

1 Roberta A. Kaplan (*pro hac vice forthcoming*)
rkaplan@kaplanhecker.com
2 John C. Quinn (*pro hac vice forthcoming*)
jquinn@kaplanhecker.com
3 Benjamin D. White (*pro hac vice forthcoming*)
4 bwhite@kaplanhecker.com
KAPLAN HECKER & FINK LLP
5 350 Fifth Avenue, Suite 7110
New York, NY 10118
6 Telephone: (212) 763-0883

7 Marc S. Williams (Bar No. 198913)
mwilliams@cohen-williams.com
8 Neil S. Jahss (Bar No. 162744)
njahss@cohen-williams.com
9 **COHEN WILLIAMS LLP**
10 724 South Spring Street, 9th Floor
Los Angeles, CA 90014
11 Telephone: (213) 232-5160
12 Facsimile: (213) 232-5167

13 Attorneys for Plaintiff
14 Social Bicycles LLC d/b/a JUMP

15
16 **UNITED STATES DISTRICT COURT**
17 **CENTRAL DISTRICT OF CALIFORNIA – WESTERN DIVISION**

18 SOCIAL BICYCLES LLC d/b/a JUMP,
19
20 Plaintiff,
21
22 v.
23 CITY OF LOS ANGELES; CITY OF LOS
ANGELES DEPARTMENT OF
TRANSPORTATION,
24
25 Defendants.

Case No. 2:20-CV-02746

**COMPLAINT FOR INJUNCTIVE
AND DECLARATORY RELIEF
DEMAND FOR JURY TRIAL**

1 INTRODUCTION

2 1. This case arises from an effort by the Los Angeles Department of
3 Transportation to seize personal geolocation data about individual Angelenos as they go
4 about their daily lives.

5 2. Plaintiff Social Bicycles LLC d/b/a JUMP (“JUMP”) owns and makes
6 available to Angelenos a fleet of GPS-enabled electric scooters and pedal-assist bikes that
7 riders can locate on their smartphones, rent for short periods of time, and use to complete
8 short trips that might otherwise occur in a car. As a condition of doing business, Defendants
9 the Los Angeles Department of Transportation (“LADOT,” and with the City of Los
10 Angeles, the “City of Los Angeles,” or the “City”) compel dockless mobility operators like
11 JUMP to produce precise time-stamped geolocation data that tracks the location of their e-
12 bikes and e-scooters *in real time while riders are on them*.

13 3. While this data is not, on its face, connected to a particular user by name, phone
14 number, credit card, or other identifying information, LADOT or others can nonetheless use
15 historical time-stamped geolocation data to identify individual users’ travel patterns and
16 then connect those travel patterns to specific users, thereby “re-identifying” them. And if
17 seized in real time, this confidential and sensitive geolocation data enables LADOT to
18 electronically surveil dockless mobility users on a massive scale while they are on a trip.
19 LADOT’s large-scale seizure of private data is manifestly unlawful.

20 4. When given a chance to defend the public policy reasons underlying LADOT’s
21 requirement that JUMP provide time-stamped geolocation data in real time in front of an
22 administrative hearing officer, LADOT dissembled and its reasoning collapsed. At bottom,
23 LADOT and its witnesses could offer *no* reasoned policy basis for the seizure of dockless
24 mobility users’ intimate time-stamped geolocation data in real time. Because there is none.
25 *Real-time* in-trip geolocation data does not assist the City in planning bike lanes, or figuring
26 out deployment patterns in different neighborhoods, or dealing with complaints about
27 devices that are parked in the wrong place, or monitoring compliance with permit
28 requirements. It is a tool for surveillance.

1 5. LADOT’s data grab did not appear in a vacuum. In recent years, the agency
2 has engaged John Ellis, a “big data futurist,” as a consultant to help write the data-
3 acquisition rules at issue here. His private company, Ellis & Associates, was in turn
4 acquired by Lacuna—a venture-backed, for-profit entity. Ellis & Associates and Lacuna
5 stand to gain economically from the countrywide, potentially even worldwide, adoption of
6 data-acquisition rules similar to those Ellis & Associates wrote for LADOT because they
7 can bill themselves as the engineer of these data-acquisition rules, and therefore the best
8 consultants to help other cities implement similar data seizures. Moreover, Ellis &
9 Associates has charged Los Angeles for services promoting its data seizure programs (in
10 which Ellis and his company have a financial interest) around the country and abroad.

11 6. Working together, LADOT and Ellis & Associates have been strikingly candid
12 about their long-term and revolutionary aims: to “actively manage” bikes, scooters, and
13 ultimately cars, as part of a “radical, significant, and daunting” effort to affect a “significant
14 cultural transformation.” LADOT’s efforts, if allowed to continue, would fundamentally
15 change the relationship between citizens and their government. LADOT’s grandiose
16 plans—largely concocted and implemented out of public view—run roughshod over
17 fundamental legal and constitutional guarantees of privacy cherished by all Americans.

18 7. More specifically, LADOT’s mandatory conditions for participants in the
19 dockless mobility device market include a series of detailed code requirements set forth in
20 a document called the “Mobility Data Specification” (“MDS”), which lives in a technical
21 data room established for computer programmers called “Github” and is not easily
22 accessible to the public. LADOT changes the MDS on a whim. Indeed, LADOT initially
23 made the changes that are most fundamental to this complaint in a “webinar,” prepared and
24 delivered by its consultant just days before first-year permit applications were due and
25 which LADOT then modified a few weeks later by e-mail. When LADOT’s witnesses were
26 put under oath, even they struggled to identify an authoritative source for the MDS
27 requirements in connection with the then-operative one-year permit. It is difficult to
28

1 imagine that a member of the public could determine what data LADOT is collecting about
2 them.

3 8. The MDS requirements relevant here compel participants to build and
4 implement two specific “application program interfaces” (“APIs”). Generally speaking, an
5 API is a piece of code that allows two software systems to communicate with each other.
6 The two compulsory APIs at the center of this lawsuit are the “Provider API,” which came
7 first and provides historical information which LADOT can “pull,” and the “Agency API,”
8 which came later, goes much farther, and forces operators to automatically transmit, or
9 “push,” the data of its devices directly to LADOT. When implemented as currently required
10 by LADOT, these APIs provide LADOT and its consultants with a massive trove of
11 confidential data about JUMP’s devices and users, including precisely where each device
12 travels to and from, through which route, and at what time. Most troubling, LADOT
13 requires operators to transmit certain geolocation data about their dockless devices, such as
14 trip-start data, in real time *as riders use them*.

15 9. In recent years, the United States Supreme Court has warned of the grave
16 dangers of allowing the Government free-wheeling access to geolocation data like the data
17 that LADOT seizes pursuant to the MDS. In *Carpenter v. United States*, for example, the
18 Supreme Court astutely observed, in a detailed opinion by Chief Justice Roberts, that
19 geolocation data provides an “intimate window into a person’s life, revealing not only his
20 particular movements, but through them his ‘familial, political, professional, religious, and
21 sexual associations.’” 138 S. Ct. 2206, 2217 (2018). Similarly, in *United States v. Jones*,
22 Justice Sotomayor explained why this data raises such grave privacy concerns: the
23 “Government can store such records and efficiently mine them for information years into
24 the future,” and “because GPS monitoring is cheap in comparison to conventional
25 surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary
26 checks that constrain abusive law enforcement practices: ‘limited police resources and
27 community hostility.’” 565 U.S. 412, 415-16 (2012) (Sotomayor, J., concurring).

1 10. The Supreme Court has also been clear that businesses have a fundamental
2 privacy right in their business records, and thus must be given an opportunity for “pre-
3 compliance review” prior to the Government effectuating a compulsory search of those
4 records. *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2015). As a result, a
5 municipality may not compel a technology company to turn over its user data with a set of
6 “sweeping” requirements that are “devoid of any tailoring” to suspected wrongdoing,
7 especially without providing any opportunity for pre-compliance review. *AirBnb, Inc. v.*
8 *City of New York*, 373 F. Supp. 3d 467, 491 (S.D.N.Y. 2019). LADOT’s seizure of JUMP’s
9 proprietary time-stamped geolocation data, without any tailoring or opportunity for review,
10 thus runs headlong into the crossroads of two lines of clear and powerful Fourth
11 Amendment precedent.

12 11. Throughout LADOT’s creation and implementation of its dockless mobility
13 program, JUMP has repeatedly explained to LADOT the profound privacy risks inherent in
14 the collection of historical trip records, combined with time-stamped geolocation data
15 collected in real time, and has repeatedly raised objections to these requirements with
16 LADOT. JUMP’s pleas have been met with effective silence. And JUMP has made plain
17 that it does not believe that it can be lawfully compelled to transmit the real-time geolocation
18 data of its dockless devices. But with LADOT unwilling to budge, and JUMP’s business
19 in Los Angeles at stake, JUMP went as far as it believed it reasonably could to accommodate
20 LADOT’s demands: JUMP agreed to provide, and has been providing, trip-start, trip-end,
21 and route data at a 24-hour latency, *i.e.*, it has sent LADOT the required data but only twenty
22 four hours after a rider’s trip-start, trip-end, and route events occur. With this slight delay
23 in data production, there is at least a theoretical possibility that JUMP could seek to
24 challenge a specific LADOT request before complying, an opportunity unavailable where
25 LADOT requires data production in real time. Moreover, by providing geolocation data
26 after a 24-hour latency period, rather than in real time, JUMP has significantly mitigated
27 the frightening risks of direct and constant government surveillance or possible interception
28 of individual users. And JUMP has complied with every other aspect of LADOT’s

1 permitting regime, which includes the provision of extensive data about, for example, the
2 location of deployed devices that are parked and not being used by riders, as well as data
3 points such as battery level and maintenance status.

4 12. This was not good enough for LADOT. In fact, JUMP's vocal privacy
5 objections only appeared to make matters worse. On October 25, 2019, the agency issued
6 a notice suspending JUMP's permit in light of its failure to provide real-time data and
7 ordering the removal of its bikes and scooters from City streets within 72 hours, after which
8 the department of sanitation would begin rounding them up.

