FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN SANCHEZ, *Plaintiff-Appellant*, v. LOS ANGELES DEPARTMENT OF TRANSPORTATION; CITY OF LOS ANGELES, *Defendants-Appellees.*	No. 21-55285 D.C. No. 2:20-cv-05044-DMG-AFM ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the Central District of California
Dolly M. Gee, District Judge, Presiding

Argued and Submitted March 8, 2022
Pasadena, California

Filed May 23, 2022
Amended July 8, 2022

Before: Kim McLane Wardlaw and Andrew D. Hurwitz, Circuit Judges, and Lee H. Rosenthal,[*] District Judge.

[*] The Honorable Lee H. Rosenthal, Chief United States District Judge for the Southern District of Texas, sitting by designation.

Order;
Opinion by Judge Hurwitz

SUMMARY**

Civil Rights

The panel amended its prior opinion affirming the district court's order dismissing, for failure to state a claim, an action brought by an e-scooter user alleging that the City of Los Angeles' e-scooter permitting program, which requires e-scooter companies to disclose real-time location data for every device, violates the Fourth Amendment and California law.

As a condition of getting a permit, the Los Angeles Department of Transportation ("LADOT") required e-scooter operators to provide vehicle location data through an application programming interface called Mobility Data Specification ("MDS"). Used in conjunction with the operators' smartphone applications, MDS automatically compiles real-time data on each e-scooter's location by collecting the start and end points and times of each ride taken.

The complaint alleged that the MDS protocols provide the location of e-scooters with Orwellian precision. A City therefore allegedly could easily use MDS data in conjunction with other information to identify trips by individuals to

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

sensitive locations. Because the location data could be preserved in accordance with LADOT data-retention policies, plaintiff alleged that the City could travel back in time to retrace a rider's whereabouts.

The panel first held that plaintiff's complaint alleged facts giving rise to Article III standing and therefore the panel rejected LADOT's assertion that the complaint was beyond the panel's constitutional purview because it was premised on a hypothetical invasion of privacy that might never occur. Drawing all reasonable inferences in favor of plaintiff as it was required to do at the Fed. R. Civ. P. 12(b)(6) stage, the proper reading of the complaint was that plaintiff alleged that the collection of the MDS location data itself—without more—violated his constitutional rights.

The panel concluded that the third-party doctrine, which provides that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, foreclosed plaintiff's claim of a reasonable expectation of privacy over the MDS data. Focusing first on "voluntary exposure," the panel had little difficulty finding that plaintiff knowingly and voluntarily disclosed location data to the e-scooter operators. Unlike a cell phone user, whose device provides location information by dint of its operation, without any affirmative act on the part of the user, plaintiff affirmatively chose to disclose location data to e-scooter operators each time he rented a device. Having voluntarily conveyed his location to the operator in the ordinary course of business, plaintiff could not assert a reasonable expectation of privacy.

The panel next determined that the nature of MDS location data indicated a diminished expectation of privacy. The data only discloses the location of an e-scooter owned

by the operator and typically rerented to a new user after each individual trip. It was thus quite different than the information generated by a cell phone, which identifies the location of a particular user virtually continuously. The complaint admitted that the MDS data could not be linked to a particular individual without more. Although the Supreme Court has rejected the proposition that inference insulates a search, there was no allegation that the MDS data was in fact used to infer the identity of any individual rider.

The panel held that because the third-party doctrine squarely applied to plaintiff's voluntary agreement to provide location data to the e-scooter operators, the collection of that data by LADOT was not a search and did not violate the Fourth Amendment or the California Constitution. The panel cautioned that its decision was narrow and expressed no view on matters not before the panel, including the result if the MDS data were alleged to have been shared with law enforcement or used to infer individual riders' identities or locations.

The panel affirmed the district court's dismissal of plaintiff's claim under the California Electronic Communications Privacy Act ("CalECPA") on the grounds that the statute did not provide plaintiff with authorization to bring an independent action to enforce its provisions.

Finally, the panel held that the district court did not err in dismissing the complaint without leave to amend. Because plaintiff had no reasonable expectation of privacy over the MDS location data, no additional facts could possibly have cured the deficiency with his constitutional claims. And, because the court rightly found that the CalECPA did not create a private right of action, dismissal of the statutory claim was also not error.

