from the companies operating those devices violates his “right to be free from unreasonable search and seizure as protected by the Fourth Amendment to the United States Constitution,” because collection of the “data is unreasonable, unconnected to any legitimate government interest, and occurs without any opportunity for administrative or judicial review pre-collection.” (3-ER-323.) Per Sanchez, the practice of receiving device data from the devices’ owners “unreasonably conditions” his own “ability to ride dockless mobility vehicles upon the disgorgement” of his “otherwise

² Eric Alejo, previously a plaintiff in this litigation, abandoned his appeal. (Doc. No. 19.) Since they were positioned identically in the district court, this brief continues to refer only to Sanchez rather than using a generic collective noun.

protected location information.” (*Id.*) Sanchez then duplicated that claim, substituting article I, section 13 of the California Constitution as the source of the allegedly infringed right. (3-ER-323–24.)

Finally, Sanchez alleged that the Department’s collection of device location data violates the California Electronic Communications Privacy Act (“CalECPA”), Cal. Penal Code §§ 1546–1546.4, because “a California government entity may only compel the production of electronic information through the execution of a probable-cause warrant or analogous order, or under a narrowly circumscribed set of exceptional circumstances.” (3-ER-325.)

For these alleged violations, Sanchez sought relief including an injunction ordering the City and Department “to destroy all precise location records associated with” his rides; to stop collecting, storing, and preserving that data; to prohibit the Department from requiring companies to provide that data as a requisite for having a permit to put their devices in Los Angeles; and for damages for violations of his constitutional rights. (3-ER-326.)

The City moved to dismiss.³

The district court granted the City’s motion, notwithstanding Sanchez’s opposition. (1-ER-5.) Accepting Sanchez’s agreement that the relevant analysis is the same under both the United States and California constitutions (2-ER-62 n.1), it found that the Department’s receipt of device location data doesn’t constitute a search under either charter. (1-ER-7–11.) The district court refused, however, to consider the devices’ user agreements—in which Sanchez *had* agreed to share location data with governments (*contra* 3-ER-320)—in reaching its conclusion. (1-ER-9 n.7.)

Alternately, the court found that if the Department is conducting a search, then it is a reasonable, administrative one. (1-ER-11–12.) Finally, reviewing the text of CalECPA, the district court found that the plain text of the law doesn’t afford Sanchez the opportunity to bring a civil claim against the City under the statute. (1-ER-12–13.) Finding

³ Municipal departments aren’t ordinarily proper defendants in § 1983 actions. *E.g.*, *Nichols v. Brown*, 859 F. Supp. 2d 1118, 1136–37 (C.D. Cal. 2012). Although for some reason Sanchez insists that the Department remain named as a defendant specifically (2-ER-85), this brief refers only to “the City” for ease of reference when describing actions taken in the litigation.

“that amendment to add more facts would be futile,” the court dismissed the action with prejudice. (1-ER-13.)

Sanchez timely appealed. (3-ER-327–33.)

SUMMARY OF ARGUMENT

Sanchez claims that because an analysis of location data from dockless mobility devices could reveal private facts about him, then the Department’s collection of that data constitutes a Fourth Amendment search. But if Sanchez lacks a reasonable expectation of privacy in data *about a device*, the fact that analyzing the data might yield information about him does not a Fourth Amendment violation make: “[A]n inference is not a search.” *Kyllo v. United States*, 533 U.S. 27, 37 n.4 (2001).

And even if one assumes that analyzing device data could constitute a Fourth Amendment violation if it revealed private facts about Sanchez, there is no allegation that anyone has ever done the analysis. Potential invasions of privacy are not Fourth Amendment searches. *United States v. Karo*, 468 U.S. 705, 712 (1984). Nor are they injuries sufficient to confer Article III standing. *Bassett v. ABM Parking Servs.*, 883 F.3d 776, 783 (9th Cir. 2018).

Putting aside the question of what an analysis of device location data might reveal, if the question is whether Sanchez has a reasonable expectation of privacy in the data itself, the answer is still “no.” The rider of an app-rented scooter has no more a reasonable expectation of privacy in where his ride begins and ends than does the passenger in a taxicab. Which is to say: none. *Azam v. D.C. Taxicab Comm’n*, 46 F. Supp. 3d 38, 50 (D.D.C. 2014).

Still further, if one assumes that Sanchez could have a reasonable expectation of privacy in the whereabouts of a dockless mobility device, then he would forfeit that expectation by sharing the location information voluntarily with the third party that owns the device. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

But assume for argument’s sake that the Department’s collection of device location data does amount to a Fourth Amendment search of the devices’ riders. “[B]alancing the nature of the intrusion on the individual’s privacy against the promotion of legitimate governmental interests,” *Bd. of Educ. v. Earls*, 536 U.S. 822, 829 (2002), the search is a reasonable one.

Finally, as to the California Electronic Communications Privacy Act: It straightforwardly lacks a private right of action. That much is evident from its plain text.

None of these issues can be corrected with the additional facts Sanchez proposes to plead. The district court correctly dismissed his complaint without leave to amend.

ARGUMENT

I. The district court properly dismissed Sanchez’s constitutional claims.

A. Review of the dismissal of Sanchez’s constitutional claims is de novo.

This Court reviews the dismissal of Sanchez’s Fourth Amendment claim—and his similar California Constitutional claim—de novo.

Kilgore v. City of S. El Monte, 3 F.4th 1186, 1189 (9th Cir. 2021). The Court must affirm the judgment dismissing the claims if it is correct on any ground supported by the record. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 839 (9th Cir. 2020).

B. There can be no Fourth Amendment search unless the Department violated Sanchez’s reasonable expectation of privacy.

The Fourth Amendment protects people against unreasonable searches. Before asking whether a search was reasonable, one must ask whether a search happened in the first place. A government official conducts a search if she does one of two things. The first is to commit a physical trespass—the official goes snooping around somewhere that she isn’t supposed to be, without permission. *United States v. Jones*, 565 U.S. 400, 404–07 (2012). The second is to invade someone’s reasonable expectation of privacy—the official intrudes on something a person expected to keep private, and the person’s expectation of privacy was an objectively reasonable one. *Bond v. United States*, 529 U.S. 334, 338–39 (2000). It is only the second form of Fourth Amendment violation—an invasion of Sanchez’s reasonable expectation of privacy—that is at issue here.⁴

⁴ The opening brief says that Sanchez’s claim under article I, section 13 of the California Constitution should be evaluated together with his Fourth Amendment claim; that the underlying rights are “functionally coterminous.” (AOB 25 n.10.) The City accedes to Sanchez’s waiver of any argument that the two claims ought to be evaluated differently.

C. Sanchez has no reasonable expectation of privacy in the whereabouts of a third party's device on public rights-of-way.

At first blush, nothing about the information the Department elicits from the companies that own and operate dockless mobility devices has anything to do with Sanchez or anyone else: “Where is that scooter and what route did it take to get there?” is a question about a third-party company's GPS-outfitted gizmo. Sanchez's complaint is that if the Department knows the answers to those two questions, it can do some data-crunching to guess if he was the one riding the device. And that, he claims, invades his privacy.

1. Sanchez doesn't have a reasonable expectation of privacy in the results of a hypothetical analysis of location data if he lacks a reasonable expectation of privacy in the data itself.

Sanchez pointed out one significant problem with this theory of the case in his own district court papers: The Fourth Amendment is implicated at the time that the Department collects information about a third party's mobility device if it is implicated at all. The Fourth Amendment isn't concerned with what the City or the Department could theoretically glean by analyzing that information later. (2-ER-68.) “The subsequent analysis and use of information has been

considered beyond the scope of Fourth Amendment protection.” Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 331–32 (2012). Consequently, if the information collected—the starting and ending points of every trip that a third party’s device takes—is not something *itself* in which Sanchez has a privacy interest, then collecting the information is not a search of Sanchez even if someone could later analyze the information to deduce facts about him. *See Lyall v. City of Los Angeles*, 807 F.3d 1178, 1186 (9th Cir. 2015) (a person cannot claim a Fourth Amendment violation just because he is unhappy about what a search of someone else reveals about him).