9 13. JUMP immediately gave LADOT notice that it would seek emergency judicial
10 relief to protect its permit and enforce its Fourth Amendment rights. In response, LADOT
11 capitulated on its threats to immediately remove JUMP's devices and hastily fashioned an
12 administrative review process (established without public notice and uncodified in any
13 statute, rule, or otherwise). LADOT allowed JUMP to remain on City streets during the
14 pendency of that process. That process ultimately consisted of a two-day hearing in which
15 multiple LADOT witnesses could offer *no* reasoned policy justification for compelling
16 production of trip data in real time, and in which JUMP vociferously argued, as it does here,
17 that the LADOT data acquisition rules violated, among other things, JUMP's Fourth
18 Amendment rights and CalECPA. Nonetheless, an LADOT hearing officer upheld the
19 suspension of JUMP's permit without addressing any of JUMP's arguments as to the
20 lawfulness of the MDS.

21 14. JUMP promptly notified LADOT that it intended to appeal the hearing
22 officer's decision to the LADOT Board of Transportation Commissioners, which was the
23 next step in LADOT's *ad hoc* suspension review process. The hearing was scheduled for
24 March 12, 2020, just three days before JUMP's one-year permit would expire and one day
25 before applications for a new six-month permit extension would be due. In light of the
26 approaching expiration of the one-year permits, and the growing threat posed by the
27 COVID-19 virus, JUMP and LADOT agreed to adjourn the Board appeal, that JUMP would
28 submit an application for a six-month extension permit, and that JUMP would agree to

1 comply with the disputed MDS data production requirements as a condition of receiving
2 that permit, while reserving any and all rights to challenge the legality of those
3 requirements. LADOT also agreed not to use JUMP's past technical non-compliance
4 against it in evaluating JUMP's application for a six-month extension permit. As of this
5 filing, JUMP's application for a six-month extension permit is pending—although JUMP
6 expects it to be granted in light of LADOT's assurances—and JUMP continues to operate
7 in Los Angeles.

8 15. JUMP now challenges LADOT's creation of, and efforts to enforce, the
9 MDS's real-time geolocation requirements, which trample on a slew of basic and
10 fundamental rights:

- 11 a. LADOT's warrantless seizure of JUMP's proprietary business records
12 constitutes an unreasonable search in violation of the Fourth Amendment
13 of the U.S. Constitution and Article 1, § 13 of the California Constitution,
14 as well as an unlawful compulsion of electronic records that violates and
15 is preempted by the California Electronic Communications Privacy Act,
16 Cal. Penal Code § 1546 *et seq.*
- 17 b. The City's unbounded delegation to LADOT to fashion rules that have
18 led to the seizure of JUMP's intimate geolocation data, and LADOT's
19 further re-delegation of that unbounded authority to for-profit, industry
20 participants, violated California's non-delegation doctrine.

21 **PARTIES**

22 16. Plaintiff JUMP is an LLC whose sole member, SMB Holding Corporation, is
23 a Delaware corporation with its principal place of business in California.

24 17. Defendant the City of Los Angeles is a municipal corporation organized and
25 existing under the laws of the State of California and is a charter city pursuant to Article XI
26 of the California Constitution.

1 18. Defendant LADOT is a government agency created by Los Angeles City
2 Ordinance whose “mission is to lead transportation planning, project delivery, and
3 operations in the City of Los Angeles.”

4 JURISDICTION AND VENUE

5 19. This Court has federal question jurisdiction over this action under 28 U.S.C.
6 § 1331 and 42 U.S.C. § 1983 because Plaintiff alleges violation of its rights under the
7 Constitution and laws of the United States.

8 20. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction over
9 Plaintiff’s claims arising under the California State Constitution and California state law
10 because they are so related to the federal claims asserted in this action that they form part
11 of the same case or controversy under Article III of the U.S. Constitution.

12 21. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because both
13 Defendants are residents of this district, and under 28 U.S.C. § 1391(b)(2) because a
14 substantial part of the events giving rise to Plaintiff’s claims occurred in this district and a
15 substantial part of property that is the subject of this action is situated in this district.

16 FACTUAL ALLEGATIONS

17 **I. JUMP’s Participation in the “Dockless Mobility” Market**

18 22. “Dockless mobility” devices, such as electric bikes and scooters (“e-bikes” and
19 “e-scooters,” respectively), are micro-mobility transportation devices that are not tethered
20 to fixed locations like docking stations. Rather, each dockless mobility device is equipped
21 with an electric battery, an integrated lock, and onboard GPS. Thus, using a smartphone
22 application, riders can locate available devices, begin their rides anywhere an available
23 device can be found, and end their rides at their precise destinations. As a result, users can
24 take these devices door-to-door or as a “last mile” solution connecting them to nearby
25 transportation hubs. Cities have had broad success with micro-mobility generally, including
26 dockless mobility, and its use has been growing rapidly.

27 23. JUMP operates a fleet of e-bikes and e-scooters and provides software enabling
28 riders to locate, reserve, use, and pay for them. JUMP was the world’s first electric-assisted

1 bikeshare company and is currently a major player in the dockless mobility market. Given
2 that each of its devices runs on an electric battery, JUMP must arrange for these batteries to
3 be charged, often overnight in JUMP's warehouse. It must also maintain the devices, which
4 requires that it pick up its deployed devices (or arrange for them to be picked up), and then
5 re-deploy them throughout the City, based on its business decisions to meet anticipated
6 demand or to comply with regulatory requirements, such as those designed to avoid over-
7 accumulation of devices in a particular area or to achieve equitable distribution targets. In
8 Los Angeles and in other cities, JUMP provides data to cities and to the public as to the
9 location of its available-for-rent devices.

10 24. Following a successful launch in San Francisco in early 2018, JUMP began
11 seeking opportunities around the country to expand its dockless mobility services. The City
12 of Los Angeles—with its large population, fair weather, generally-level topography, and
13 underdeveloped public transportation infrastructure—was an appealing location for
14 expansion. Thus, in the middle of 2018, JUMP began assessing a strategy for market entry.

15 **II. The City of Los Angeles' Development of a Regulatory Regime for Dockless** 16 **Mobility Devices**

17 **A. The City Tasks LADOT With Creating Rules for Dockless Devices**

18 25. In late 2017, after dockless devices (operated by other companies) began
19 appearing on City streets, LADOT asked the L.A. City Council to direct LADOT to draft
20 rules and regulations for a dockless bike share program. The City Council did so on
21 December 13, 2017.

22 **B. LADOT Partners with Ellis & Associates**

23 26. Shortly after being given authority to create rules for a dockless mobility
24 program, on March 9, 2018, LADOT signed a three-year contract with a for-profit
25 consultancy called Ellis & Associates. *See* [http://clkrep.lacity.org/onlinecontracts/2018/C-](http://clkrep.lacity.org/onlinecontracts/2018/C-130956_c_3-9-18.pdf)
26 [130956_c_3-9-18.pdf](http://clkrep.lacity.org/onlinecontracts/2018/C-130956_c_3-9-18.pdf); *see also* Laura Bliss, *Why Real-Time Traffic Control Has Mobility*
27 *Experts Spooked*, CityLab, Jul. 19, 2019, *available at* bit.ly/citylabMDS. Ellis & Associates
28 was retained to lead the LADOT's efforts in establishing a dockless mobility program.

1 27. Ellis & Associates is led by John Ellis, the former “chief technologist” of the
2 Ford Motor Company, and the author of a recent book describing how “[u]ser data mined
3 from vehicles – based on location, intentions and preferences – is gold to marketers and
4 money to anyone that can harvest, analyze, and process it.” John Ellis, *THE ZERO DOLLAR*
5 *CAR: HOW THE REVOLUTION IN BIG DATA WILL CHANGE YOUR LIFE* (2017). Ellis describes
6 himself as a “big data futurist,” and has produced an October 2017 “TEDx talk” at a TedX
7 event that was titled “Who’s in the Driver’s Seat? The Transformation of Transportation.”

8 28. In that TEDx talk, Ellis declares that “data is the new oil,” and that the
9 “transportation data bonanza is too big and too important to miss out.” Ellis describes
10 privacy as a mere obstacle to be overcome, recommending that we “accept the fact that
11 humans will be tempted to sell data and they will succumb to that temptation, and therefore
12 we should stop trying to regulate privacy and rather treat it as a product.”

13 29. On information and belief, in December 2019, Ellis & Associates sold itself to
14 Lacuna Technologies, a venture-backed entity which bills itself as a visionary civic mobility
15 company seeking to provide “[t]he missing link between public interest and private
16 innovation.” Although Lacuna portrays itself as independent, it is in fact controlled and
17 operated by individuals such as Ellis, who now, due to their work advising and writing rules
18 for agencies like LADOT, have deep ties to the municipalities with which they aim to
19 partner. Indeed, on information and belief, until just recently, Lacuna’s operatives,
20 including Ellis, publicly touted their insider status with municipalities, including LADOT,
21 in an effort to grow their venture-backed business.

22 30. The goals of Ellis & Associates and Lacuna are clear: first, they work through
23 their municipal partners and insiders to ensure that cities such as Los Angeles and others
24 seize as much lucrative data as possible from private industry. Then, Ellis & Associates
25 and Lacuna ensure that those cities allow them to access the data, with as few restrictions
26 on data use as possible, so that they can use it for the benefit of their own business. As Ellis
27 has himself stated: “The only thing that stands between us and the sale of our personal data
28 is in fact a policy . . . that can be easily overturned.”

1 31. Ellis & Associates and Lacuna stand to profit if cities beyond Los Angeles
2 adopt similar data sharing rules. Ellis & Associates and Lacuna can market themselves as
3 the engineers of the system and thus a key consultant partner for other cities, with a view
4 towards securing lucrative consultancy agreements like the one obtained from Los Angeles.
5 Worse still, Ellis & Associates and Lacuna could seek to monetize the user data they obtain
6 from such cities, subject only to limits placed on such data usage by these cities themselves.
7 And to the extent that Ellis & Associates and/or Lacuna seek to monetize the data that cities
8 compel from private entities like JUMP, they would in effect be competitors of those private
9 entities, while still crafting the very rules mandating and governing the seizure of that data.

10 32. In fact, Ellis & Associates has already profited handsomely from its
11 relationship with LADOT. And not just from its seven-figure contracts, but also by
12 leveraging its contractual relationship as an opportunity to “coach” and “train” LADOT
13 personnel on the “values and key messaging” behind LADOT’s grandiose efforts. Notably,
14 for these training and coaching sessions, LADOT paid Ellis & Associates \$60,000. Ellis
15 has also invoiced LADOT for his efforts to promote MDS in other cities across the country
16 and abroad.