COUNSEL

Mohammad Tajsar (argued), ACLU Foundation of Southern California, Los Angeles, California; Jacob A. Snow, ACLU Foundation of Northern California, San Francisco, California; Jennifer Lynch and Hannah Zhao, Electronic Frontier Foundation, San Francisco, California; Douglas E. Mirell and Timothy J. Toohey, Greenberg Glusker Fields Claman & Machtinger LLP, Los Angeles, California; for Plaintiff-Appellant.

Jonathan H. Eisenman (argued) and Jeffrey L. Goss, Deputy City Attorneys; Blithe S. Bock, Managing Assistant City Attorney; Scott Marcus, Chief Assistant City Attorney; Kathleen A. Kenealy, Chief Deputy City Attorney; Michael N. Feuer, City Attorney; Office of the City Attorney, Los Angeles, California; for Defendants-Appellees.

Kendra K. Albert and Mason A. Kortz, Cyberlaw Clinic, Harvard Law School, Cambridge, Massachusetts, for Amici Curiae Seven Data Privacy and Urban Planning Experts.

Brian E. Klein and Melissa A. Meister, Waymaker LLP, Los Angeles, California; Samir Jain and Gregory T. Nojeim, Center for Democracy & Technology, Washington, D.C.; Alan Buter, Megan Iorio, and Melodi Dincer, Electronic Privacy and Information Center; for Amici Curiae Center for Democracy & Technology, and Electronic Privacy Information Center.

Jordan R. Jaffe, Quinn Emanuel Urquhart & Sullivan LLP, San Francisco, California, for Amicus Curiae Kevin Webb.

Alana H. Rotter and Nadia A. Sarkis, Greines Martin Stein & Richland LLP, Los Angeles, California, for Amicus Curiae Open Mobility Foundation.

ORDER

The opinion is amended as follows:

1. At slip opinion page 21, replace <We decline the invitation to conclude that LADOT's collection of anonymous data about traffic movements is somehow rendered a search because it may be used in the future (in connection with other non-private material) to reveal an individual's previous locations. Even accepting Sanchez's contention that anonymous MDS data can be used in the future to draw inferences about who was using a scooter at a particular time, "an inference is not a search." *Kyllo*, 533 U.S. at 37 n.4.> with <Although the Supreme Court has "rejected the proposition that 'inference insulates a search,'" *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo*, 533 U.S. at 36)), there is no allegation that the MDS data was in fact used to infer the identity of any individual rider.>.

2. At slip opinion page 23, after <does not violate the Fourth Amendment or the California Constitution.> include <We caution that our "decision today is a narrow one." *Carpenter*, 138 S. Ct. at 2220. We "express no view on matters not before us," *id.*, including the result if the MDS data were alleged to have been shared with law enforcement or used to infer individual riders' identities or locations. *See Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2018) (privacy interests are "lessened" where there

is "no prosecutorial intent" (citing *Camara v. Mun. Ct. of San Francisco*, 387 U.S. 523, 530 (1967)).>

OPINION

HURWITZ, Circuit Judge:

Faced with a near-overnight invasion of motorized electric scooters ("e-scooters"), which cluttered sidewalks and interfered with street access, the City of Los Angeles adopted a permitting program and required e-scooter companies to disclose real-time location data for every device.[1] In this action, an e-scooter user claims that the location disclosure requirement violates the Fourth Amendment and California law. The district court dismissed the complaint for failure to state a claim. We affirm.

I.

Companies such as Bird, Lime, and Lyft began offering e-scooters for rent to the public in Los Angeles in 2017. The e-scooters are dockless, meaning they can be left anywhere after use and picked up by the next rider. They are also internet-connected, and are rented through the companies' smartphone applications, which charge riders based on the distance and duration of the trip taken.