Now, Sanchez takes the opposite tack, suggesting that courts are willing to hold that it *is* a Fourth Amendment search to analyze information in which a person lacks a reasonable expectation of privacy, if the analysis allows the government to deduce sensitive facts about the person. This is an application of the so-called “mosaic theory” of the Fourth Amendment: A collection of innocuous facts is sometimes a mosaic that can reveal private things about a person, and assembling that mosaic amounts to performing a search. *E.g., United States v. Maynard*, 615 F.3d 544, 561–62 (D.C. Cir. 2010).

But “[d]espite garnering passing endorsement from some—if not most—of the justices . . . the [mosaic] theory has not received the Court’s full and affirmative adoption.” *United States v. Tuggle*, 4 F.4th 505, 519–20 (7th Cir. 2021). Instead, “many courts that have considered the theory have expressed disapproval, though not without exception,” and “the mainstream academic view has urged courts to reject the theory.” *Id.* at 520. Why? For starters, it is not clear when exactly it should apply; when deducing a fact from a collection of non-private data becomes a Fourth Amendment search rather than simply “good police work.” Kerr, *supra*, at 328.

Nevertheless, without using the term, Sanchez contends that *Carpenter v. United States*, 138 S. Ct. 2206 (2018) compels the application of the mosaic theory in this case. (AOB 35–36.)⁵

Carpenter’s facts are undoubtedly familiar to this Court. After *Carpenter*’s confederates identified him as an accomplice in a series of robberies, the FBI obtained a court order (but not a warrant) allowing it

⁵ It’s strange that the opening brief accuses the district court of “turn[ing] a blind eye” to *Carpenter* and its forebear, *Jones*. (AOB 26.) Approximately a third of the district court’s opinion is a discussion of *Carpenter* and *Jones*. (1-ER-8–10.)

to retrieve Carpenter’s cell phone location information from his cellular service provider. 138 S. Ct. at 2212. The data allowed the Government to place Carpenter “within a wedge-shaped sector ranging from one-eighth to four square miles” of four in a series of robberies. *Id.* at 2212–13, 2218. Carpenter challenged the Government’s collection of the data as an interference with his reasonable expectation of privacy, undertaken without a warrant and so in violation of the Fourth Amendment. *Id.* at 2212. This presented two questions: First, whether Carpenter had a reasonable expectation of privacy in the location data generated by his personal cell phone, *id.* at 2217–19, and second, whether he squandered that expectation by sharing the location data voluntarily with his cell service provider, *id.* at 2219–20.

Resolving the first question in Carpenter’s favor, the Court observed that “individuals have a reasonable expectation of privacy *in the whole* of their physical movements.” *Id.* at 2217 (italics added). Because cell phones are “almost a ‘feature of human anatomy,’” they track “nearly exactly the movements” of their owners. *Id.* at 2218 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). “A cell phone faithfully follows its owner beyond public thoroughfares and into

private residences, doctor’s offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves nearly perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” *Id.*

That much augurs the conclusion that cell phone location data is reasonably private. *Id.* at 2219. The Government and a dissenting justice protested this conclusion, arguing that the location data on its own wouldn’t be enough to put Carpenter precisely at any of the crime scenes. *Id.* at 2218. But once investigators interfere with someone’s reasonable expectation of privacy to gain a piece of evidence, it doesn’t matter for the Fourth Amendment’s sake that they must infer additional facts before the evidence yields a useful conclusion. The Fourth Amendment violation—the search—has already happened. Which is why the *Carpenter* majority noted that the Supreme Court had previously “rejected the proposition that ‘inference insulates a search.’” *Id.* (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

This sentence is the source for Sanchez’s invocation of the mosaic theory. He reads the Court’s rejection of the idea that “inference insulates a search” to mean that inference can *constitute* a search; that

if one can deduce Sanchez’s whereabouts from data in which he enjoys no reasonable expectation of privacy, then the process of deduction amounts to a search. That is why Sanchez spills so much ink explaining how easy it would be to perform the revealing analysis of the mobility device location data.

This reading of *Carpenter* is wrong. If there were any question about that, consider *Kyllo*—the source of *Carpenter*’s “inference insulates a search” quotation. In *Kyllo*, police officers used a thermal imaging device to see heat radiating from a house. 533 U.S. at 29–30. They inferred (correctly) that the heat was generated by lights used to grow marijuana. *Id.* at 30. The *Kyllo* Court held that the officers conducted a warrantless search, in violation of the Fourth Amendment, when they “use[d] a device that is not in general public use” to “explore details of the home that would previously have been unknowable without physical intrusion.” *Id.* at 40. The four dissenting justices argued that the police officers did no such thing; they merely measured “the heat emanating from a building,” and then inferred that it was created by grow lights. *Id.* at 43 (Stevens, J., dissenting).

To this, the *Kyllo* majority responded that “[t]he issue in this case is not the police’s allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house.” *Id.* at 37 n.4. If the use of the imaging device *in and of itself* constitutes a search of the house, it makes no difference to the Fourth Amendment that “the technologically enhanced emanations had to be the basis of inferences before anything inside the house could be known.” *Id.* The majority agreed with the dissent, however, “that an inference is not a search.” *Id.*

Here, too, an inference is not a search. Unlike the goings-on inside a house—per *Kyllo* and much other Fourth Amendment authority—or someone’s cell phone location data—per *Carpenter*, information of a “unique nature,” 138 S. Ct. at 2217—the location of a scooter *in and of itself* is not something in which a rider like Sanchez enjoys Fourth Amendment protection. Nothing private can possibly be revealed about him *until* someone analyzes the scooter’s location data. And because that analysis—that inference—is not a Fourth Amendment search, the district court was correct to dismiss Sanchez’s Fourth Amendment claim.

2. In any event, Sanchez lacks Article III standing to sue over an allegedly privacy-invading analysis that has never taken place.

But assume that Sanchez is correct that conducting an analysis of device data in which he lacks a privacy interest *could* violate the Fourth Amendment if the analysis allows someone to deduce private facts about him. There is still the problem that Sanchez cannot allege that someone did (or imminently will) analyze the device location data to that end. This means Sanchez’s plea for an opportunity to develop his case in the federal courts—really, to impose his privacy-policy preferences on the City by judicial fiat—gets it backwards. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (“the law of Article III standing serves to prevent the judicial process from being used to usurp the powers of the political branches,” cleaned up).

Because unless and until the City or Department does such an analysis, Sanchez cannot claim to have been injured by their invasion of his privacy: He lacks standing not only in the substantive “shorthand” particular to Fourth Amendment disputes, *Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018), but more importantly, he lacks standing for Article III’s jurisdictional purposes. *See Summers v. Earth Island Inst.*,

555 U.S. 488, 499 (2009) (courts have an independent obligation to assure themselves of a plaintiff's standing).

Demonstrating Article III standing requires Sanchez to show at least a “certainly impending” injury, *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) (italics omitted), that is “‘real,’ and not ‘abstract,’” *Spokeo*, 136 S. Ct. at 1548. The Supreme Court has “never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.” *United States v. Karo*, 468 U.S. 705, 712 (1984). That someone *might* perform an analysis of device location data, which *might* disclose Sanchez’s scooter-borne peregrinations, does not an injury-*in-fact* to Sanchez make. Regardless of how easy the analysis *might* be to perform. *See, e.g., Bassett v. ABM Parking Servs.*, 883 F.3d 776, 783 (9th Cir. 2018) (no injury-in-fact to a person’s privacy in the potential that someone will read credit card information printed openly and unlawfully on a receipt); *cf. Laird v. Tatum*, 408 U.S. 1, 9–15 (1972) (no First Amendment injury in the subjective chill allegedly caused by the bare existence of a surveillance program).