17 33. Among Ellis & Associates’ first tasks for LADOT was drafting the rules that
18 the City Council directed LADOT to make. LADOT shared its proposed rules with the City
19 Council on May 18, 2018. Next, Ellis & Associates was tasked with preparing LADOT’s
20 “Strategic Implementation Plan: A Plan to realize the visions outlined in the *Urban Mobility*
21 *for a Digital Age* and *Blueprint for Autonomous Urbanism* documents” (the “Strategic
22 Implementation Plan”), which was released in June 2018.

23 34. The Strategic Implementation Plan is a striking document—by its terms, it
24 outlines a “radical, significant, and daunting” plan to transform the relationship between
25 LADOT and City residents. It imagines a “next-generation urban mobility system,” referred
26 to as “Transportation 2.0.” According to the Strategic Implementation Plan, “[t]he
27 foundation of Transportation 2.0 is that LADOT will explicitly manage the movement of
28 vehicles in the Los Angeles transportation product.” The Strategic Implementation Plan

1 acknowledges (if significantly understates) the fact that Transportation 2.0 would be “a
2 marked departure from the current policy context of managing the movement of people and
3 goods through the system.”

4 35. Indeed, Transportation 2.0 is part of a self-described “significant cultural
5 transformation” that LADOT and its consultants intend to affect, and which would work to
6 their financial benefit. “Transportation 2.0 is an umbrella term that encapsulates the
7 creation and convergence of dozens of disruptive technologies.” In the Strategic
8 Implementation Plan, LADOT and its consultants claim to be “aware of the unintended
9 ways this will change our culture and world at large,” and identify several ways to meet the
10 demands of this “cultural transformation,” including the creation of a new “shared
11 *language*” and “[r]eaching for new *values*.”

12 36. A central component of Transportation 2.0 is what the Strategic
13 Implementation Plan calls “Active Management.” “Active Management” refers to the
14 ultimate goal of taking broad control over the movement of people throughout Los Angeles.
15 According to the Strategic Implementation Plan, “[c]ontrol is a fundamental aspect of
16 today’s transportation network and will become even more critical in the future,” and so
17 LADOT wants “a radically different and faster approach to control.” In practice, “Active
18 Management” reflects LADOT’s effort to position itself so that it can physically control a
19 broad array of transportation devices, even as users ride them, starting with bikes and
20 scooters and ultimately expanding to driverless cars and beyond.

21 37. The touchstone of LADOT’s Active Management plan is “[b]uild[ing] a solid
22 data foundation.” To do this, LADOT intends to effect a massive seizure of confidential
23 and sensitive real-time data from private entities that have acquired that proprietary data
24 after significant resource investment, including the building of costly infrastructure. The
25 Strategic Implementation Plan boldly envisions seizing that data directly from private
26 industry participants such as JUMP, as well as JUMP’s parent company, Uber, which the
27 SIP refers to collectively as the “Transportation Technology Bench.”

28

1 38. In short, the large-scale seizure of private data that gives rise to this lawsuit
2 seems to be only the beginning.

3 **C. Ellis & Associates Creates the “Mobility Data Specification” for LADOT**

4 39. To take the first step outlined in the Strategic Implementation Plan, LADOT
5 tasked Ellis & Associates with writing a “new data language”: the Mobility Data
6 Specification, or “MDS.” *See Bliss, Mobility Experts Spooked.* This new language was the
7 tool that LADOT would ultimately use to seize reams of sensitive data from dockless
8 mobility providers such as JUMP.

9 40. The MDS, as implemented, forces dockless mobility providers to write code
10 into their systems that provides LADOT unfettered, on-demand, and real-time access to
11 private time-stamped geolocation data about each and every device, including when riders
12 are on them.

13 41. More specifically, the MDS consists of a “data specification”—a set of
14 requirements for the types of data that can be stored in a particular database—and centers
15 on application programming interfaces (“APIs”). APIs are common amongst programmers
16 and are essentially pieces of software (*i.e.*, a set of code) that allow one software application
17 to communicate with another (*e.g.*, an operating system or another application). At a basic
18 level, APIs work by defining the rules and methods for one piece of software to issue
19 commands to, request information from, or submit information to, another piece of
20 software.

21 42. Ellis & Associates first created what it called the “Provider API,” which
22 requires dockless mobility operators to collect data and make it available in a segregated
23 database, and then allows LADOT to query that data on demand, often called a “pull”
24 technology. JUMP refers to this internally as the “Provider” database.

25 43. Most relevant here, and in its present incarnation, the Provider API enables
26 LADOT and its consultants to make queries about individual “trips,” a technical term of art
27 that refers to a bundle of data points about a ride taken by a customer, including (i) the
28 Provider ID, (ii) the unique ID of the vehicle, (iii) the distance and duration of the trip,

1 (iv) the cost of the trip, (v) the precise, time-stamped start and end points of the trip (referred
2 to herein as “trip-start” and “trip-end” events), and (vi) time-stamped GPS “breadcrumbs”
3 showing the precise route traveled by the rider (referred to herein as “route data” or “route
4 events”).¹

5 **D. With LADOT Armed with the MDS and the Provider API, the City**
6 **Formally Delegates Dockless-Mobility Regulatory Authority to LADOT**

7 44. In September 2018, the L.A. City Council passed an ordinance authorizing
8 LADOT to implement and issue rules for a pilot permit program for dockless mobility
9 operators. The ordinance, codified at § 71.29 of the L.A. Administrative Code (the
10 “Ordinance”), provided broad and unbounded authority to the LADOT. Specifically, it
11 provided in relevant part:

12 [LADOT] shall implement a Shared Mobility Device Pilot Program, and
13 issue a permit to a qualified pilot program operator, as defined in the
14 Department’s Rules and Guidelines, including, but not limited to, an
15 operator of a dockless bicycle, electric bicycle, motorized scooter and
16 electric scooter. Under the Pilot Program, an operator of a shared
17 mobility device shall obtain a permit from the Department and comply
18 with all Department permit rules, regulations, indemnification, insurance
19 and fee requires set forth in the Department’s Rules and Guidelines.
20 Failure to comply with the Department’s Rules and Guidelines may result
21 in the suspension, revocation, or a reduction of the number of permits
22 issued by the Department to an operator. The Department may amend its
23 Rule and Guidelines as necessary during the life of the Pilot Program.

24 45. Section 71.29 also contained an “Urgency Clause” stating that the Ordinance
25 “is required for the immediate protection of public peace, health and safety” because
26

27 ¹ Throughout this Complaint, JUMP generally refers to the requirements imposed by the MDS that
28 operators provide trip-start, trip-end, and route data to LADOT as the “MDS geolocation
requirements.”

1 “[m]any people are currently operating shared mobility devices in the City of Los Angeles
2 without regulations, which are needed to protect the health and safety of the public.” The
3 sole “health and safety” issues identified in the urgency clause, however, were “the
4 placement or parking of shared mobility devices,” as well as “safe speed limits for the
5 operation of shared mobility devices.”

6 46. At no time did the L.A. City Council call for, let alone authorize, a program
7 under which LADOT could compel sensitive data from providers in real time. Section
8 71.29 is silent as to LADOT’s authority to compel operators under the program to produce
9 proprietary data as a condition of operating a dockless mobility device. Nor does the
10 Ordinance make any reference to the MDS. Indeed, the sole reference to “data” within the
11 Ordinance comes in a singular prefatory “WHEREAS” clause, stating that “by
12 implementing the pilot program, the City intends to study the data collected during the pilot
13 period to ensure safe and equitable access, maintenance and operations, to determine proper
14 fleet size in various locations within the City, and to fine tune and update the current rules
15 and regulations in real time to ensure compliance with local and state laws, including the
16 development of data programs to aid in enforcement, and to prevent the accumulation of
17 devices on sidewalks or other public rights-of-way.”

18 **E. LADOT Releases Initial Applications for the Program**

19 47. On October 1, 2018, pursuant to the sweeping—indeed, unbounded—authority
20 delegated to it by the Ordinance, LADOT released applications for 120-day conditional
21 permits to be issued to dockless mobility providers. The applications included a draft of
22 the program’s Rules and Guidelines, which mandated compliance with the MDS.
23 Specifically, the Rules and Guidelines provided that all operators must abide by the MDS
24 and that “the City may, in its sole discretion, release subsequent versions and/or updated
25 versions of the [MDS] and require Operators to use the most current version by releasing
26 an automatic update.” The rules also provided a non-exhaustive list of grounds on which
27 LADOT could terminate permits. A “failure to share data” and a “[f]ailure to abide by the
28 Mobility Data Specification” were listed grounds for LADOT to terminate a permit.

1 48. LADOT's sole means of making the specific required MDS code known to
2 providers and the public was by posting detailed requirements, often including specific
3 code, on a website called GitHub. GitHub is a coders' dataroom known to experienced
4 computer programmers but virtually unknown, confusing, and effectively inaccessible to
5 the general public. Moreover, as a general matter, applicants and providers were not (and
6 are not) informed directly when revisions to the MDS were made. For example, LADOT
7 informed JUMP as part of its application that "for the upcoming 1 year permit, we will
8 require a more up-to-date version of MDS," and that the company should "[k]eep an eye on
9 the MDS GitHub page for updates."

10 49. Further, as alleged above, applicants were required to agree to *any* unforeseen
11 future versions of the MDS, leaving operators entirely unaware of what LADOT's specific
12 intentions (and operators' specific obligations) might be. Specifically, LADOT required
13 applicants to agree that the "City may, in its sole discretion, release subsequent versions
14 and/or updated versions of the Specification and require Operators to use the most current
15 version by releasing an automatic update and/or disabling support for the previous version."
16 In effect: we can do whatever we want, whenever we want, however we want, and you will
17 have no choice but to comply.

18 **III. JUMP's Application for a 120-Day Permit**

19 50. JUMP had significant concerns about the breadth of the MDS requirements
20 even in their first incarnation, where only the Provider API was unveiled, and JUMP voiced
21 certain of these concerns in an open letter to LADOT on October 9, 2018, just days after
22 the program applications were released. In that letter, JUMP informed LADOT that the
23 "MDS requires production of certain categories of location data that may unintentionally
24 endanger rider privacy without specifying how that data will be secured, stored, and used
25 by LADOT." Although JUMP reluctantly stated without choice that it would be "prepared
26 to implement the Provider API in compliance with the MDS," it implored LADOT to "abide
27 by the following data protection principles": "1. Security of Trip Data must be maintained
28 by LADOT"; "2. Uses of Trip Data should be limited and communicated to riders"; "3. Trip

1 Data should be obfuscated when stored at rest”; and “4. Additional data sharing must be
2 restricted.” LADOT took no action on any of these pleas.