In 2018, Los Angeles enacted a "Shared Mobility Device Pilot Program" to regulate the fledgling industry. L.A. Ord. 185,785 (Sept. 13, 2018). The program required companies

[1] We use the term "e-scooter" to refer to the panoply of so-called micro-mobility devices offered for rent by permittees. *See* L.A. Ord. 185,785 (Sept. 13, 2018).

to obtain a permit from the Los Angeles Department of Transportation ("LADOT") to offer e-scooters for rent and mandated that permittees "comply with all Department permit rules, regulations, indemnification, insurance and fee requirements." *Id*. As a condition of getting a permit, LADOT required e-scooter operators to provide vehicle location data through an application programming interface ("API")[2] called Mobility Data Specification ("MDS"). Used in conjunction with the operators' smartphone applications, MDS automatically compiles real-time data on each e-scooter's location by collecting the start and end points and times of each ride taken.[3] Because LADOT obtains data directly from the companies in real time, it can manage the public right-of-way actively and "communicate directly with product companies in real time using code."[4]

Plaintiff Justin Sanchez uses e-scooters to travel from his home to work, visit friends, frequent local businesses, and access places of leisure. His complaint asserts that the collection of MDS location data by LADOT violates the Fourth Amendment to the United States Constitution; Article I, Section 13 of the California Constitution; and the

[2] An API "acts as an intermediary between two other programs . . . to exchange information." Dave Johnson, *A guide to APIs, software that helps different apps work together,* Bus. Insider (May 13, 2021), https://www.businessinsider.com/what-is-an-api.

[3] LADOT also requires the submission of data on the specific route taken between those points within twenty-four hours of the trip.

[4] *See* "Mobility Data Specification: Information Briefing," L.A. Dep't of Transp. (Oct. 31, 2018), https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf.

California Electronic Communications Privacy Act ("CalECPA"), Cal. Penal Code § 1546 *et seq.*

The complaint alleges that the MDS protocols provide the location of e-scooters with Orwellian precision, to within 1.11 centimeters of their exact location. It acknowledges that "MDS does not collect any information directly identifying the rider of a particular vehicle." But, Sanchez alleges that government actors could subsequently "match users' trajectories in anonymized data from one dataset, with deanonymized data in another," and research indicates programmers "could identify 50% of people from only two randomly chosen data points in a dataset that contained only time and location data." The City therefore can "easily," he alleges, use MDS data in conjunction with other information to identify trips by individuals to sensitive locations. And, because the location data may be preserved in accordance with LADOT data-retention policies, Sanchez alleges that the City can travel back in time to retrace a rider's whereabouts.

The district court granted LADOT's motion to dismiss the complaint without leave to amend. *Sanchez v. L.A. Dep't of Transp.*, No. CV-20-5044-DMG, 2021 WL 1220690 (C.D. Cal. Feb. 23, 2021). It found that the LADOT program is not a search under the Fourth Amendment because Sanchez has no reasonable expectation of privacy over anonymous MDS location data. *Id.* at *4. It alternatively concluded that, even if the collection of MDS data were a search, it is a reasonable administrative one and thus constitutional. *Id*. at *5–6. Because "the right to be free from unreasonable searches under Art. I § 13 of the California Constitution parallels the Fourth Amendment inquiry," *Sanchez v. Cnty. of San Diego*, 464 F.3d 916, 928–29 (9th Cir. 2006), the district court also dismissed

Sanchez's state constitutional claim. *Id.* at *2. And it rejected the CalECPA claim, finding that the statute did not provide Sanchez a private right of action. *Id*. at *6.

Finding any amendment futile, the district court dismissed the complaint with prejudice. *Id.* This timely appeal followed.

II.

LADOT first argues that we must dismiss Sanchez's claims because he lacks Article III standing. *See In re Apple iPhone Antitrust Litig.*, 846 F.3d 313, 319 (9th Cir. 2017) (noting that Article III standing is a jurisdictional requirement that may be raised "at any time"). LADOT argues that this complaint is beyond our constitutional purview because it is premised on a hypothetical future invasion of privacy that may never occur.

To establish Article III standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). We must "assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id*. at 2204 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). "[T]hose traditional harms may also include harms specified by the Constitution itself." *Id*. (citing *Spokeo*, 578 U.S. at 340; *Pleasant Grove City v. Summum*, 555 U.S. 460 (2009) (abridgment of free speech); *Church of Lukumi Babalu Aye, Inc. v. Hialeah*, 508 U.S. 520 (1993) (infringement of free exercise)). And, although "traditional tangible harms, such as physical harms and monetary

harms," most "readily qualify as concrete injuries," "intangible harms can also be concrete." *Id*.

Applying this settled doctrine, we conclude that Sanchez's complaint alleges facts giving rise to Article III standing. The harm alleged is one "specified by the Constitution itself," *id.*—the violation of the Fourth Amendment guarantee against unreasonable searches and seizures. Moreover, the alleged injury has a close nexus to those traditionally providing a "basis for a lawsuit in English or American courts," *Spokeo*, 578 U.S. at 341, such as "disclosure of private information" and "intrusion upon seclusion." *TransUnion*, 141 S. Ct. at 2204.