In the absence any actual injury—and one pauses here to wonder especially about Sanchez’s basis for seeking damages (3-ER-326)—the federal courts have no reason, let alone jurisdiction, to tackle a thorny constitutional question.⁶

3. Nor does Sanchez have a reasonable expectation of privacy in the underlying location data itself.

Sanchez may respond that he has already suffered an actual invasion of his privacy, because when he’s riding a scooter, he has the same “exclusive possessory interest” in it that he would in something like a rental car. (2-ER-64.) That interest, Sanchez claims, gives him a reasonable expectation of privacy in the scooter’s whereabouts— notwithstanding that it belongs to a third party—so that the act of collecting its location data is an intrusion directly on his privacy.

(AOB 42.)

⁶ So many of the Fourth Amendment cases cited in both Sanchez’s brief and this one involve criminal prosecutions because by the time someone is prosecuted, there’s usually little question that a search has occurred, and the person who is on trial has at least arguably been injured as a result of what the search turned up. In any event, a criminal *defendant* doesn’t have to show that he has suffered an Article III injury. *See United States v. Moalin*, 973 F.3d 977, 994 n.8 (9th Cir. 2020).

This argument is also unavailing. Having a possessory interest in a rented scooter might give Sanchez a reasonable expectation of privacy in the *contents* of something like a closed basket affixed to its handlebars. *Cf. Byrd*, 138 S. Ct. at 1528–29 (reasonable expectation of privacy in a rental car’s contents). But it doesn’t provide a reasonable expectation of privacy in the scooter’s *location* on public roads. *Cf. United States v. Knotts*, 460 U.S. 276, 281–82 (1983) (no reasonable expectation of privacy in a car’s movements “on public thoroughfares”).

The two expectations aren’t coextensive, which is why someone would retain a reasonable expectation of privacy in the contents of her van even after subjecting the world to a #VanLife barrage of photos of the van parked in all kinds of scenic places—a disclosure that would probably forfeit any reasonable expectation of privacy in the van’s whereabouts. Or why the stops at which someone gets on and off a bus aren’t facts in which that person has a reasonable expectation of privacy, even if the rider has a reasonable expectation of privacy in the contents of the luggage that he brings aboard the bus. *Bond*, 529 U.S. at 338–39; *see generally United States v. Weaver*, No. 96-1068, 1996 U.S. App. LEXIS 25708, *2 (2d Cir. 1996) (summary op.) (“A person

dismounting a bus in a public station has no reasonable expectation of privacy with respect to his conduct in public areas”); *cf. United States v. Moffett*, 84 F.3d 1291, 1293 (10th Cir. 1996) (a train passenger has no reasonable expectation of privacy in a passenger manifest that reveals he is on the train).

It’s also why a person ordinarily has an expectation of privacy in the contents of their hotel room, *United States v. Young*, 573 F.3d 711, 715–16 (9th Cir. 2009), even if they have no reasonable expectation of privacy in the fact that they’ve booked the hotel room, *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000), and likely no reasonable expectation of privacy in anyone’s comings or goings from the room, *see Patel v. City of Montclair*, 798 F.3d 895, 900 (9th Cir. 2015) (police do not conduct a search by entering areas of a motel open to the public); *cf. Tuggle*, 4 F.4th at 511 (police do not conduct a search by watching a suspect’s front door for 18 months with remote cameras mounted on public property).

And it’s why “neither taxicab drivers nor passengers have a reasonable expectation of privacy in the pick-up and drop-off data collected by the GPS tracking aspect” of taxicab meters, *Azam v. D.C.*

Taxicab Comm'n, 46 F. Supp. 3d 38, 50 (D.D.C. 2014), though either a passenger or driver may have some expectation of privacy in the cab's contents, see *United States v. Perea*, 986 F.2d 633, 639 (2d Cir. 1993) (passenger lacks reasonable expectation of privacy in the cab's trunk generally); *id.* at 642 (passenger has a reasonable expectation of privacy specifically in the contents of a closed duffel bag within the cab's trunk).

Given the relatively tight analogy between a taxicab for hire and a scooter for rent, the best Sanchez did to distinguish *Azam* in the district court was to claim that cab drivers have a diminished privacy interest in their workplaces. (2-ER-78.) That distinction doesn't speak at all to *Azam's* holding that passengers *also* lack a reasonable expectation of privacy in where they are picked up or dropped off. 46 F. Supp. 3d at 50. Further still: In addressing the taxicab analogy, Sanchez inadvertently conceded that there's nothing new or uniquely privacy-gutting about the kind of data collection to which he claims he's being subjected by the Department when he rides a scooter. As he said, "[t]he GPS requirement challenged in those cases does not appear to be any more invasive than the pre-digital requirement that cab drivers record start and location [*sic*] points." (2-ER-78.)

Sanchez gives away the game with this admission that the data at issue here is not of the same “unique nature” as the cell phone location data the Supreme Court considered in *Carpenter*, 138 S. Ct. at 2220. So even if one assumes (though the City does not agree) that *Carpenter* “signals a new kind of expectation of privacy test,” as with taxicabs, the “basic kind of record at issue—where a person was picked up, what path a person took, and where they were dropped off—is not new.” Orin S. Kerr, *Implementing Carpenter* 6, 48 (USC Law Legal Studies Paper No. 18-29, 2018), <http://ssrn.com/abstract=3301257>. And that kind of record is not subject to a rider’s reasonable expectation of privacy, before or after *Carpenter*. *Id.* at 48–49.

For whatever Sanchez alleges in his pleadings, it borders on silly to claim that a scooter rented for a short time and then dumped unceremoniously on a sidewalk is “such a pervasive and insistent part of daily life” that it is, like *Carpenter*’s cell phone, “indispensable to participation in modern society,” and so generating data that ought to be treated uniquely. *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 386). Sure, Sanchez can *contend* that like a cell phone, a scooter or bicycle is an “appendage[] of a person” (2-ER-65.) But he can’t mean

it seriously. Which is why Sanchez adds the caveat that he means it only “during the pendency of a ride.” (*Id.*) The whole reason that the Supreme Court treats cell phones differently, though, is that they aren’t subject to that caveat: “While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.” *Carpenter*, 138 S. Ct. at 2218. Unlike a cell phone, no one could mistake a scooter or bicycle—or a taxicab; the logic is the same—for “an important feature of human anatomy.” *Riley*, 573 U.S. at 385.⁷

Nor, contrary to Sanchez’s suggestion, has the Department’s collection of device location data created the kind of panopticon that the majority of a badly fractured Fourth Circuit feared in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc). Put aside the merits of the Fourth Circuit’s holding in that case that a series of photographic overflights violated the reasonable expectations of privacy of virtually everyone in

⁷ Few important anatomical features are treated like dockless mobility devices. Ryan Fonseca, *When People Rage Against The Scooter Machines, This LA Instagram Shares The Destruction*, LAist (Jun. 13, 2019), <https://laist.com/news/bird-graveyard-scooter-instagram-q-and-a>.

Baltimore by “track[ing] every movement’ of every person outside.” *Leaders of a Beautiful Struggle*, 2 F.4th at 341; *but see id.* at 360–62 (Wilkinson, J., dissenting) (challenging the majority’s predicate facts, and in light of precedent on aerial surveillance, its holding). Because whatever the merits of that holding, the Department hasn’t conducted any remotely similar form of surveillance here.

The Department has simply required third-party companies to provide data on the whereabouts of *their* scooters and bicycles in the City’s *public* rights-of-way, so that it may effectively maintain those rights-of-way. *Compare Carpenter*, 138 S. Ct. at 2218 (the “newfound tracking capacity” in cell phone location information “runs against everyone,” continuously surveilling “400 million devices in the United States”). Sanchez has no reasonable expectation of privacy in that location data. Collecting it is not a search of Sanchez.

D. Even if Sanchez had an expectation of privacy in the location data generated while he rides a scooter, by willingly providing that data to the device’s owner, he cannot reasonably expect it to remain private.