3 51. A week later, and with these concerns in mind, on October 19, 2018, JUMP
4 applied for a 120-day permit pursuant to the program, proposing a fleet of 1,000 scooters
5 and 2,000 e-bikes. Because it had no choice, JUMP “commit[ted] to meeting all applicable
6 Rules and Guidelines” outlined above and certified its compliance with the program’s tax,
7 insurance, and indemnification requirements. JUMP also certified its compliance with the
8 program’s “Data Sharing Requirements” by submitting “proof of compliance for the
9 Conditional Permit MDS implementation in Los Angeles” in the form of a verification from
10 the City.

11 52. JUMP would not have complied with the MDS requirement to build out or
12 implement the Provider API were doing so not a required condition for the receipt of a
13 permit under the program, which is required to do business in Los Angeles.

14 53. On November 9, 2018, LADOT approved JUMP’s application for a 120-day
15 permit.

16 **IV. LADOT Introduces the “Agency API” Through a “Webinar”**

17 54. On February 7, 2019, as JUMP’s 120-day permit was expiring, and just over a
18 week before applications for follow-on one-year permits were due, Ellis & Associates
19 presented a “webinar,” which was posted on Github, titled “MDS & One Year Permitting
20 Overview.” Through this “webinar,” LADOT announced for the first time that it was
21 unveiling a new API that would be mandatory in connection with the one-year permit: the
22 “Agency API.”

23 55. Although the details were not clear at first, the Agency API ultimately went
24 significantly further than the Provider API. It requires JUMP and other dockless mobility
25 operators to generate a feed of trip geolocation data and send it, or “push” it, to LADOT
26 and its chosen recipients automatically and in real time, *i.e.*, when the events creating the
27 data points occur. Critically, the Agency API presently requires providers to report trip-
28 start time (*i.e.* when there is an individual on the device) and location and trip-end time and

1 location data for each vehicle trip within *5 seconds* of the trip’s start and end, followed by
2 detailed route data within 24 hours. These specific timing requirements were not in the
3 MDS itself during the relevant period for the one-year permit, but could be found solely in
4 the Ellis & Associates “webinar” posted in the Github. The underlying data specification
5 includes the vehicle’s unique ID number, the vehicle’s position, and its heading and speed
6 (calculated using GPS). Time and location data points must be reported for every 300 feet
7 while a vehicle is moving and every 30 seconds while at rest.

8 56. Essentially, the Agency API requires dockless mobility providers to give the
9 City a real-time feed of intricately detailed, time-stamped geolocation data about individual
10 bikes and scooters while riders are using them. The Agency API thus allows LADOT near
11 immediate and unchecked access to down-to-the-second information about JUMP riders
12 that LADOT and its consultants can use to track and surveil citizens on a massive scale.

13 57. On information and belief, the Agency API is the broadest suspicionless
14 demand for individual trip data that any government entity has ever imposed on a mobility-
15 service provider. Simply put, it is unprecedented.

16 58. Moreover, as alleged in the following section, the data that LADOT can, does,
17 and will seize pursuant to the Agency API—and which ends up in the hands of entities like
18 Ellis & Associates and Lacuna—can be some of the most sensitive data of JUMP’s users,
19 especially when collected over extended periods of time.

20 **V. LADOT’s Data Collection Practices Risk Re-identification and Surveillance of** 21 **Individual Users**

22 59. The extensive amount of data that LADOT seizes, both in real time and on a
23 historical basis, provides LADOT with various means to first identify and then surveil and
24 even intercept residents, oftentimes in deeply intimate and private aspects of their lives.

25 60. At the outset, LADOT is (and has been since the Fall of 2018) building a
26 massive historical database of trips at a trip-specific level, showing not only the start and
27 end locations and times of the trips, but also the precise routes taken, and even the speed
28 travelled moment-to-moment throughout the trip. LADOT, or anyone else with access to

1 this database of historical trips, can sort the data to identify travel patterns. For example,
 2 LADOT may see in the data a series of trips that end in front of a particular house. LADOT
 3 can then look at readily available information (such as home address information) to see
 4 who lives in that house, and thus who is likely taking the trips that end there. LADOT
 5 would then know where that person is starting trips, which may be at the person's doctor's
 6 office or any other location which the rider might have an interest in keeping private.
 7 LADOT would likewise be able to review trips starting at that house and see where they
 8 end, which likewise may reveal personal information. In this manner, LADOT could gather
 9 detailed information about a person, such as where they live and work, where they go for
 10 social or romantic interactions, and even what time they leave their office each day.

11 61. Numerous studies and research papers have demonstrated the risk that precise,
 12 individualized geolocation data such as that compelled by the MDS can be used to re-
 13 identify and reveal specific information about individuals:

- 14 i. A report published in Nature found that 95% of individuals can be identified
 15 using only four spatiotemporal data points.²
- 16 ii. In 2014, an analyst used Freedom of Information laws to obtain all NYC taxi
 17 records for the previous year, including pickup and drop-off GPS and other data.
 18 Even though the dataset was "anonymized," and no specific rider or driver
 19 identifiers were shared, researchers were able to identify the patrons of a strip
 20 club by cross-referencing the taxi records against other publicly available
 21 information.³

23 ² Yves-Alexandre de Montoye et al., *Unique in the Crowd: The privacy bounds of human*
 24 *mobility*, 3 NATURE 1, 2 (2013), <https://www.nature.com/articles/srep01376>. A similar study
 25 identified 30-50% individuals in an anonymized dataset with 10 additional pieces of
 26 metadata. Chris Y.T. Ma et al., *Privacy Vulnerability of Published Anonymous Mobility*
Traces, 21 IEEE/ACM TRANSACTIONS ON NETWORKING 1, 1 (2013),
<https://www.osti.gov/servlets/purl/1095747>.

27 ³ Chris Gayomali, *NYC Taxi Data Blunder Reveals Which Celebs Don't Tip - And Who*
Frequents Strip Clubs, FAST COMPANY (Oct. 2, 2014),
 28 [https://www.fastcompany.com/3036573/nyc-taxi-data-blunder-reveals-which-celebs-dont-](https://www.fastcompany.com/3036573/nyc-taxi-data-blunder-reveals-which-celebs-dont-tip-and-who-frequents-strip-clubs)
[tip-and-who-frequents-strip-clubs](https://www.fastcompany.com/3036573/nyc-taxi-data-blunder-reveals-which-celebs-dont-tip-and-who-frequents-strip-clubs) (last accessed Mar. 13, 2020).

1 iii. Most recently, researchers at the Massachusetts Institute of Technology
2 conducted an analysis of user “matchability” in two large-scale datasets from
3 Singapore—one from a mobile network operator and one from a local
4 transportation system. They built a model that could match around 17% of
5 individuals with just one week’s worth of data, and more than 55% of
6 individuals after one month of collected data.⁴

7 62. This research plainly demonstrates that the volume of data LADOT collects
8 pursuant to the MDS—millions of timestamped, geolocation coordinates of individual
9 trips—is highly prone to re-identification and the subsequent tracking of individuals as they
10 go about their daily lives.

11 63. As a governmental entity, LADOT’s maintenance of this trove of sensitive data
12 raises further concerns about surveillance through re-identification. For instance, if the Los
13 Angeles Police Department knows that a community group focused on opposing police
14 brutality meets at a certain location every other Thursday until 7:00 p.m., the Police
15 Department could review historical trip records to see where people who leave that meeting
16 at 7:00 p.m. next travel to following the meeting. This information would thus in turn allow
17 the police department to determine the identity of those attending the meetings by, for
18 example, cross-referencing other sources of information to determine who lives in the
19 houses to which the attendees traveled.

20 64. Further, while the historical trip data that LADOT is collecting allows for a
21 massive re-identification effort and thus presents serious privacy concerns, the real-time
22 data requirement LADOT imposes adds another level of intrusion. It allows LADOT to
23 move beyond simply learning of its citizens’ movement patterns, and into surveilling them
24 in real time.

25
26
27
28 ⁴ See Dániel Kondor et.al., *Towards matching user mobility traces in large-scale datasets*,
IEEE TRANSACTIONS ON BIG DATA 1,1, 3 (2017), <https://arxiv.org/pdf/1709.05772.pdf>

1 65. For example, as alleged above, LADOT could determine based on historical
2 data that a specific person rides a scooter to a particular place each morning along a
3 particular route. LADOT could then cross-reference the real-time data feed it forces
4 operators like JUMP to provide, *i.e.*, it could use the real-time trip-start data to see when
5 that specific individual starts a trip, very likely on her way to her habitual destination. Such
6 information—route and destination, coupled with real-time trip-start data—would allow the
7 government to, for example, intercept that person off the street or follow her with a
8 surveillance drone.

9 66. For these reasons, the combination of LADOT’s collection of historical trip
10 data with the mandatory production of trip data in real time permits LADOT unprecedented
11 capability to surveil and monitor citizens that use micro-mobility devices. Such
12 surveillance and monitoring will only become easier as the data sets grow ever larger, giving
13 the City more pieces of the puzzle. Consequently, over time, the data seized through the
14 MDS requirements will provide the City, and whatever law enforcement, commercial, non-
15 governmental actors, or consultants that the City gives or sells the data to, a simple method
16 for tracking the comings-and-goings of large numbers of City residents on an unprecedented
17 scale.

18 67. For example, City actors (or non-governmental actors to whom the City either
19 intentionally or unintentionally provides the data) could easily use the compelled data to
20 uncover that:

- 21 i. Individual A, a psychotherapy patient, takes a JUMP bike every Friday from his
22 residence to his therapist’s office and, one hour later, returns to the same
23 residential address.
- 24 ii. Individual B, a pregnant high school senior, regularly takes a JUMP bike to her
25 obstetrician’s office after soccer practice, and then back home.
- 26 iii. Individual C, a City employee, travels from his home to his government office
27 by JUMP bike, and also at times travels from home or work to the office of the
28

1 *Los Angeles Times* as part of his efforts to blow the whistle on official
2 misconduct.

3 iv. Individual D, a restaurant employee, flees her place of employment on a JUMP
4 bike in fear following a raid by immigration authorities.

5 v. Individual E, a City employee, usually takes a JUMP bike home after work; on
6 some days he goes instead to a local medical marijuana store on his way home
7 from work.

8 vi. Individual F, a member of a religious mosque, uses a JUMP bike to travel
9 between her home and her religious services.