Drawing all "reasonable inferences" in favor of Sanchez as we are required to do at the Rule 12(b)(6) stage, the proper reading of this complaint is not, as LADOT asserts, that someone someday "*might* perform an analysis of device location data, which *might* disclose Sanchez's scooter-borne peregrinations." Rather, Sanchez alleges that the collection of the MDS location data itself—without more—violates his constitutional rights today.

It makes no difference for the purposes of determining Article III standing whether Sanchez's complaint states a valid Fourth Amendment claim. That "confuses the jurisdictional inquiry . . . with the merits inquiry." *Ecological Rights Found. v. Pac. Lumber Co.*, 230 F.3d 1141, 1151 (9th Cir. 2000). We therefore turn to the merits.

III.

The Fourth Amendment prohibits "unreasonable searches and seizures." U.S. Const. amend. IV. The initial issue for decision is whether LADOT's collection of MDS

location data is a search for Fourth Amendment purposes.[5] Only if collection of the data is a search do we need to address the separate question of whether that search is unreasonable. *See Florida v. Jimeno*, 500 U.S. 248, 250 (1991).

For much of our Nation's history, the definition of a search under the Fourth Amendment was "tied to common-law trespass," focusing on whether government actors had obtained "information by physically intruding on a constitutionally protected area." *United States v. Jones*, 565 U.S. 400, 405, 406 n.3 (2012). In *Olmstead v. United States*, for example, the Supreme Court found that wiretaps attached to telephone wires on public streets did not constitute a search because "[t]here was no entry of the houses or offices of the defendants." 277 U.S. 438, 464 (1928).

The Court significantly expanded the doctrinal scope of the analysis in *Katz v. United States*, finding that the attachment of an eavesdropping device to a public telephone booth was a search, memorably stating that "the Fourth Amendment protects people, not places." 389 U.S. 347, 351 (1967). Its subsequent decisions have framed the inquiry as whether the challenged government action violates a person's "reasonable expectation of privacy," citing Justice Harlan's seminal *Katz* concurrence. *Id*. at 360. Thus, when an individual "seeks to preserve something as private," and that expectation of privacy is "one that society is prepared to recognize as reasonable," government intrusion into that private sphere generally qualifies as a search requiring a

[5] Sanchez does not raise any independent arguments about the illegality of the data collection under the California Constitution, acknowledging that that inquiry is "functionally coterminous" with Fourth Amendment review.

warrant supported by probable cause. *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (cleaned up).

A.

Thus, the essential inquiry is whether collection of MDS location data "violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Answering that question implicates "the intersection of two lines of cases, both of which inform [an] understanding of the privacy interests at stake." *Carpenter v. United States*, 138 S. Ct. 2206, 2214–15 (2018). The first line "addresses a person's expectations of privacy in his physical location and movements." *Id*. at 2215. The second concerns the "line between what a person keeps to himself and what he shares with others," implicating the so-called third-party doctrine. *Id.* at 2216. That doctrine teaches that a person "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44.

1.

In the first line of cases, Supreme Court decisions after *Katz* have considered a person's reasonable expectation of privacy with respect to his physical location and movements. In *United States v. Knotts*, the Court addressed police officers' use of a GPS "beeper" planted in a container to track an automobile to a remote cabin. *See* 460 U.S. 276, 281–82 (1983). Reasoning that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," the Court held that Knotts had no privacy interest in the information obtained through use of the beeper. *Id*. *Knotts* stressed the "limited use which the government made of the signals from [a] particular beeper" during a discrete

"automotive journey." *Id.* at 284–85. But, the Court left for another day whether "different constitutional principles may be applicable" if "twenty-four-hour surveillance of any citizen of this country" were involved. *Id*. at 283–84.

Subsequently, the Court considered installation of a GPS tracking device on the defendant's vehicle and continuous remote monitoring of its movement for 28 days. *See Jones*, 565 U.S. at 402–03. Although the Court's opinion ultimately turned on the physical trespass of the vehicle when the device was planted, *see id*. at 404–05, five Justices suggested in concurrences that reasonable privacy concerns would also be raised by "surreptitiously activating a stolen vehicle detection system" in Jones's car to track him or conducting GPS tracking of his cell phone, *id*. at 426 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *see also id*. at 415 (Sotomayor, J., concurring). They suggested that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id*. at 430 (Alito, J., concurring); *see also id*. ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."); *id.* at 415 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.") (Sotomayor, J., concurring).