Assume for argument’s sake that Sanchez lives in a world where he had, at some point, a reasonable expectation of privacy in the location of a third party’s mobility device. Sanchez waived that

expectation of privacy by voluntarily sharing the location data with the third-party device owner. “[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979), “even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed,” *United States v. Miller*, 425 U.S. 435, 443 (1976). (In *Smith*, a phone number was deemed to have been voluntarily disclosed to the phone company when dialed, 442 U.S. at 744; in *Miller*, negotiable instruments were deemed to have been voluntarily disclosed to a bank when negotiated, 425 U.S. at 442.)⁸

The most obvious way that Sanchez voluntarily shared his location data with third parties was by entering into contracts with device owners explicitly to share the data with them. Those agreements even stipulate that the owners may subsequently turn the location data over to regulators or government entities. So Sanchez implored the

⁸ Rumors of the third-party doctrine’s demise (e.g., AOB 37 n.14) are premature. See *Carpenter*, 138 S. Ct. at 2220 (“We do not disturb the application of *Smith* and *Miller*”).

district court to ignore the contents of the user agreements in evaluating his pleadings. (2-ER-70.) If the district court committed any error in judgment, it was in acceding to Sanchez’s argument that his complaint “does not rely upon or reference these policies.” (*Id.*; 1-ER-9 n.7.) In fact, when Sanchez alleged that he “never agreed to share . . . precise location data” (3-ER-320), he put at issue exactly the terms to which he *did* agree. Having done that, Sanchez made those terms “part of the complaint.” *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).

Since Sanchez uses Lime devices (3-ER-313), consider the terms of the current Lime user agreement. Those terms can be found at <https://www.li.me/user-agreement>. The terms are lucid, and direct the user via hyperlink to an incorporated “Privacy Notice.” That Privacy Notice, at <https://www.li.me/privacy>, is even more straightforward. As of November 5, 2021, it provides in any one of 21 languages (including plain English) that “[w]e collect and process location data” and that “[d]ata such as the location of the vehicle, the routes taken by the moped, bike, scooter, or other vehicle and its rental status” are necessary to provide Lime’s services. Then, under the bold heading

“How We Use Information,” the policy informs the rider that “[w]e use your information, including information about your location . . . to comply with our legal obligations including to meet regulatory or local law requirements.”

But even without the straightforward terms of the devices’ user agreements and incorporated privacy policies, Sanchez cannot deny the obvious fact “that the vehicles he rides necessarily transmit his GPS coordinates”—really, the *vehicles*’ GPS coordinates—to their owners. (AOB 38.) Any rider understands that much when he uses a device owner’s app to find one of its devices to rent, and is then billed for his ride based on the device’s “precise GPS coordinates” as transmitted to its owner. (3-ER-314.) When that universally understood reality is combined with the devices’ privacy policies, the third-party doctrine applies as a matter of law to eliminate any reasonable expectation of privacy that Sanchez may ever have had in a device’s location data.

It’s hard to see how the contrary could be true; how the facts here add up to anything *except* a rider’s “voluntary exposure” of location data that is thereby subject to the third-party doctrine. *Carpenter*, 138 S. Ct. at 2220. The doctrine’s bite in this case is even clearer when one

contrasts the device data disclosed here with the kind of data that led the *Carpenter* majority to reject the third-party doctrine’s application to cell phone location information: “[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.” *Id.* Consequently, “[a]part from disconnecting the phone from the network”—and so rendering essentially useless an essential and omnipresent device, *Riley*, 573 U.S. at 395—“there is no way to avoid leaving behind a trail of location data.” *Carpenter*, 138 S. Ct. at 2220.

Thus, *Carpenter*’s “narrow” carve-out from the third-party doctrine exists *not* because a person is “using a phone,” and not even because cell phone location information discloses a “person’s movement at a particular time.” *Id.* It exists because the “unique nature” of cell phone location information amounts to no less than “a detailed chronicle of a person’s presence compiled every day, every moment, over several years”—and one that a person cannot meaningfully be said to have provided voluntarily. *Id.* at 2217, 2220; *see id.* at 2220 & n.4 (stating explicitly that the Court’s “decision today is a narrow one” that does “not express a view on matters not before us”).

By *Carpenter*'s lights, applying *Smith* and *Miller* to *that* kind of "detailed chronicle" would not be a "straightforward application" of the third-party doctrine; it would be "a significant extension of [the doctrine] to a distinct category of information." *Id.* at 2219. But does information from dockless mobility devices fall in a similarly distinct category? It beggars belief that "nearly three-quarters" of dockless mobility device users spend "most of the time" living "within five feet" of bicycles they've rented—as people do with their cell phones. *Riley*, 573 U.S. at 395. And no one is bringing her rented scooter routinely into the shower. *Id.* At least, no one should be. *See* p. 39 & n.7, *supra*.

The bottom line is that the third-party doctrine would gut any reasonable expectation of privacy Sanchez may ever have had in device location data, even after *Carpenter*. None of Sanchez's arguments to the contrary is convincing. For instance, Sanchez disputes whether an express agreement to share location data with a third party affects his reasonable expectation of privacy in that data. (AOB 43.) He is correct inasmuch as he contends that the terms of an agreement with a third party do not *always* control a person's expectation of privacy; sometimes

agreements just address things like “risk allocation between private parties.” *Byrd*, 138 S. Ct. at 1529.

That is not the same as saying, as the opening brief does, that the terms of an agreement can *never* control a person’s expectation of privacy. *E.g.*, *United States v. Yang*, 958 F.3d 851, 861–62 (9th Cir. 2020). Especially if the agreement purports expressly to govern the parties’ expectations of privacy. *See, e.g.*, *Airbnb, Inc. v. City of N.Y.*, 373 F. Supp. 3d 467, 485 (S.D.N.Y. 2019) (when businesses notify customers of their obligation “to disclose user data to regulators,” it bears on whether the customers “may claim a reasonable expectation of privacy as against the [businesses’] disclosure of such data”).

Sanchez resists even this straightforward point, contending that allowing contracts to control parties’ expectations of privacy “would ‘make a crazy quilt of the Fourth Amendment,’ in a fashion the Supreme Court cautioned against.” (AOB 43, quoting *Smith*, 442 U.S. at 745.) The Supreme Court “cautioned against” no such thing. The crazy-quilt quote from *Smith* responds to an argument that a criminal defendant’s expectation of privacy in a number he dialed should depend on (1) “[t]he fortuity of whether or not the phone company in fact elects

to make a quasi-permanent record of a particular number” instead of (2) whether the defendant voluntarily conveyed that information to the phone company by making the call in the first place. *Smith*, 442 U.S. at 745. The Court refused to countenance the first of those two options: It would make “a crazy quilt” of the Fourth Amendment, it held, to inquire about the infinitely variable business practices of third parties, rather than about the voluntariness of a principal party’s disclosure, in determining whether to apply the third-party doctrine to the information disclosed. *Id.*

That holding does suggest *something* about the value of contracts in deciding whether the third-party doctrine applies—but it’s the opposite of what Sanchez would like. The existence of a contract speaks to the voluntariness of an agreement between the parties. A contract could include an agreement to share information voluntarily (as in this case). Following *Smith*, then, an agreement to share information is *precisely* the kind of thing a court should consider in deciding whether the third-party doctrine applies.

Given his repeated reference to *United States v. Diggs*, 385 F. Supp. 3d 648 (N.D. Ill. 2019), Sanchez might ask how allowing an

agreement between parties to affect the third-party doctrine can be squared with the holding in that case. The district court there held that Diggs had a reasonable expectation of privacy in location data from his wife's car, which Diggs borrowed and allegedly used to rob a jewelry store. *Id.* at 649–50. The purchase contract for the car allowed its seller to use “an electronic tracking device . . . to find the vehicle.” *Id.* at 650. The seller used the device at the (warrantless) request of local detectives, revealing that the car was in the alley behind the jewelry store during the robbery. *Id.* The district court found that notwithstanding the terms of his wife's purchase contract, Diggs maintained a reasonable expectation of privacy in the car's location. *Id.* at 652–54. It excluded the location evidence as obtained in violation of the Fourth Amendment. *Id.* at 655.

There are a few ways to square the result in *Diggs* with the unremarkable proposition that an agreement to share information can bear, even decisively, on a person's reasonable expectation of privacy. One way is simply to ignore the holding in *Diggs*, which doesn't bind even the district court that issued it. *Gould v. Bowyer*, 11 F.3d 82, 84 (7th Cir. 1993).