10 68. The City’s unchecked ability to track the movements of its residents raises
11 additional concerns when it comes to law enforcement (or criminal actors who might come
12 into possession of the MDS data). The data seized pursuant to the MDS would be an
13 invasive new tool to surveil, track, and investigate millions of people completely outside
14 the constitutionally mandated warrant and subpoena process. For example, law
15 enforcement could track all users who pass through an intersection known to be frequented
16 by drug traffickers, and in doing so, track the movements of an untold number of City
17 residents of whom the officer lacks any suspicion of criminal activity.

18 69. In recent years, the Supreme Court has expressed deep concern about the
19 government’s seizure of geolocation data. In *United States v. Jones*, for example, Justice
20 Sotomayor noted that “GPS monitoring generates a precise, comprehensive record of a
21 person’s public movements that reflects a wealth of detail about her financial, political,
22 professional, religious, and sexual associations. . . . The Government can store such records
23 and efficiently mine them for information years into the future. And because GPS
24 monitoring is cheap in comparison to conventional surveillance techniques and, by design,
25 proceeds surreptitiously, it evades the ordinary checks that constrain abusive law
26 enforcement practices: ‘limited police resources and community hostility.’” 565 U.S. 400,
27 415-16 (2012) (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)).

1 70. Similarly, in *United States v. Carpenter*, the Court confirmed that “GPS
2 information . . . provides an intimate window into a person’s life. . . . These location records
3 hold for many Americans the privacies of life . . . [and] is remarkably easy, cheap, and
4 efficient compared to traditional investigative tools. With just the click of a button, the
5 Government can access each carrier’s deep repository of historical location information at
6 practically no expense.” 138 S. Ct. 2206, 2217-18 (2018) (quotation marks omitted).

7 71. These concerns are paramount here, but LADOT has repeatedly refused to take
8 them seriously. When JUMP applied for and received its one-year permit in 2019, the
9 operative rules governing the MDS requirement placed no limitations on the purposes for
10 which LADOT may use the data it seizes pursuant to its dockless program. Indeed, the
11 “City [was] permitted to use all data the Operator provides in accordance with the
12 Specification.” And LADOT reserved the right to “share data collected with third parties”
13 so that it could “process and analyze data,” whatever that may mean. Further, “[t]hird
14 parties [were] permitted to republish any data the City publishes.” And as alleged above,
15 there were no limitations on the monetization of the providers’ data, either by the City or
16 by non-governmental actors that republish the providers’ data. Put simply, the City was
17 free to hand this data to law enforcement or sell it to private parties, who can then do with
18 that deeply-intimate data whatever they wish.

19 72. In March 2019, LADOT published a set of non-binding “Data Protection
20 Principles,” which purported to address some (but certainly not all) of these concerns. But
21 as JUMP and privacy rights advocates made clear to LADOT at the time, these Data
22 Protection Principles are inadequate to protect JUMP’s users. Among other things, the they
23 fail to: (i) recognize that user trip data is “personally identifiable data” that can be used to
24 reidentify individual riders; (ii) place any restrictions on how LADOT plans to use user trip
25 data; (iii) delineate how long LADOT will retain raw data about users or when and how
26 LADOT would destroy such data; (iv) explain what data security controls, and data breach
27 protocols, LADOT would implement to protect user data; and (v) precisely address whether
28 and under what circumstances LADOT would share this data with law enforcement. What

1 is more, even these high-level, non-specific “Principles” remained non-binding for months
2 during the life of JUMP’s initial one-year April 2019 Permit.

3 73. Nevertheless, in November 2019, the L.A. City Council endorsed LADOT’s
4 Data Protection Principles and directed LADOT to incorporate them into the Rules and
5 Guidelines for programs that use MDS. Accordingly, when LADOT recently released its
6 applications for a six-month permit extension in March 2020, LADOT (for the first time)
7 expressly committed itself to abide these Principles when it collects data through the MDS.
8 Nonetheless, LADOT’s rules still fail to meaningfully address the serious confidentiality
9 and privacy concerns inherent in its compelled data collection under the MDS. Besides
10 gesturing to the vague and inadequate March 2019 Data Protection Principles—the
11 shortcomings of which LADOT was aware of for months—the program’s Rules and
12 Guidelines remain inadequate and insufficient with respect to confidentiality, data
13 protection, and data retention.

14 74. Given the opacity of LADOT’s promulgation of the MDS rules—including its
15 initial reliance on GitHub as the sole method of publishing the MDS’s requirements—many
16 dockless mobility users might be entirely unaware of the scope of information about them
17 that is being seized by LADOT. Indeed, as alleged above, the requirement that operators
18 provide data to LADOT in real time was originally announced on a “webinar” presented to
19 dockless mobility operators. Consequently, the psychotherapy patient, the pregnant high
20 school student, the whistleblower, the restaurant employee in fear of immigration
21 authorities, the medical marijuana consumer, and the mosque-goer, to name a few examples,
22 might well have no idea that the City can watch as they start and end trips, in real time, in
23 granular detail, and with the benefit of a trove of historical trip data.

24 75. LADOT does not need the data compelled by the MDS to serve any essential
25 functions or for any proper and lawful purpose. As alleged further below, when LADOT
26 was given an opportunity to explain the need for MDS requirements as to geolocation in
27 real time, it came up empty. It did not identify a single public policy justification for those
28 MDS requirements.

VI. JUMP's Application for a One-Year Permit

76. When LADOT announced the rough contours of the Agency API for the first time through the February 7, 2019 webinar (including its demand for operators to provide real-time geolocation data of its devices), JUMP and others immediately raised vociferous privacy objections. Subsequently, JUMP and LADOT (along with other stakeholders, privacy advocates, and city officials) negotiated certain terms of the one-year permit.

77. While those negotiations were ongoing, JUMP submitted an application for a full one-year permit on February 15, 2019. The permit application forms appended essentially the same Rules and Guidelines as were released with the 120-day permit application, *see supra* at ¶ 47.

78. In its application, JUMP again (reluctantly) verified its intention to comply with the then-operative version of the MDS (as was required), but at that time the MDS itself still only required compliance with the Provider API, which did not contain a real-time requirement. And JUMP stated in its application for a one-year permit: “JUMP is currently compliant with the Mobility Data Specification (MDS) Provider v 0.3.0, and will continue to remain compliant with this data sharing requirement.” JUMP also informed LADOT in its application that it intended to collaborate on a going-forward basis with LADOT “to improve upon the Provider API and any other required APIs to develop additional privacy protections for sensitive data.”

79. After JUMP submitted its application, but prior to that application being approved, LADOT conceded that it would offer a modest limitation to the timing requirements associated with the Agency API. Originally, LADOT purported to require that all trip-data, which includes route data (again, the “breadcrumbs” of an exact route taken by a device while on a trip), be sent in real time every five seconds. On March 6, 2019, however, LADOT notified JUMP via e-mail that it was “removing the in-ride five-second telemetry reporting requirement from our One Year Dockless Mobility Permit requirements,” meaning that it would accept this route data (which it referred to as “telemetry” data) within a 24-hour window.

1 80. On April 15, 2019, JUMP obtained a permit to operate its dockless mobility
2 service in Los Angeles pursuant to the one-year program.⁵ As it had during the period in
3 which it operated under the 120-day permit, however, JUMP continued to express strong
4 concerns to LADOT about any requirements to produce sensitive trip data in real time.

5 81. On May 17, 2019, after LADOT had been operating its dockless program for
6 more than six months, LADOT issued a document entitled “MDS & One-Year Permitting:
7 MDS Agency API Technical Compliance Overview,” which, on information and belief,
8 was drafted by and presented to providers by Ellis & Associates. That document
9 endeavored more specifically to “define[] MDS compliance,” and purported to be “the
10 authoritative source for MDS Agency API compliance.” Most relevantly, the document
11 stated that (i) operators must produce time-stamped geolocation trip-start data “within 5
12 seconds of a user unlocking the vehicle for use,” thus effectively in real time; (ii) operators
13 must similarly produce time-stamped geolocation trip-end data “within 5 seconds of a user
14 ending a trip,” thus also effectively in real time; and (iii) “[t]rip telemetry data must be
15 provided via the telemetry endpoint (/vehicles/telemetry) during the trip or within 24 hours
16 of trip completion.”

17 82. JUMP continued to object to, and not comply with, any requirement to push to
18 LADOT time-stamped geolocation data at a five-second latency, which was a vastly over-
19 invasive and unprecedented demand. Subject to these repeated invocations of its objections
20 to real-time production of its sensitive trip data, JUMP agreed to (and did) provide trip-start,
21 trip-end, and route data at a 24-hour latency (meaning 24 hours after the relevant events
22 occurred), and continued to substantially comply with the LADOT permitting rules,
23 including all other MDS requirements.

24
25
26
27 ⁵ On February 12, 2020, LADOT recommended that the L.A. City Council extend the current
28 one-year permits for an additional six months, which would extend permits under the
program through September 15, 2020.

1 83. JUMP would not have complied with the MDS requirements to build out the
2 Agency API, or to provide trip-start, trip-end, or route data (even at a latency of 24 hours),
3 were compliance not a required condition for the receipt of a permit under the program.

4 84. For the next several months, LADOT—often represented not just by public
5 officials but by representatives of Ellis & Associates, often using LADOT.gov e-mail
6 addresses—and JUMP communicated from time to time by email and in telephone
7 conferences. Certain of these routine communications at times related to LADOT’s view
8 that JUMP was not in compliance with the requirements that it provide trip-start and trip-
9 end events within five seconds (and that it was not producing route data at *exactly* within
10 24 hours).

11 85. Throughout this same period (the summer of 2019), Ellis & Associates
12 continued their practice of providing LADOT with “Weekly Status Reports,” listing their
13 “Accomplishments,” “New Requests,” and “Priorities.” These reports documented
14 operators’ compliance with the mobility program’s technical requirements such as MDS.
15 For example, on July 12, 2019, Ellis & Associates reported as one accomplishment that it
16 had “[c]ompleted technical Compliance meetings with Spin, Lyft, and Wheels,” three of the
17 other eight program operators. Notably, Ellis & Associates then reported to LADOT that
18 at that time “Spin and Lyft are the first two providers *close* to technical compliance.”

19 86. Also during this period, JUMP continued to repeatedly inform LADOT (and
20 Ellis & Associates) that it had serious privacy objections to being compelled to turn over
21 time-stamped geolocation trip-start and trip-end data points at a five-second latency,
22 principally because they effectively required JUMP to transmit the geolocation data of its
23 users in real time, *i.e.*, as they were riding them.