Most recently, in *Carpenter*, the Court held that government collection of historical cell site location information ("CSLI") violated a reasonable expectation of privacy. Because "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record

of the holder's whereabouts," 138 S. Ct. at 2217, the Court concluded that "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle . . . in *Jones*," *id*. at 2218. Acting as "almost a 'feature of human anatomy,'" the Court noted, a cell phone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id*. (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). "Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*.

Carpenter also stressed the "retrospective quality of the data." *Id*. "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id*. But, with historical CSLI, the government can "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers," which kept those records for "up to five years." *Id*. "Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when"—resulting in a "tireless and absolute surveillance" for anyone with a cell phone. *Id*. Accordingly, when the government acquired Carpenter's CSLI from wireless carriers, it violated his "reasonable expectation of privacy in the whole of his physical movements." *Id*. at 2219.

The Court repeatedly stated that the unique nature of cell phones raises Fourth Amendment concerns. *See id.* at 2218 ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time."); *see also Riley*, 573 U.S. at 395 (observing "nearly three-quarters" of cell phone users spend "most of the time" living

"within five feet" of their phone). But it carefully underscored that the decision was "a narrow one," noting, "[w]e do not express a view on matters not before us: real-time CSLI or 'tower dumps.'" *Carpenter*, 138 S. Ct. at 2220. And, critically, the decision concluded: "We do not disturb the application of *Smith* and *Miller*." *Id*. It is this second line of cases—concerning a person's expectation of privacy with respect to information he voluntarily turns over to others—to which we next turn.

2.

The third-party doctrine teaches that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44; *see also United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016) (noting that the "third-party doctrine" instructs "that a person's privacy interest is diminished where he or she reveals information to a third party, even in confidence"). This is true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller*, 425 U.S. 435, 443 (1976). "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2216.

In *Miller*, investigating tax evasion, the government subpoenaed the defendant's banks, seeking cancelled checks, deposit slips, and monthly statements. *See* 425 U.S. at 438–39. The Court rejected Miller's Fourth Amendment challenge because he could "assert neither ownership nor possession" of these "business records of the banks." *Id*. at 440. Moreover, the Court found that the nature of the records confirmed Miller's limited expectation of privacy with respect to them. *See id*. at 442. The checks were "not

confidential communications but negotiable instruments to be used in commercial transactions"; and the bank statements were "exposed to [bank] employees in the ordinary course of business." *Id*. Having "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government," Miller's purported expectations of privacy were unavailing. *Id*. at 443.

Smith applied these principles to information conveyed to a telephone company. *See* 442 U.S. at 737–46. The Court held that the government's use of a "pen register"—which records the phone number dialed on a landline—was not a "search." *Id*. at 745–46. In so ruling, the Court noted its "doubt that people in general entertain any actual expectation of privacy in the numbers they dial." *Id*. at 742. Telephone users know, the Court reasoned, that the numbers are used "for a variety of legitimate business purposes" by the telephone company, including routing calls. *Id*. at 743. Thus, when Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." *Id*. at 744. He also "assumed the risk" that the company's records "would be divulged to police." *Id*. at 745. Thus, any subjective expectation Smith had that the numbers he dialed would be kept private "is not one that society is prepared to recognize as reasonable." *Id*. at 743 (cleaned up).

We have applied the "voluntary exposure" concept underpinning the third-party doctrine to find that a person has no reasonable expectation of privacy in the fact that he has booked a hotel room. *See United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000). So too, we have found that a person has no reasonable expectation of privacy in who

comes and goes from the hotel room. *See Patel v. City of Montclair*, 798 F.3d 895, 900 (9th Cir. 2015); *see also United States v. Rosenow*, No. 20-50052, 2022 WL 1233236, at *13 (9th Cir. Apr. 27, 2022) (observing that a person has no expectation of privacy in information knowingly "provided to and used by internet service providers for the specific purpose of directing the routing of information"). The familiar proposition that an individual has no expectation of privacy over items left in "plain view" of others derives from the same general principle. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 133–34 (1990) ("If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."). The third-party doctrine has also been cited to explain why "neither the 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).[6]