Another is to observe—consistently with the law and the City’s position here—that while the terms of a contract can bear on a person’s reasonable expectation of privacy, they aren’t always dispositive of it. *Byrd*, 138 S. Ct. at 1529. That would be particularly true for Diggs, given that—unlike the data-sharing terms governing dockless mobility devices—the electronic-tracking term in the Indiana purchase contract for his wife’s car was almost certainly meant to be triggered only if his wife defaulted (RJN 8).⁹ See *First Fed. Sav. Bank v. Key Markets, Inc.*, 559 N.E.2d 600, 603–04 (Ind. 1990) (contracts should be interpreted according to the parties’ intent, harmonizing their provisions “as disclosed by the language used to express their rights and duties”); see generally *Byrd*, 138 S. Ct. at 1529 (it is the purpose of a rental agreement’s terms, and not simply the fact of the agreement, that governs the terms’ effect on a renter’s expectation of privacy).

For while it might defy an objectively reasonable expectation of privacy for a third party to track a car that someone else owns free and clear, it is not nearly as unreasonable for a creditor to maintain the

⁹ The City is filing a request for judicial notice concurrently with this brief.

ability to locate a car that it has a right to repossess in the event of default. *Cf. Yang*, 958 F.3d at 861–62 (a renter loses a reasonable expectation of privacy in car’s whereabouts once its owner is entitled by agreement to repossess it).

The worst way to treat *Diggs*, though, is the way that Sanchez would: As a broad declaration that a person can *never* forfeit an expectation of privacy, particularly in his location data, by agreement with a third party. *Carpenter*, which holds narrowly that cell phone location data isn’t given voluntarily to cellular service providers, 138 S. Ct. at 2220, certainly does not compel that result. *Contra Diggs*, 385 F. Supp. 3d at 653–54.

Sanchez’s doubts that privacy policies can serve as the predicate for invoking the third-party doctrine do not become any more convincing with either the addition of his claim that such policies “are rarely read or understood by consumers,” or his citation to this Court’s decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). (AOB 43.) As for the former, it’s the general rule that parties cannot escape the terms of contracts by failing to read them. *See, e.g., Norcia v. Samsung Telecomms. Am., LLC*, 845 F.3d 1279, 1284 (9th Cir.

2017) (applying California law). As for the latter, *Nosal* has nothing whatsoever to do with a person's reasonable expectation of privacy. It held that the rule of lenity counsels against applying the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, to criminalize "violations of a company or website's computer restrictions." 676 F.3d at 863.

Anyway, the privacy policies at issue here only amplify something that is readily apparent to anyone who rides one of the devices: The device doesn't function unless the rider is sharing location data with *at least* the third party that owns the device. To avoid sharing that data, a person may choose not to ride.

Which leads to Sanchez's normative argument. He contends that the third-party doctrine shouldn't vitiate someone's expectation of privacy in a dockless mobility device, because a rider ought to have the same expectation of privacy in the whereabouts of a rented scooter as he would in the whereabouts of his own car. According to Sanchez, allowing a person's reasonable expectation of privacy to depend on the mode of transportation he uses is "classist." (AOB 42.)

Whether or not such distinctions are classist, a descriptive account of Fourth Amendment law reveals that courts make them regularly

among different places and things. An easy example: A person has a reasonable expectation of privacy in his private car, but not in the cabin or luggage compartment of a public bus. *Compare Byrd*, 138 S. Ct. at 1527 with *United States v. Wise*, 877 F.3d 209, 218 (5th Cir. 2017). To call that distinction “classist” is to quarrel not with the district court’s judgment in this case (AOB 42), but with the Supreme Court’s Fourth Amendment reasonable-expectation-of-privacy jurisprudence from Justice Harlan’s seminal concurrence in *Katz v. United States*, 389 U.S. 347, 361 (1967) on out. Because privacy has always been something that people could buy. (Ask anyone who can afford not to have roommates.)

The modern innovation is that privacy has become something that people can sell: Information is currency with which people can pay for convenience or entertainment. People are generally free to forgo particular expedients or amusements when they do not want to expend that currency. To the extent Sanchez might ever have had a reasonable expectation of privacy in the whereabouts of a third party’s dockless mobility device—he did not, *see* § I.C.3, *supra*—the price of using that device is sharing its location data with the device’s owner. Having done

that, Sanchez cannot complain when the device's owner shares the data with the Department. He no longer has a reasonable expectation of privacy, and a concomitant Fourth Amendment claim, to assert.

E. And even if the collection of a third party's data about the location of its device amounts to a search of Sanchez, the search is a reasonable one.

Finally, consider what happens if Sanchez *does* have a reasonable expectation of privacy in the location of a third party's device: The result is that the Department conducts a Fourth Amendment search when it obtains the data, but there's still the question whether the search was reasonable. The answer depends on "balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests." *Bd. of Educ. v. Earls*, 536 U.S. 822, 829 (2002). "Therefore, in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Id.* (cleaned up).

The district court concluded, correctly, that the Department's collection of the location data from dockless mobility devices satisfies

those special-needs criteria. It did so by analogy to a case that Sanchez himself cites repeatedly: *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521 (7th Cir. 2018). Because it is a good analog, *Naperville*, and its relationship to the facts of this case, are worth discussing in depth.

The City of Naperville replaced its residential electric meters with “smart meters” that “collect residents’ energy-usage data at fifteen-minute intervals,” and then it “store[d] the data for up to three years.” *Id.* at 524. “[A] group of concerned citizens sued Naperville over the smart meter program,” alleging “that Naperville’s smart meters reveal intimate personal details,” like “when people are home and when the home is vacant, sleeping routines, eating routines, specific appliance types in the home and when used, and charging data for plug-in vehicles that can be used to identify travel routines and history.” *Id.* (cleaned up). The district court dismissed a Fourth Amendment claim premised on those allegations; the Seventh Circuit affirmed. *Id.* at 529.

First, the *Naperville* Court quoted *Kyllo* for the proposition that using “a device that is not in general public use, to explore details of the home that would have been previously have been unknowable without

physical intrusion,” amounts to a search. *Id.* at 526 (cleaned up). The data collected by the smart meters, the Court concluded, “even when collected at fifteen-minute intervals, reveals details about the home that would be otherwise unavailable to government officials without a physical search.” *Id.* at 527.

But then, having determined that the use of the smart meters constituted a search, the *Naperville* Court held that the search was a reasonable one. *Id.* at 528. While “[r]esidents certainly have a privacy interest in their energy-consumption data,” the way Naperville collected the data, “even if routine and frequent,” was “far less invasive than the prototypical Fourth Amendment search of a home” and, “[c]ritically,” it was conducted “with no prosecutorial intent” by “[e]mployees of the city’s public utility.” *Id.* at 528.

The Seventh Circuit then balanced the residents’ privacy interest “against the government’s interest in the data collection,” which it found was “substantial in this case.” *Id.* Smart meters “allow utilities to restore service more quickly when the power goes out;” they “also permit utilities to offer time-based pricing, an innovation which reduces strain on the grid by encouraging consumers to shift away from peak

demand periods,” and they “reduce utilities’ labor costs because home visits are needed less frequently.” *Id.* at 528–29. Those interests “render the city’s search reasonable, where the search is unrelated to law enforcement, is minimally invasive, and presents little risk of corollary criminal consequences.” *Id.* at 529. (It is worth observing that the Seventh Circuit cited only a journal article about smart metering to describe its benefits.)