24 **VII. The Legislative Counsel Bureau Concludes LADOT’s Rules Are Unlawful**

25 87. On August 1, 2019, California’s Legislative Counsel Bureau issued an opinion
26 letter explaining in effect that the requirements that LADOT was imposing violate the newly
27 enacted California Electronic Communications Privacy Act (“CalECPA”). Specifically, the
28 Legislative Counsel Bureau opined that:

1 CalECPA restricts a department of a city or county from requiring a
2 business that rents dockless bikes, scooters, or other shared mobility
3 devices to the public to provide the department with real-time location
4 data from its dockless shared mobility devices as a condition of granting
5 a permit to operate in the department's jurisdiction.

6 88. On August 15, 2019, LADOT issued a public response to the Legislative
7 Counsel Bureau's opinion. Specifically, it filed a memorandum with the City Council
8 stating that it disagreed with the Legislative Counsel Bureau, and taking the remarkable
9 position that CalECPA does not apply to LADOT at all.

10 **VIII. LADOT's (Unlawful) Revocation of JUMP's Permit**

11 89. On October 8, 2019, after JUMP had participated in LADOT's permitting
12 programs for nearly a year, and after JUMP had repeatedly voiced its well-founded and
13 serious privacy concerns which had by then been endorsed by the California Legislative
14 Counsel Bureau, LADOT sent a letter threatening to revoke JUMP's permit for failing to
15 produce trip-start and trip-end data in near real time, and for not always delivering route
16 data through the Agency API exactly within 24 hours from the completion of a
17 ride. LADOT's letter relied on "the technical compliance guidelines outlined in 'MDS &
18 One-Year Permitting: MDS Agency API Technical Compliance Overview' document [*sic*],
19 first presented and published in the Mobility Data Specification (MDS) webinar on
20 February 7, 2019."

21 90. After some back-and-forth between JUMP and LADOT, after business hours
22 on Friday, October 25, 2019, LADOT announced that it was suspending JUMP's permit
23 effective 5:00 p.m. on Monday, October 28, 2019. Specifically, LADOT stated that it "will
24 issue a notice of suspension," "take action to collect on the performance bond that was
25 required as a condition of your permit, require the immediate suspension of all rentals
26 through your application, and require the removal of any of your dockless mobility vehicles
27 operating within the City of Los Angeles."

1 91. As LADOT’s letter seemed designed to prevent JUMP any opportunity from
2 seeking relief in advance of LADOT taking aggressive action the following Monday, JUMP
3 took the unusual step of giving notice on a Sunday—October 27, 2019—that it would seek
4 emergency injunctive relief *ex parte* in court the next morning. LADOT then took the
5 position in an October 27, 2019 e-mail that JUMP’s notice was ineffective because it was
6 sent on a Sunday and without sufficient notice, even though LADOT had itself created the
7 conditions—*i.e.*, suspending JUMP’s permit on a Friday—that required notice at that time.

8 92. LADOT, however, then backed away from its threat to immediately remove
9 JUMP’s devices from the streets and permitted JUMP to continue operating pending a
10 newly announced, undefined, and uncodified “administrative process” that LADOT
11 envisioned “relative to the dockless program permit, including the opportunity to request
12 an administrative hearing to appeal a permit suspension before the Los Angeles Board of
13 Transportation Commissioners.” The following day, LADOT issued a letter temporarily
14 suspending JUMP’s one-year permit and providing limited details to JUMP about its *ad hoc*
15 administrative review process that it was inventing on the fly.

16 93. On October 28, 2019, JUMP responded to LADOT’s October 25th
17 noncompliance letter, reiterating its privacy concerns and legal objections to the MDS
18 geolocation requirements and reiterating that JUMP planned to file suit seeking injunctive
19 relief against the anticipated permit suspension. And on October 29, 2019, JUMP sought
20 additional clarity on LADOT’s administrative review process. JUMP ultimately elected to
21 engage in that process, and through correspondence over the following weeks, LADOT
22 fashioned the new administrative process.

23 **IX. LADOT’s Administrative Hearing to Review JUMP’s Permit Suspension**

24 94. LADOT convened an administrative hearing before Hearing Officer David B.
25 Shapiro (“H.O. Shapiro”) on January 24 and 27, 2020.⁶ At that hearing, both in pre- and
26

27
28 ⁶ Attached to this Complaint are the transcripts of the hearing on January 24, 2020 (Exhibit A) and
January 27, 2020 (Exhibit B), as well as H.O. Shapiro’s February 11, 2020 Decision (Exhibit C).

1 post-hearing briefing and through witness testimony, JUMP contended that LADOT’s MDS
2 geolocation requirements, and the concomitant suspension of JUMP’s permit for alleged
3 violations of those requirements, was unconstitutional, violated and was preempted by
4 CalECPA, and constituted arbitrary and unlawful agency action.

5 95. LADOT elicited testimony from two witnesses at the hearing. LADOT’s
6 witnesses testified that JUMP was not complying with the requirement that trip-start and
7 trip-end data be transmitted via the Agency API at a latency of five seconds and the
8 requirement that route data be transmitted via the Agency API at a latency of 24 hours. (Ex.
9 A at 57:22-59:5.) Per LADOT’s witnesses, JUMP had been transmitting all three data
10 points at a latency, on average, of just over 24 hours. (Ex. A at 173:25-174:3.)
11 Nevertheless, LADOT’s witnesses could not point to any single authoritative source for
12 these supposed requirements. (See Ex. A at 100:18-101:7.)

13 96. LADOT also elicited testimony from its witnesses regarding the purported
14 public policy bases for requiring that trip-start and trip-end data points be transmitted at a
15 latency of five seconds (rather than 24 hours, as JUMP had been providing). Specifically,
16 LADOT’s witnesses proffered three “use cases” for the purported need for such real-time
17 MDS data—but each swiftly fell apart.

18 97. *First*, Marcel Porras, Head of LADOT’s Bureau of Transportation
19 Technology, testified that LADOT required trip data in real time in order to identify
20 historical deployment patterns in Venice Beach and to craft and audit compliance with a
21 daily deployment cap there. (Ex. A at 40:11-41:4.) In other words, Mr. Porras testified that
22 LADOT could use real-time trip data to determine if providers like JUMP were complying
23 with rules prohibiting providers from placing too many bikes and scooters within an area of
24 Venice Beach that had more than enough devices. On cross-examination, however, Mr.
25 Porras conceded that LADOT used “historical trend data,” not real-time data, to identify the
26 issue and craft the cap, and used “deployment” data, not real-time trip data, to audit
27 compliance with those daily deployment limits in Venice Beach. (Ex. A at 73:12-77:2.)
28 The number and location of devices that providers place into the field, for example, after

1 charging their batteries, is among the many types of non-trip deployment data that providers
2 give to LADOT. And Mr. Porras admitted that JUMP is in compliance with all requirements
3 relating to historical aggregate data and deployment data. (Ex. A at 71:7-18.)

4 98. *Second*, Mr. Porras testified that LADOT requires trip data in real time to aid
5 its responses to 311 complaints and improperly parked dockless vehicles. (Ex. A at 39:24-
6 40:-10.) But on cross-examination, Mr. Porras conceded that JUMP already provides real-
7 time data about *parked* devices through a separate system, compliance with which is also
8 (and separately) required. (Ex. A at 75:2-78:5; *see also id.* at 177:3-12.) Moreover, both
9 LADOT witnesses admitted that JUMP is in compliance with all 311 integration
10 requirements, and that the 311 system itself provides additional information about the
11 location of complaints. (Ex. A at 69:7-25; 77:3-6; 77:17-78:5; 174:8- 177:-12.) In fact,
12 trip-start and trip-end data points do not say anything about a parked device. A device can
13 be parked in a location, and its location would be provided in real time. The trip start rules
14 at issue here do not call for the production of any data unless and until a rider starts a trip
15 on the device.

16 99. *Third*, Vladimir Gallegos, LADOT's Geographic Information Systems
17 Specialist, testified that LADOT needs trip data in real time in order to understand the scope
18 of vehicle deployment during emergencies such as the Los Angeles "Getty Fires." (Ex. A
19 at 169:5-171:6.) On cross-examination, however, Mr. Gallegos conceded that information
20 about deployment requires deployment data, not real-time individual trip-data, and that
21 JUMP complies with all requirements relating to production of deployment data. (Ex. A at
22 173:20-174:7; 185:22-194:13.) And Mr. Porras also confirmed that JUMP also provides
23 real-time information about available (*i.e.*, parked) devices. (Ex. A at 75:6-77:2.) LADOT
24 also did not dispute that JUMP works closely with law enforcement and first responders in
25 emergency situations, including by creating a bespoke warning screen that was pushed to
26 all users in the entire City of Los Angeles during the Getty Fires. (*See* Ex. B at 34:18-35:13;
27 Ex. A at 193:24-194:13.)

28

1 100. Mr. Gallegos also testified about real-time graphs that he monitors on his
2 computer that tracks individual operators. (Ex. A at 163:16-166:6.) He also made passing
3 reference to sometimes receiving requests for trip information from City officials. (Ex. A
4 at 169:5-11.)

5 101. Following JUMP's cross-examination of LADOT's witnesses, LADOT's
6 counsel made no effort to revive any of the proffered "use cases" in summation.

7 102. For its part, JUMP elicited testimony from three witnesses at the hearing. Jeb
8 Burchenal, Uber's Head of Strategy and Data Science, New Mobility Division, testified to
9 the commercial and proprietary value of JUMP's data about its riders and how JUMP uses
10 such data to improve its product. (Ex. A at 226:3-10; 239:2-23, 241:20-242:2.) He also
11 testified to JUMP's interest in securing the privacy and confidentiality of such data on
12 behalf of its users to safeguard their trust and goodwill towards the company. (Ex. A at
13 240:8-16.) Mr. Burchenal testified that, for these reasons, JUMP has invested significant
14 resources to safeguard its data from disclosure, including hiring a large engineering security
15 team, (*see* Ex. A at 240:4-7), and has developed a reputation among its users for a strong
16 commitment to user data security and privacy protection, (Ex. A at 243:2-6).

17 103. Further to this commitment to privacy, Mr. Burchenal testified as to JUMP's
18 privacy concerns, on behalf of its users, that real-time data production increases the
19 potential re-identification and surveillance risks to users should such data fall into the wrong
20 hands. (Ex. A at 233:8-16.) He testified that he was not aware of any other market in which
21 JUMP operates in which a real-time data production requirement is imposed. (Ex. A at
22 233:5-7.)