Nevertheless, as we recently observed, "commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities." *United States v. Moalin*, 973 F.3d 977, 992 (9th Cir. 2020).[7] Justice Sotomayor, for instance, has

[6] *See also* Orin S. Kerr, *Implementing Carpenter* (Dec. 14, 2018), THE DIGITAL FOURTH AMENDMENT (Oxford University Press), Forthcoming, USC Law Legal Studies Paper No. 18–29, https://ssrn.com/abstract=3301257 (suggesting that 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 Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[7] *See, e.g.*, *Evan Frohman, 23PolicemenAndMe: Analyzing the Constitutional Implications of Police Use of Commercial DNA Databases*, 22 U. PA. J. CONST. L. 1495 (2020).

noted that the assumption-of-risk rationale underlying the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). And, in *Carpenter*, Justice Gorsuch remarked:

> Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* . . . teach[es] that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

138 S. Ct. at 2262 (Gorsuch, J., dissenting).

And, of course, *Carpenter* itself rejected application of the third-party doctrine to government collection of historical CSLI. *See id*. at 2220. In so doing, the Court observed that it has "shown special solicitude for location information in the third-party context," citing the concurrences in *Jones*, *id*. at 2219–20, and concluded that the "detailed chronicle of a person's physical presence" presented by historical CSLI "implicates privacy concerns far beyond those considered in *Smith* and *Miller*," *id*. at 2220.

But, notably, *Carpenter* did not overrule *Smith* and *Miller*, despite Justice Gorsuch's invitation to do so. *See id.* at 2262 (dissenting opinion). Rather, it simply found the third-party doctrine inapplicable in the case before it, while expressly declining to "disturb the application of *Smith* and *Miller*" in other contexts. *Id.* at 2220. Specifically, the Court found that collection of historical CSLI fell outside the

doctrine by focusing on its two underlying rationales—first, whether the nature of the material revealed to third-parties indicates a "reduced expectation of privacy," and, second, whether there was "voluntary exposure" of the information to others. *Id*. at 2219–20.

Addressing the first rationale, the Court noted that although one normally does not have an expectation of privacy in his movement on public streets, the "pervasive" tracking of movements revealed by historical CSLI was different because it provided "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 2220. The Court rejected the government's reliance on *Knotts* as failing "to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." *Id*. at 2219. And it noted that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*" and the "exhaustive chronicle of location information casually collected by wireless carriers today." *Id*. Thus, the reduced expectation of privacy normally occurring when one reveals his location by traveling on public streets was much diminished. *Id*.

Addressing the second rationale—"voluntary exposure"—the Court highlighted that CSLI is "not truly 'shared' as one normally understands the term." *Id*. at 2220. Rather, it recognized that CSLI is generated as a background function to cell phone use, simply by powering up the device. *See id*. Because carrying a cell phone "is indispensable to participation in a modern society," *Carpenter* concluded that "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a

comprehensive dossier of his physical movements." *Id.* (quoting *Smith*, 442 U.S. at 745).

B.

Relying heavily on the Court's statement in *Carpenter* that it has "shown special solicitude for location information in the third-party context," *id*. at 2219, Sanchez argues that we must treat the collection of MDS data as a search under the Fourth Amendment. But, because *Carpenter* expressly stated that it was not disturbing the application of the third-party doctrine in contexts other than the collection of historical CSLI, that case only begins, rather than ends, our inquiry. Rather, as the Court did in *Carpenter*, we focus on whether application of the doctrine to this case would be consistent with its underlying rationales. *See Rosenow*, 2022 WL 1233236 at *12–13 (finding "*Carpenter* is distinguishable" and applying third-party doctrine). We conclude that the doctrine does apply here, foreclosing Sanchez's claim of a reasonable expectation of privacy over the MDS data.

Focusing first on "voluntary exposure," we have little difficulty finding that Sanchez knowingly and voluntarily disclosed location data to the e-scooter operators. Unlike a cell phone user, whose device provides location information "by dint of its operation, without any affirmative act on the part of the user," *Carpenter*, 138 S. Ct. at 2220, Sanchez affirmatively chose to disclose location data to e-scooter operators each time he rented a device. Indeed, his complaint concedes that, in order to charge him, an e-scooter operator necessarily must "track rides" by obtaining location data on the route taken. And, before renting an e-scooter, Sanchez must agree to the operator's privacy policies. Lyft's privacy policies, for instance, a copy of which Sanchez attached to his complaint, expressly state that "location data"

will be collected, stored by the rental company, and shared with government authorities to "comply with any applicable . . . local law or regulation."