The Department’s alleged search in this case is even less intrusive than *Naperville*’s. The Department isn’t using technology to look into the home. There is no allegation that its data collection is related to law enforcement, and there is no allegation that it presents *any* risk of corollary criminal consequences. Like *Naperville*’s “amended ‘Smart Customer Bill of Rights,’” *id.* at 528, the Department’s “Data Protection Principles” limit access to the data the Department collects, and state explicitly that “[l]aw enforcement and other government agencies, whether local, state, or federal *will not have access* to raw trip data other than as required by law, such as a court order, subpoena, or other legal process.” (2-ER-182, emphasis in original). “To be clear, the City will make no data available to law enforcement agencies through this

process that is not already available to them” directly from the devices’ owners. *Id.*

On the other side of the balance, the current “On-Demand Mobility Rules and Guidelines” show in detail why the Department is collecting device location data, including to make sure devices are not parked in places they are not allowed to be. *On-Demand Mobility Rules and Guidelines 2021 13–23*, <https://ladot.lacity.org/sites/default/files/documents/on-demand-mobility-rules-and-guidelines-2021.pdf>.

Sanchez’s complaint itself recognizes this is a substantial problem. (3-ER-310.)

What, then, is the issue? Sanchez’s chief argument—one that he does not articulate as thoroughly in the opening brief as he did in the district court—is that the Department collects more data than is necessary to satisfy “the administrative need that justifies” its collection of the data. (AOB 44, cleaned up; 2-ER-76–77.)¹⁰

¹⁰ Sanchez continues to claim that the Department “ignored City Council requests to offer a specific, legitimate regulatory interest” that would support its data collection. (AOB 45.) Yet he objected (2-ER-46–47) when the City provided the Department’s supposedly missing response to the City Council’s “requests.” (2-ER-170–80).

A court’s inquiry into the precision of an administrative search is not as demanding as Sanchez would like it to be, though. The Supreme Court “has repeatedly stated that reasonableness under the Fourth Amendment does *not* require employing the least intrusive means” in arranging an administrative search regime. *Earls*, 536 U.S. at 838 (italics added).

That quote from *Earls* seems inconsistent with Sanchez’s authority from this Court (AOB 44) that “an administrative screening search must be as limited in its intrusiveness as is consistent with satisfaction of the administrative need that justifies it.” *United States v. Bulacan*, 156 F.3d 963, 967 (9th Cir. 1998) (quoting *United States v. Davis*, 482 F.2d 893, 910 (9th Cir. 1973)). Suffice it to say, if the cases are inconsistent, then the Ninth Circuit rule yields to Supreme Court authority that postdates it. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc).

Whether it is consistent with *Earls* or not, though, it’s worth a quick detour through *Bulacan*—a case about otherwise-lawful searches undertaken for unlawful secondary purposes, 156 F.3d at 967—to *Davis*. *Davis* holds that in order to render a routine search of an airline

passenger's carry-on bags “as limited in its intrusiveness as is consistent with the satisfaction of the administrative need that justifies it,” the government need only “recognize the right of a person to avoid search by electing not to board the aircraft.” 482 F.2d at 910–11. If that is the rule, well, the Department readily recognizes Sanchez's right to avoid its alleged administrative search by electing not to ride a dockless mobility device.

And there is more mileage still to be had from *Davis*. Sanchez argues that the Department cannot collect location data from dockless mobility devices without first giving him—or the third-party device owners—a mechanism for pre-compliance review. (AOB 47–48.) Even if it is true that some, or even many, kinds of administrative searches require their subjects to have pre-compliance access to a “neutral decisionmaker,” *City of L.A. v. Patel*, 576 U.S. 409, 420 (2015), that cannot be a requirement before *every* kind of administrative search.

There is, after all, no dial-a-judge from *Davis*'s airport security line; there is no magistrate on call at a DUI checkpoint, *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990). Nor, for that matter, is there any explanation why Sanchez has standing to complain in the

first place that the Department provides third-party device owners with inadequate pre-compliance review before collecting their data. *See Meland v. Weber*, 2 F.4th 838, 847 (9th Cir. 2021) (the general rule is that parties must assert their own rights).

II. The district court properly dismissed Sanchez’s California Electronic Communications Privacy Act claim.

A. Review of the dismissal of Sanchez’s CalECPA claim is also de novo.

As with his constitutional claims, this Court reviews the district court’s Rule 12(b)(6) dismissal of Sanchez’s CalECPA claim de novo.

Freeman v. DirecTV, Inc., 457 F.3d 1001, 1004 (9th Cir. 2006).

B. Remedies under CalECPA are prescribed by the statute, and a private right of action against a government entity is not one of the enumerated remedies.

CalECPA limits the circumstances and methods by which “a government entity” may access “electronic device information.” Cal. Penal Code § 1546.1(a); *see id.* §§ 1546(g), (i) (defining “government entity” and “electronic device information”). And it sets forth a list of remedies available if a government entity defies those limits: (a) a person “in a trial, hearing, or proceeding may move to suppress” the information obtained in violation of the restrictions; (b) the California

Attorney General can sue “to compel any government entity” to comply with the restrictions; and (c) a person whose information “is targeted by a warrant, order, or other legal process” that is inconsistent with the restrictions “may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation” of the restrictions or of the California or United States constitutions. *Id.* § 1546.4.

Assuming for argument’s sake that the Department violated CalECPA—something that the City does *not* admit—nowhere in the statute’s list of remedies does one find a private right of action against the Department (or the City).

Consider Sanchez’s contrary position; that is, that hidden somewhere in the plain text of the preceding list of elements (a)–(c) is a private right of action for him. To reveal it, he argues that under § 1546.4(c), any court that *could* issue process is an “issuing court,” and so can be petitioned to destroy information collected by a government entity. That’s his private right of action. (AOB 55–56.)

It’s hard to square Sanchez’s interpretation with the text of the statute—at least, as this brief has recounted it on the preceding page.

But the opening brief offers a holey, if not wholly different, version of the law: “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.” (AOB 55, Sanchez’s ellipses.)

With the opening brief’s ellipses, one indeed might wonder what the phrase “issuing court” means, as the term is left largely devoid of context. Without the opening brief’s elision, it isn’t even a close question. Here is the relevant language returned to the places from which the opening brief excised it: “An individual whose information is targeted [by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the United States Constitution] . . . may petition the issuing court to [void or modify the warrant, order, or process, or] to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.”

When the text is restored, there can be no dispute that “issuing court” means the court (1) that issued the order, which (2) the owner of the targeted information can petition to “void” or to “modify”—two verbs

presupposing that there has been an order issued to be voided or modified. The plain text of the statute thus tells this Court all that it needs to know to dispense quickly with Sanchez’s CalECPA claim. *See Larkin v. Workers’ Comp. Appeals Bd.*, 358 P.3d 552, 555 (Cal. 2015) (“In interpreting a statute, we begin with its text”); *see generally Herrera v. Zumiez, Inc.*, 953 F.3d 1063, 1070 (9th Cir. 2020) (California rules of construction are applied to construe California law).

Which is just as well, because the remainder of the arguments supporting the opening brief’s misleading presentation of the statutory text don’t do anything to buttress its implausible reading of the law. For example, one learns little about the meaning of a term in CalECPA by looking to a federal criminal prohibition on possessing, producing, or distributing fake IDs, 18 U.S.C. § 1028. (AOB 57.) To be sure, the federal statute defines “issuing authority” as an entity that *can issue* identification, rather than as an entity that *has issued* a particular ID—and that’s akin to how Sanchez would define “issuing court” in CalECPA. But the context in which 18 U.S.C. § 1028 uses the phrase “issuing authority” isn’t at all the same as the context in which CalECPA uses “issuing court.” The former prohibits a would-be

criminal defendant from (for example) producing a hologram or watermark that is used by an entity that issues identifications, i.e., an “issuing authority.” 18 U.S.C. §§ 1028(a)(1), (d)(1), (d)(6). The federal law, unlike CalECPA, does not prescribe some action to be taken by the issuing authority vis-à-vis something that has been, or will be, issued.¹¹

The better place to look, if one wants to compare CalECPA with federal law, is the federal Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523. When it enacted CalECPA, the California Legislature was well aware of the federal law (RJN 13), which expressly authorizes a private right of action for violations, 18 U.S.C. § 2520(a). Yet CalECPA lacks an analogous provision. Its legislative history makes no mention of a private right of action, and there is no “dog that didn’t bark theory of statutory construction” that uses legislative silence “to reach a contradictory interpretation of unambiguous text.”