23 104. Mr. Burchenal further testified to JUMP's business operations, including the
24 anticipated impacts of a permit revocation. He testified that JUMP's dockless vehicles are
25 reliably available to users 24-hours per day, seven days per week, to serve their
26 transportation needs. (Ex. A at 243:23-244:11.) He also testified to JUMP's due diligence
27 and capital investments in the Los Angeles market, including the purchasing of thousands
28 of vehicles to serve Los Angeles, leasing a warehouse, staffing a large team of engineers,

1 managers, and mechanics, and spending thousands of dollars in marketing and brand
2 development in Los Angeles. (Ex. A at 246:6-19.) Finally, Mr. Burchenal testified to the
3 challenges inherent in removing all of JUMP’s vehicles within 72 hours if JUMP’s permit
4 were revoked, as JUMP has several thousand dockless vehicles, scattered throughout a
5 sizeable service area in Los Angeles, all of which would need to be located, picked up, and
6 returned to JUMP’s warehouse within a matter of days. (Ex. A at 245:16-246:1.)

7 105. JUMP next elicited testimony from Charles Noling, JUMP’s Senior Program
8 Manager. Mr. Noling testified to the technical functionality of the APIs required under
9 MDS and the types of data that JUMP must produce as a condition of its permit. He also
10 testified to JUMP’s privacy concerns about producing its users’ real-time geolocation data
11 under Agency API. (Ex. B at 40:24-41:10.) Mr. Noling also testified as to a demonstrative
12 map that made plain the re-identification and surveillance risk provided by the data
13 compelled pursuant to the MDS, even though the data is technically anonymized. (Ex. B at
14 42:19-45:1, 48:3-50:18.) Mr. Noling carefully went through each of LADOT’s witnesses
15 “use cases” and explained that JUMP already provides all the data LADOT actually needed
16 to meet their identified needs, and that time-stamped geolocation trip-start, trip-end, and
17 route data points are not useful for those purposes (and are only good at surveilling people).
18 (Ex. B at 28:11-38:10.) Mr. Noling also explained that JUMP does in fact make all three
19 of the disputed data points (trip-start, trip-end, and route data) available through the
20 Provider API database *exactly* 24 hours after each trip ends. (Ex. B at 57:14-58:12.) Then,
21 consistent with industry custom and best practice, JUMP transmits the same data via
22 Agency API as a package delivered to LADOT once every hour. (Ex. B at 56:15-57:13.)

23 106. Finally, JUMP elicited testimony from Emily Strand, Uber’s Head of Data
24 Sharing Policy. Ms. Strand testified to the history of correspondence between JUMP and
25 LADOT, highlighting JUMP’s immediate and consistent privacy-based objections to
26 MDS’s user-data production requirements. (Ex. B at 83:12-84:8.) Ms. Strand also testified
27 to her understanding of the relationship between LADOT and Ellis & Associates, including
28 Ellis & Associates’ role in crafting and implementing the MDS geolocation requirements.

1 (Ex. B at 85:20-86:18; 87:17-91:9, 99:22-100:25.) Ms. Strand’s testimony also made clear
2 that despite repeated requests, LADOT (i) never explained its latency requirements; or
3 (ii) put any adequate confidentiality or data security policies in place. (Ex. B at 115:22-
4 116:7; 121:7-11.)

5 107. On February 11, 2020, H.O. Shapiro issued a decision upholding LADOT’s
6 suspension of JUMP’s operating permit. (See Ex. C.) H.O. Shapiro did not address the
7 lawfulness of LADOT’s MDS geolocation requirements, somehow concluding that he was
8 “permit[ted], but [was] not compel[led]” to address those issues. (Ex. C at 11:20.) H.O.
9 Shapiro reached this conclusion notwithstanding JUMP’s repeated reference to the
10 California Supreme Court’s decision in *Woods v. Superior Court*, 28 Cal. 3d 668 (1981),
11 which made clear that “an *invalid* regulation *should* be vulnerable to attack at the
12 administrative level.” *Id.* at 680. H.O. Shapiro likewise did not directly address JUMP’s
13 contention that LADOT acted arbitrarily, capriciously, and without fair or substantial reason
14 in suspending its permit. H.O. Shapiro instead deferred to LADOT’s judgment that the
15 “MDS rule best serves the citizens of the City of Los Angeles,” (Ex. C at 12:14-16), without
16 explaining how or considering arguments that the rules themselves violated the federal and
17 state constitution, state law, and basic principles of administrative law.

18 **X. JUMP’s Application for a Six-Month Permit Extension**

19 108. On February 20, 2020, JUMP requested an administrative appeal of H.O.
20 Shapiro’s decision before the LADOT Board of Commissioners (“Board”). And JUMP was
21 informed that, if JUMP were to lose its appeal before the Board, it would have up to 72
22 hours to remove its entire fleet of vehicles from the streets and cease operating in Los
23 Angeles. On March 6, 2020, however, as the March 15, 2020 expiration of JUMP’s one-
24 year permit was quickly approaching, LADOT released applications for a follow-on six-
25 month extension permit.⁷

26
27 ⁷ The MDS data production requirements were unchanged with respect to the March 2020
28 six-month permit. Most importantly, LADOT continued to insist that providers produce trip-

1 112. In taking the actions described herein, Defendants acted under color of the
2 statutes, regulations, customs and usages of the City of Los Angeles and the State of
3 California for purposes of establishing “state action” under 42 U.S.C. § 1983.

4 113. The Fourth Amendment to the U.S. Constitution protects “[t]he right of the
5 people to be secure in their persons, houses, papers, and effects, against unreasonable
6 searches and seizures.” The Fourth Amendment applies to state and city actors by virtue of
7 the Fourteenth Amendment to the U.S. Constitution.

8 114. JUMP has a reasonable expectation of privacy in its business records. The data
9 compelled pursuant to the LADOT’s MDS geolocation requirements consist of confidential
10 and highly sensitive time-stamped geolocation information relating to users of JUMP’s
11 platform and commercially sensitive information about JUMP’s business. JUMP takes
12 various measures to guard such confidential business information from public disclosure,
13 which is crucial for JUMP to maintain its business success.

14 115. JUMP’s users also have significant privacy interests in the non-public personal
15 information that they disclose to JUMP. Users expect that their private information will be
16 used only for limited purposes as outlined in JUMP’s Privacy Policy. And JUMP shares
17 the interests of its users in maintaining their privacy, so that users will continue to have
18 confidence in JUMP’s platform.

19 116. The Fourth Amendment prohibits the government from executing an
20 administrative search unless the subject of the search has “an opportunity to obtain
21 precompliance review before a neutral decisionmaker.” *City of Los Angeles, Calif. v. Patel*,
22 135 S. Ct. 2443, 2451-52 (2015); *see also AirBnB, Inc. v. City of New York*, 373 F. Supp.
23 3d 467, 482-495 (S.D.N.Y. 2019).

24 117. The data being compelled pursuant to LADOT’s APIs is time-stamped
25 geolocation data, which only heightens the privacy interests at stake.

26 118. The requirement to comply with LADOT’s MDS geolocation requirements
27 violates the Fourth Amendment to the U.S. Constitution because the MDS geolocation
28 requirements operate in practice as an administrative search that is fundamentally untailed

1 and unreasonable and provides no opportunity for precompliance review. Moreover, the
2 real-time Agency API requirements are particularly and especially invasive and
3 unreasonable, and by their nature make precompliance review impossible.

4 119. The Fourth Amendment also prohibits the government from unreasonably
5 conditioning the grant of a discretionary benefit on an applicant's acquiescence to the
6 disclosure of information over which it has a privacy interest and which it would not
7 otherwise produce to the government.

8 120. The obligation to comply with LADOT's MDS geolocation requirements as a
9 condition of receiving a permit under the Program constitutes an unconstitutional condition
10 to a discretionary government benefit.

11 121. Pursuant to 42 U.S.C. § 1983 and the Court's equitable powers, JUMP seeks
12 injunctive relief against the City and LADOT, whose enforcement of the MDS geolocation
13 requirements violates the Fourth Amendment.

14 **SECOND CLAIM FOR RELIEF**

15 **VIOLATION OF ARTICLE 1, § 13 OF THE CALIFORNIA STATE**
16 **CONSTITUTION AND CLAIM FOR INJUNCTIVE RELIEF, PURSUANT TO 28**
17 **U.S.C. § 1367 AND THE COURT'S EQUITABLE POWERS**

18 122. JUMP incorporates all of the preceding paragraphs as if fully set forth herein.

19 123. Like the Fourth Amendment to the U.S. Constitution, Article 1, § 13 of the
20 California Constitution protects "[t]he right of the people to be secure in their persons,
21 houses, papers, and effects against unreasonable seizures and searches."

22 124. JUMP has a reasonable expectation of privacy in its business records. The data
23 compelled pursuant to the MDS consists of confidential information relating to users of
24 JUMP's platform and commercially sensitive information about JUMP's business. JUMP
25 takes various measures to guard such confidential business information from public
26 disclosure.

27 125. The data being compelled pursuant to LADOT's APIs is time-stamped
28 geolocation data, which only heightens the privacy interests at stake.

1 126. JUMP’s users also have privacy interests in the non-public personal
2 information that they disclose to JUMP. Users expect that their private information will be
3 used only for limited purposes outlined in JUMP’s Privacy Policy. And JUMP shares the
4 interests of its users in maintaining their privacy, so that users will continue to have
5 confidence in JUMP’s platform.

6 127. The obligation to comply with the MDS geolocation requirements violates
7 Article 1, § 13 of the California Constitution because the MDS geolocation requirements
8 operate in practice as an unreasonable administrative search without any form of
9 precompliance review, and the obligation to comply with MDS as a condition of receiving
10 a permit under the Program constitutes an unconstitutional condition to a discretionary
11 government benefit.

12 128. Pursuant to Article 1, § 13 of the California Constitution, 28 U.S.C. § 1367,
13 and the Court’s equitable powers, JUMP seeks injunctive relief against the City and
14 LADOT, whose enforcement of the MDS geolocation requirements violates the California
15 Constitution.

16 **THIRD CLAIM FOR RELIEF**

17 **VIOLATION OF AND PREEMPTION BY THE CALIFORNIA ELECTRONIC**
18 **COMMUNICATIONS PRIVACY ACT, CAL. PENAL CODE § 1546 ET SEQ., AND**
19 **CLAIM FOR INJUNCTIVE RELIEF PURSUANT TO 28 U.S.C. § 1367 AND THE**
20 **COURT’S EQUITABLE POWERS**

21 129. JUMP incorporates all of the preceding paragraphs as if fully set forth herein.