When Sanchez rents an e-scooter, he plainly understands that the e-scooter company must collect location data for the scooter through its smartphone applications. Thus, the voluntary exposure rationale fits far better here than in *Carpenter*. Having "voluntarily conveyed" his location to the operator "in the ordinary course of business," Sanchez cannot assert a reasonable expectation of privacy. *Smith*, 442 U.S. at 744. Rather, because MDS data is knowingly disclosed as a central feature of his transaction with a third party—much like the route of a taxi ride is disclosed to a cab driver, *see Azam*, 46 F. Supp. 3d at 50—the situation fits comfortably within the ambit of *Smith* and *Miller*.

Second, the nature of MDS location data indicates a diminished expectation of privacy. The data only discloses the location of an e-scooter owned by the operator and typically rerented to a new user after each individual trip. It is thus quite different than the information generated by a cell phone, which identifies the location of a particular user virtually continuously.[8] Sanchez alleges that, armed with MDS data, government actors could later "easily" associate a given ride with an individual rider, using non-MDS information. But his complaint admits that the MDS data cannot be linked to a particular individual without more. Although the Supreme Court has "rejected the proposition

[8] It also makes the data unlike the telephony metadata collected by the NSA which we considered in *Moalin*, which included "comprehensive communications routing information" that "provides information about where a phone connected to the network, revealing data that can locate the parties" subject to the metadata capture. 973 F.3d at 991.

that 'inference insulates a search,'" *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo*, 533 U.S. at 36)), there is no allegation that the MDS data was in fact used to infer the identity of any individual rider.

So too, in contrast to the CSLI at issue in *Carpenter* and the beeper tracking in *Jones*, the MDS data does not "pervasive[ly] track" users over an extended period, *see* 138 S. Ct. at 2220, instead capturing only the locations of e-scooters during discrete trips. Those e-scooters are continuously collected, recharged, and rerented. Even a regular rider could find herself using one e-scooter for her ride to work on Friday, picking up a different one to meet friends Saturday, and making her way home Sunday on yet another.

The location data is thus far afield from the dragnet, continuous monitoring of an identified individual's movements at issue in *Carpenter* and *Jones*.[9] For example, in *Carpenter*, authorities specifically requested cell records to trace the whereabouts of Timothy Carpenter over the course of 127 days. 138 S. Ct. at 2212. Here, the collection of MDS data is more like the remote monitoring of a discrete "automotive journey" in *Knotts*, 460 U.S. at 285, as MDS

[9] It also makes the MDS data collection far afield from the continuous monitoring central to the decisions in two recent cases upon which Sanchez extensively relies. *Leaders of a Beautiful Struggle v. Baltimore Police Department* involved the use of wide-angle cameras throughout the City of Baltimore, which "continuously records public movements." 2 F.4th 330, 347 (4th Cir. 2021) (en banc). And, in *Commonwealth v. McCarthy*, the Massachusetts Supreme Judicial Court emphasized that it was only with "enough cameras in enough locations"—allowing for continuous monitoring—that a program of automated readers capturing license plates could be said to "invade a reasonable expectation of privacy" and "constitute a search." 142 N.E.3d 1090, 1104 (Mass. 2020).

only collects route data and real-time location of an e-scooter for a single ride.

And, perhaps most obviously, e-scooters, unlike cell phones, are simply not "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. They are but one of many different means available for short-distance travel in some urban environments. Cell phones function for users as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, [and] newspapers"—and "also happen to have the capacity to be used as a telephone." *Riley*, 573 U.S. at 393. And, given "their immense storage capacity," cell phones allow users to carry in their pocket "millions of pages" of material—as if they carried around "every piece of mail they have received" or "every picture they have taken." *Id*. at 393–94. Cell phones are a "pervasive and insistent part of daily life" such that users are within several feet of them most of the time, with some "12% admitting that they even use their phones in the shower." *Carpenter*, 138 S. Ct. at 2218 (quoting *Riley*, 573 U.S. at 385, 395). By contrast, immediately following a ride, as Sanchez acknowledges in his complaint, an e-scooter user unceremoniously "leaves the scooter on the street."