Freeman, 457 F.3d at 1007 (cleaned up). The legislative history is silent

¹¹ The opening brief’s other federal-law analogy, from a regulation governing “unique device authentication” for medical devices, is no better. (AOB 57.)

about a private right of action because the Legislature didn't intend for the law to allow private civil actions against government entities.

The Legislature intended that if government entities were to be held to account civilly for CalECPA violations, it would be by only one person: the California Attorney General. Cal. Penal Code § 1546.4(b). It hardly needs to be said, but “[t]he expression of some things in a statute necessarily means the exclusion of other things not expressed.” *Gikas v. Zolin*, 863 P.2d 745, 752 (Cal. 1993). Sanchez has no private right of action under CalECPA.

III. No amendment can revive Sanchez's claims. The district court correctly dismissed them with prejudice.

This brief ends where the opening brief began, with the question whether Sanchez should be entitled leave to amend his pleadings and try again. The district court's judgment that he should not have been is reviewed de novo. *S.F. Herring Ass'n v. U.S. Dep't of the Interior*, 946 F.3d 564, 575 (9th Cir. 2019).

Whatever the standard of review, the result is the same. The district court correctly denied Sanchez leave to amend.

Start with Sanchez's CalECPA claim. He can allege no facts that will create a private right of action where the California Legislature did not. *See Kroessler v. CVS Health Corp.*, 977 F.3d 803, 815 (9th Cir. 2020) (futility of amendment justifies denying a plaintiff leave to try). Perhaps that is why there are no facts related to Sanchez's CalECPA claim in the list of things "opportunity to amend would have allowed" him to present the district court. (AOB 24.)

There are no facts in that list that bear on the outcome of Sanchez's constitutional claims, either. Sanchez says that he has much to teach the district court about how easy it would be for someone to analyze devices' location data and so to figure out who was riding them. (AOB 24.) None of it matters, though, since there is no whiff of an allegation that someone is actually doing that analysis. *See* § I.C.2, *supra*. Nor is it clear why it should make a lick of difference how difficult it is to analyze the data; all that matters is that the data being analyzed is data in which Sanchez lacks a reasonable expectation of privacy to begin with. *See* § I.C.1, *supra*. Still further, if the data isn't

reasonably private, it makes no constitutional difference why the Department collects the data or what the Department does with it.¹²

If Sanchez does have a reasonable expectation of privacy in the data, though, it's difficult to see how this case differs materially—in procedural posture or in its relevant facts—from *Naperville*. Which means that the Department is conducting a proper administrative search when it obtains that data.

All of that, together, explains why the district court properly put an end to this lawsuit. No facts elaborated in the opening brief compel this Court to revive it.

¹² It's worth pointing out that Sanchez persistently and misleadingly takes out of context a quotation, attributed to the Department's general manager, that the Department is collecting location data to “experiment” with it. (*E.g.*, AOB 10 & n.7.) Reading the article from which Sanchez sourced the quote—it is linked in the opening brief—reveals a discussion about experimenting with different methods for transmitting information from device owners to regulators, not a discussion about experimenting with location data.

CONCLUSION

This Court should affirm the district court's judgment of dismissal without leave to amend.

Respectfully submitted,

Dated: November 5, 2021

LOS ANGELES CITY ATTORNEY'S OFFICE

Michael N. Feuer
Kathleen A. Kenealy
Scott Marcus
Blithe S. Bock
Jonathan H. Eisenman
Jeffrey L. Goss

s/ Jonathan H. Eisenman
Jonathan H. Eisenman

**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)

I am the attorney or self-represented party.

This brief contains **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 **Date**

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

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

ADDENDUM (LOS ANGELES ORDINANCE 186,955)

ORDINANCE NO. 186955

An ordinance amending Article 1, Chapter VII of the Los Angeles Municipal Code to replace the existing shared mobility device pilot program with an annual permit program.

WHEREAS, state law authorizes a local authority to regulate the operation and use of bicycles, scooters, and other shared mobility devices within its jurisdiction to the extent that the local regulations are not in conflict with state law;

WHEREAS, regulations are necessary to ensure that service providers and shared mobility device users obey local and state laws, as well as the Los Angeles Department of Transportation's (Department) Rules and Guidelines governing the safe operation of shared mobility devices in the City;

WHEREAS, for the past two and a half years, the City has implemented a shared mobility pilot program to study the data collected during the pilot period in order to: (1) ensure safe and equitable access to shared mobility devices; (2) adopt rules for the operation, parking, and maintenance of the devices; (3) determine proper fleet size in various locations within the City; and (4) refine and update the current rules and regulations in real time to ensure compliance with local and state laws, including the development of data programs to aid in enforcement, and to prevent the accumulation of devices on sidewalks or other public rights-of-way; and

WHEREAS, the City Council now seeks to make the shared mobility pilot program permanent by authorizing the Department to issue a permit on an annual basis to a service provider of shared mobility devices, and to enforce Rules and Guidelines developed by the Department regarding the use of the devices on City public rights-of-way.

NOW, THEREFORE,

**THE PEOPLE OF THE CITY OF LOS ANGELES
DO ORDAIN AS FOLLOWS:**

Section 1. Section 71.29 of the Los Angeles Municipal Code is amended in its entirety to read as follows:

SEC. 71.29. REGULATION OF SHARED MOBILITY DEVICES.

(a) **Shared Mobility Device Permit Program.** The Department shall implement a Shared Mobility Device Permit Program (Program) and may issue a permit on an annual basis to a qualified service provider (Provider) to operate a shared mobility device (Device) in the City. For purposes of this section, a "shared mobility device," as defined in Civil Code Section 2505, means an electrically motorized board, motorized scooter, electric bicycle, bicycle, or a similar personal transportation device. For

purposes of this section, a “shared mobility device provider,” as defined in California Civil Code Section 2505, means a person or entity that offers, makes available, or provides a Device in exchange for financial compensation or membership via a digital application (app) or other electronic or digital platform. A Provider of a Device shall obtain a permit from the Department and shall be subject to all permit terms and conditions, the Department’s Rules and Guidelines (Rules), this Code, and state or federal law. Failure to comply with the permit terms and conditions, Rules, this Code, or state or federal law may result in: (1) suspension or revocation of the Provider’s permit; (2) penalties as listed in the Rules; (3) reduction in the Provider’s authorized fleet size in the City; and (4) criminal prosecution for a violation of state or federal law.

(b) **General Manager Authority.** Notwithstanding Section 71.29.1 and Section 71.29.2 below, the General Manager of the Department shall have the authority to make technical changes to the Rules as needed, and to make changes necessary to implement the Program, including, but not limited to: (1) updating permit application procedures, permit standards, and permit conditions; and (2) updating operating standards for public safety, data sharing, data privacy, fleet size, and Provider maintenance of the Devices.

Sec. 2. Sections 71.29.1 through 71.29.4 of the Los Angeles Municipal Code are added to read as follows:

SEC. 71.29.1. PROVIDER AND DEVICE FEES.

(a) A Provider of a Device shall pay an initial permit fee in the amount of \$20,000, an annual permit renewal fee in the amount of \$20,000, and trip fees in the range of \$0.06 to \$0.40 per trip. The Department shall determine and calculate the trip fees by the geographic zone where a Device is operated. Each geographic zone shall be defined in the Rules. The Rules shall contain a map or maps of the boundaries of each geographic zone. Each geographic zone depicted on a map or maps shall include the trip fee range for a Device’s operation within the geographic zone.

(b) The City Council, by ordinance, shall approve any amendment to this section to add a new fee, or modify or remove an existing fee, prior to its implementation by the Department. The City Council, by resolution, may amend the Rules to modify the boundaries for operation of a Device in a geographic zone. The Department shall update the Rules to incorporate a fee change or modification of a geographic zone, and any other requirements established by the City Council in the amending fee ordinance or amending resolution.

SEC. 71.29.2. RULES.