22 130. California’s Electronic Communications Privacy Act (“CalECPA”), Cal. Penal
23 Code § 1546, *et seq.*, is “the most privacy-protective legislation of its kind in the nation.”
24 Susan Freiwald, *At the Privacy Vanguard: California’s Electronic Communications*
25 *Privacy Act (CalECPA)*, 33 Berkeley Tech. L.J. 131, 133 (2018).

26 131. Article 11, § 7 of the California Constitution provides that a city may only
27 “make and enforce within its limits all local, police, sanitary, and other ordinances and
28 regulations not in conflict with general laws.”

1 132. CalECPA generally prohibits any “government entity” from “compel[ling] the
2 production of or access to electronic device information from any person or entity other
3 than the authorized possessor of the device.” Cal. Penal Code § 1546.1(a)(2).

4 133. CalECPA defines an “electronic device” as “a device that stores, generates, or
5 transmits information in electronic form.” Cal. Penal Code § 1546(f). JUMP’s bikes and
6 scooters are “electronic devices” within this definition because they store, generate and
7 transmit information in electronic form, including location, battery level, direction, speed,
8 and maintenance status.

9 134. CalECPA defines “electronic device information” as “any information stored
10 on or generated through the operation of an electronic device, including the current and
11 prior locations of the device.” Cal. Penal Code § 1546(g). A variety of the electronic data
12 generated and transmitted by JUMP’s scooters and bikes constitutes “electronic device
13 information.”

14 135. When a JUMP bike or scooter is not being used by a rider, and is instead on
15 the right of way available to be rented by an individual, it is the property of JUMP, and in
16 effect possessed either by JUMP or by no one. When a rider has rented and has unlocked a
17 JUMP bike or scooter, however, that person is by virtue of its rental agreement with JUMP,
18 the “authorized possessor” of the device, for purposes of CalECPA, and remains so until
19 the user ends the trip.

20 136. The City and LADOT are each a “government entity.”

21 137. The City and LADOT each violate Cal. Penal Code § 1546.1(a)(2) because,
22 pursuant to the MDS geolocation requirements, LADOT compels JUMP to produce and to
23 provide access to electronic device information, including trip-start and trip-end time-
24 stamped geolocation, while a rider is in possession of the device. Such compelled
25 production also conflicts with the requirements of state law in contravention of Article 11,
26 § 7 of the California Constitution, and is thus preempted.

1 138. CalECPA further prohibits any “government entity” from “[a]cces[ing]
2 electronic device information by means of physical interaction or electronic communication
3 with the electronic device.” Cal. Penal Code § 1546.1(a)(3).

4 139. CalECPA defines “electronic communication” as “the transfer of signs,
5 signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by
6 a wire, radio, electromagnetic, photoelectric, or photo-optical system.” Cal. Penal Code §
7 1546(c).

8 140. The City and LADOT each violate Cal. Penal Code § 1546.1(a)(3) because,
9 pursuant to the MDS geolocation requirements, LADOT accesses JUMP’s electronic device
10 information by physical interaction and electronic communication with JUMP’s electronic
11 devices. Such access also conflicts with the requirements of state law in contravention of
12 Article 11, § 7 of the California Constitution, and is thus preempted.

13 141. None of the circumstances listed in Cal. Penal Code § 1546.1(b) apply to the
14 City’s compulsion of and access to electronic device information pursuant to the MDS.

15 142. Pursuant to CalECPA, Cal. Penal Code § 1546.4(c), 28 U.S.C. § 1367, and the
16 Court’s equitable powers, JUMP seeks injunctive relief against the City and LADOT, whose
17 enforcement of the MDS geolocation requirements violates and is preempted by CalECPA.

18 **FOURTH CLAIM FOR RELIEF**

19 **VIOLATION OF CALIFORNIA’S NON-DELEGATION DOCTRINE AND CLAIM**
20 **FOR INJUNCTIVE RELIEF, PURSUANT TO 28 U.S.C. § 1367 AND THE**
21 **COURT’S EQUITABLE POWERS**

22 143. JUMP incorporates all of the preceding paragraphs as if fully set forth herein.

23 144. California’s non-delegation doctrine is “rooted in the principle of separation of
24 powers that underlies [California’s] tripartite system of Government.” *Golightly v. Molina*,
25 229 Cal. App. 4th 1501, 1516 (2014) (quoting *Samples v. Brown*, 146 Cal. App. 4th 787,
26 804 (2007)). “[T]he doctrine prohibiting delegation of legislative power . . . precludes
27 delegation of the legislative powers of a city.” *Kugler v. Yocum*, 69 Cal. 2d 371, 375 (1968).

1 145. A delegation of power is unconstitutional if “a legislative body confers upon
2 an administrative agency unrestricted authority to make fundamental policy decisions.”
3 *Golightly*, 229 Cal. App. 4th at 1516. Any such grant of power “must be accompanied by
4 safeguards adequate to prevent its abuse.” *Bayside Timber Co. v. Bd. of Supervisors*, 20
5 Cal. App. 3d 1, 11 (1971) (quotation marks omitted).

6 146. “When legislative authority without standards for its guidance is delegated to
7 a[] . . . group of individuals with a pecuniary interest in its subject matter, the constitutional
8 fault is compounded.” *Id.* at 12.

9 147. The Los Angeles City Council provided a boundless delegation of authority to
10 LADOT pursuant to L.A. Admin. Code. § 71.29, which allowed LADOT to regulate a “truly
11 fundamental” area without direction: the seizure and examination of business records
12 owned by JUMP and concerning the privacy and security of individual time-stamped
13 geolocation data that reflects the real time movement of private citizens.

14 148. The substantive provisions of § 71.29 say nothing about data sharing, trip data,
15 or the MDS, and only makes mention of “data” just once in a prefatory “Whereas” clause.
16 Instead, § 71.29 simply directs LADOT to implement a “Shared Mobility Device Pilot
17 Program” and to promulgate “permit rules, regulations, indemnification, insurance and fee
18 requirements . . . in Rules and Guidelines.” This standardless delegation of authority to
19 craft rules that seize intimate geolocation data of City residents from dockless mobility
20 operators, and with for profit private companies like Ellis & Associates and Lacuna to gain,
21 is an unconstitutional delegation of legislative authority.

22 149. LADOT “compounded” this “constitutional fault” by re-delegating its own
23 standardless rulemaking authority to Ellis & Associates, a for-profit industry participant
24 that stands to profit from the rules LADOT tasked it to create and enforce.

25 150. Pursuant to 28 U.S.C. § 1367, and the Court’s equitable powers, JUMP seeks
26 injunctive relief against the City and LADOT, whose enforcement of the MDS geolocation
27 requirements violates California’s non-delegation doctrine.

28

FIFTH CLAIM FOR RELIEF

DECLARATORY RELIEF PURSUANT TO 28 U.S.C. § 2201

151. JUMP incorporates all of the preceding paragraphs as if fully set forth herein.

152. This action presents an actual controversy between JUMP and the City and LADOT concerning the validity of LADOT’s MDS geolocation requirements and their enforcement against JUMP. Any further compliance with the MDS geolocation requirement will cause immediate, irreparable harm to JUMP’s privacy and constitutional rights, as well as the privacy and security of its users.

153. Based on the foregoing allegations, JUMP is entitled to a declaration, pursuant to 28 U.S.C. § 2201, that LADOT’s MDS geolocation requirements cannot be enforced against JUMP because such enforcement violates the Fourth Amendment to the U.S. Constitution as incorporated into the Fourteenth Amendment), Article 1, §§ 2 & 13 of the California Constitution, and CalECPA.

WHEREFORE, JUMP SEEKS RELIEF AS FOLLOWS:

1. For a declaration that LADOT’s MDS geolocation requirements violate the Fourth Amendment to the U.S. Constitution (as incorporated into the Fourteenth Amendment), and/or Article 1, § 13 of the California Constitution, because they improperly authorize the City to execute an unreasonable administrative search without precompliance review, and they improperly condition a government benefit on JUMP’s foregoing of its right as to property over which it has a reasonable expectation of privacy;
2. For a declaration that LADOT’s MDS geolocation requirements violate and are preempted by CalECPA because they improperly compel the production of and access to JUMP’s data without a warrant;
3. For a declaration that LADOT’s MDS geolocation requirements violate California’s non-delegation doctrine because LADOT is acting pursuant

1 to L.A. Admin Code § 71.29, which provides a standardless grant of
2 authority to LADOT with respect to the seizure of intimate geolocation
3 data, and LADOT compounded that constitutional infirmity by
4 re delegating that authority to a for-profit industry participant;

- 5 4. For the Court to preliminarily and permanently enjoin LADOT; its
- 6 agencies, officers, agents, servants, employees, and attorneys; and all
- 7 persons acting in concert or participation with them from taking any
- 8 actions to implement or enforce LADOT’s MDS geolocation
- 9 requirements, including any actions to deny, withhold, withdraw, or
- 10 cancel a permit for JUMP to operate in the City;
- 11 5. For an award of JUMP’s reasonable costs and attorneys’ fees pursuant
- 12 to 42 U.S.C. § 1988; and
- 13 6. For any other relief that the court deems just and proper.

14
15 Dated: March 24, 2020

KAPLAN HECKER & FINK LLP

16
17 By: /s/ Roberta A. Kaplan

18 Roberta A. Kaplan
19 John C. Quinn
20 Benjamin D. White

21 Dated: March 24, 2020

COHEN WILLIAMS LLP

22
23 By: /s/ Marc S. Williams

24 Marc S. Williams
25 Neil S. Jahss

26 *Attorneys for Plaintiff-Petitioner,*
27 *Social Bicycles LLC d/b/a JUMP*
28

DEMAND FOR JURY TRIAL

Plaintiff Social Bicycles LLC d/b/a JUMP demands a jury trial in this matter.

Dated: March 24, 2020

KAPLAN HECKER & FINK LLP

By: /s/ Roberta A. Kaplan

Roberta A. Kaplan

John C. Quinn

Benjamin D. White

Dated: March 24, 2020

COHEN WILLIAMS LLP

By: /s/ Marc S. Williams

Marc S. Williams

Neil S. Jahss

Attorneys for Plaintiff

Social Bicycles LLC d/b/a JUMP