We therefore conclude that the considerations animating the Court's "narrow" decision in *Carpenter* declining to apply the third-party doctrine are not present here. *See* 138 S. Ct. at 2220. Because the third-party doctrine squarely applies to Sanchez's voluntary agreement to provide location data to the e-scooter operators, the collection of that data by LADOT is not a search, and does not violate the Fourth Amendment or the California Constitution.[10] We

[10] Because we find that collection of the MDS location data was not a search, we do not separately address the district court's determination

caution that our "decision today is a narrow one." *Carpenter*, 138 S. Ct. at 2220. We "express no view on matters not before us," *id.*, including the result if the MDS data were alleged to have been shared with law enforcement or used to infer individual riders' identities or locations. *See Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2018) (privacy interests are "lessened" where there is "no prosecutorial intent" (citing *Camara v. Mun. Ct. of San Francisco*, 387 U.S. 523, 530 (1967)).

IV.

We next review the dismissal of the CalECPA claim. That statute limits how state entities may access "electronic device information." Cal. Penal Code § 1546.1(a); *see id.* § 1546(g) (defining "electronic device information" as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device"). Except after adherence with certain procedures, *see* § 1546.1(b)–(k), it prevents state actors from: (1) compelling the production of electronic communication information from a service provider, *id.* § 1546.1(a)(1); (2) compelling the production of electronic device information from anyone other than the authorized possessor, *id.* § 1546.1(a)(2); and (3) accessing electronic device information by means of physical interaction or

---

that it was a reasonable one "in the context of safety and administrative regulations." *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottwatomie Cnty. v. Earls*, 536 U.S. 822, 829 (2002).

electronic communication with the device, *id.* § 1546.1(a)(3).[11]

But not anyone may sue for enforcement. The statute permits: (a) a person "in a trial, hearing, or proceeding" to "move to suppress" information obtained in violation of its provisions, *id*. § 1546.4(a); (b) the California Attorney General to "commence a civil action to compel any government entity" to comply with the restrictions, *id*. § 1546.4(b); and (c) a person whose information "is targeted by a warrant, order, or other legal process" inconsistent with the restrictions to "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, *id*. § 1546.4(c) (emphasis added).

Sanchez's relies on § 1546.4(c), claiming that the phrase "issuing court" refers to "courts with the authority to issue legal process"—and that because the district court has such authority, he has a private right of action. But, the plain text of the statute indicates that the term "issuing court" is one that previously issued "a warrant, order, or other legal process" that "targeted" an individual's information which the individual seeks to "void or modify." *Id*. § 1546.4(c). Because no court previously issued such an order here, the statute does not authorize Sanchez to bring an independent action to enforce its provisions. Indeed, in contrast, the statute expressly allows the California Attorney General to "commence a civil action" to enforce the statute. *Id*. at § 1546.4(b); *see Gikas v. Zolin*, 863 P.2d 745, 752 (Cal.

[11] *See also* Bill Analysis, Senate Committee on Public Safety, SB 178 (March 23, 2015) at 1 ("The purpose of this bill is to require a search warrant or wiretap order for access to all aspects of electronic communications . . . .").

1993) ("The expression of some things in a statute necessarily means the exclusion of other things not expressed.").

V.

Finally, Sanchez challenges the dismissal of his complaint without leave to amend. A district court may dismiss a complaint without leave to amend if "the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency." *Albrecht v. Lund*, 845 F.2d 193, 195 (9th Cir. 1988) (cleaned up); *see also Kroessler v. CVS Health Corp.*, 977 F.3d 803, 815 (9th Cir. 2020) (futility of amendment justifies denying leave).

Accepting "as true all well-pleaded allegations of material fact," and construing them "in the light most favorable to the non-moving party," we find the district court did not err in dismissing the complaint without leave to amend. *See Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). Courts are to "consider the relevant factors and articulate why dismissal should be with prejudice instead of without prejudice," *Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003), and the district court did so here. It correctly concluded that because Sanchez has no reasonable expectation of privacy over the MDS location data, no additional facts could possibly have cured the deficiency with his constitutional claims. And, because the court rightly found that the CalECPA does not create a private right of action, dismissal of the statutory claim was also not error.

AFFIRMED.