The Board of the Transportation Commission (Commission) by resolution shall approve any amendment to the Rules that adds a penalty, or modifies or removes a penalty prior to its implementation by the Department. The Department shall update the

Rules to incorporate the amended penalty and any other requirements established in the amending resolution.

SEC. 71.29.3. VIOLATIONS AND NOTICE OF VIOLATIONS.

(a) **Violations of Section 71.29.** Within six months of discovering a violation of Section 71.29, the Department's Rules, or a permit condition, the Department may issue the Provider a Notice of Violation (NOV) and impose any penalties or order corrective actions listed in the Rules, as authorized in Section 71.29.2. An action by the Department does not preclude any enforcement agency from taking its own enforcement action for violation of any local, state, or federal law or regulation.

(b) **Notice of Violation.**

(1) The Department shall issue a NOV by mail to the Provider's agent for service of process as shown on the Provider's application for a permit. The NOV shall contain all of the following:

- (i) a brief description of the violation(s);
- (ii) a brief description of and bases for the penalties and corrective action, if any, imposed; and
- (iii) a timeframe in which the Provider shall take corrective action, if any, and comply with the penalties, if any, which shall not be sooner than 15 days from the date of mailing of the NOV.

The NOV shall also inform the Provider that the Provider may request an administrative hearing, pursuant to Section 71.29.4, within 15 days of the date the Department mailed the NOV. The Provider's right to an administrative hearing shall be deemed waived if the Provider fails to file a timely request for an administrative hearing.

(2) The NOV shall be final and effective 15 days after the date of its mailing if no administrative hearing was timely requested. If a Provider timely requests an administrative hearing, any portion of the NOV upheld or modified by an appellate body shall be final and effective 15 days after the date the appellate body's decision is deemed final under Section 71.29.4.

(3) If after a NOV becomes final and effective, a Provider fails to comply with the penalties and corrective action, if any, in the NOV, the Department may take one or more of the following actions: 1) denial of a permit or permit renewal; 2) revocation or suspension of a permit; or 3) imposition of more restrictive permit conditions.

(c) **Stipulated Agreement.** Prior to or after issuing a NOV, the Department, at its discretion, may enter into a written agreement with a Provider whereby the

Provider stipulates to having committed a violation in exchange for a negotiated penalty or corrective action, if any. If a Provider violates a stipulated agreement, the Department may issue or re-issue a NOV and impose any penalties listed in the Rules, as authorized under Section 71.29.2.

(d) **Suspension of Permit During Pendency of Administrative Hearing and Appeal.** Depending on the severity of the violation alleged in the NOV, the Department may suspend the Provider's permit during the pendency of the administrative hearing and any appeal. The Department shall give written notice, by mail, of the suspension to the Provider, and shall provide the basis for issuing the suspension. The Provider shall remove all of its Devices from the public right of way within seven calendar days of the date the Department mailed the notice of suspension. While the suspension is in effect, Provider is prohibited from deploying, storing, or operating its Devices within the public right-of-way.

SEC. 71.29.4. REQUESTS FOR ADMINISTRATIVE HEARING AND APPEAL.

(a) A request for an administrative hearing may be filed for the following Department actions:

(1) Issuance of a NOV by the Department.

(2) Denial of an application for a Device permit or permit renewal by the Department.

(b) A request for an administrative hearing shall be filed with the Department within 15 days of the date of mailing of the notice of the Department's action, unless a later date is provided in the NOV or the notice of denial of an application for a Device permit or permit renewal. Failure to timely request an administrative hearing shall constitute a failure to exhaust administrative remedies. If the Department suspends the Provider's permit pursuant to Section 71.29.3(d), the suspension shall remain in effect pending the outcome of the administrative hearing.

(c) The Department shall select a hearing officer and schedule an administrative hearing within 45 calendar days from the date the Department received the request for an administrative hearing. The Department shall mail the notice of the hearing to the Provider's agent for service of process no later than 20 calendar days prior to the date of the hearing. The time for holding a hearing may be extended by mutual agreement between the Department and the Provider.

(d) **Pre-Hearing Disclosures.** No later than seven calendar days prior to an administrative hearing, the Department and the Provider shall make the following pre-hearing disclosures to the hearing officer, with simultaneous email service upon the other party: (i) a brief statement of the facts and issues relating to the request for an administrative hearing; (ii) a copy of all documentary evidence to be offered at the

hearing; and (iii) a list of all witnesses to be presented at the hearing. The hearing officer shall not issue any decision relating to the request before the hearing.

(e) Administrative hearings shall be conducted as follows:

(1) The hearing shall be recorded by an audio device provided by the Department. Any party to the hearing may, at its own expense, cause the hearing to be audio recorded and transcribed by a certified court reporter;

(2) The Department shall have the burden of proof by the preponderance of the evidence;

(3) The hearing officer may accept evidence on which persons would commonly rely in the conduct of their business affairs;

(4) The hearing officer may continue the hearing and request additional relevant information from any party; and

(5) Within 30 days of the conclusion of the hearing, the hearing officer shall issue a written decision that includes a statement of the factual and legal basis of the decision. The hearing officer shall use a de novo standard of review and may uphold or reject, in whole or in part, the Department's action. The hearing officer may waive or reduce the penalties in a NOV after considering the factors specified listed in the Rules, as authorized in Section 71.29.2.

(f) The hearing officer's decision shall be sent by mail to the Provider and shall become final within 15 days of the mailing date, unless the Provider files a timely appeal to the Commission.

(g) The Commission shall hold a public hearing on an appeal by the appellant from a hearing officer's decision within 60 days of the date of filing the appeal to the Commission. The Department shall provide notice of the public hearing no less than 20 days prior to the date of the public hearing. The Commission shall consider de novo the record before the hearing officer and uphold, modify or reject, in whole or in part, the hearing officer's written decision. The Commission may waive or reduce the penalties in the hearing officer's decision after considering the factors listed in the Rules, as authorized in Section 71.29.2. The Commission shall not consider evidence outside of the record before the hearing officer. The Commission shall issue a decision within 30 days of the conclusion of the hearing and mail it to the appellant. The Commission's decision is final.

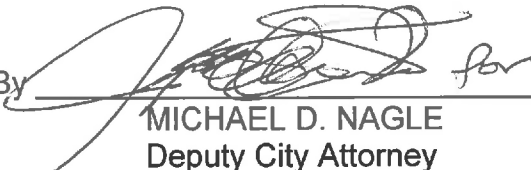
Sec. 3. URGENCY CLAUSE. The City Council finds and declares that this ordinance is required for the immediate protection of the public peace, health, and safety for the following reason: The shared mobility device pilot program is set to expire on March 31, 2021. Therefore, this ordinance must become effective by April 1, 2021, in order to preserve the Department's ability to regulate shared mobility devices

operating in the City and protect its residents in the public right-of-way. The City Council adopts this ordinance to become effective upon publication pursuant to Los Angeles City Charter Section 253.

Sec. 4. The City Clerk shall certify to the passage of this ordinance and have it published in accordance with Council policy, either in a daily newspaper circulated in the City of Los Angeles or by posting for ten days in three public places in the City of Los Angeles: one copy on the bulletin board located at the Main Street entrance to the Los Angeles City Hall; one copy on the bulletin board located at the Main Street entrance to the Los Angeles City Hall East; and one copy on the bulletin board located at the Temple Street entrance to the Los Angeles County Hall of Records.

Approved as to Form and Legality

MICHAEL N. FEUER, City Attorney

By  for
MICHAEL D. NAGLE
Deputy City Attorney

Date MAR 10 2021


File No. 17-1125

M:\GENERAL COUNSEL DIVISION\ORDINANCES AND REPORTS\ORDINANCES - FINAL YELLOW\LAMC 71.29 Shared Mobility Device Program Ordinance 3.10.21.docx

The Clerk of the City of Los Angeles hereby certifies that the foregoing ordinance was passed by the Council of the City of Los Angeles, **by a vote of not less than three-fourths** of all its members.

CITY CLERK

MAYOR





Ordinance Passed April 6, 2021

Approved 04/19/2021

Publish Date: 04-26-21
Ordinance Effective Date: 04-26-21