U.C.L.A. Law Review

Jump v. Los Angeles: Removing Platforms Further From Democratic Control?

Beatriz Botero Arcila

ABSTRACT

In March 2020, Jump, Uber's escooter subsidiary, sued the Los Angeles Department of Transportation over a rule that requires the company to share realtime location data about its escooters with the city government. Jump argues that the rule operates in practice as a warrantless administrative search. It also argues that all the data it collects from its users are part of its business records and is thus its private property. This Essay argues that a ruling recognizing that all of the data collected by platforms are their property, and that all data requests are searches, would further insulate platforms from democratic and regulatory control at a time when our era of informational capitalism is already characterized by remarkable platform power. Data sharing programs, however, can be designed in ways that are privacy aware and compliant with current Fourth Amendment doctrine; this Essay briefly discusses how.

AUTHOR

Beatriz Botero Arcila is an S.J.D. candidate at Harvard Law School and a fellow at the Berkman Klein Center for Internet and Society.

I thank the participants of the 2020 Big Ten & Friends Business Law & Ethics Research Seminar, Professor Martha Minow, Camila Gómez, Elena Chachko, and Helena Alviar for their comments and feedback on this paper and previous drafts. I am also grateful to Abbey Stemler for her encouragement and to the editors of the *UCLA Law Review*, in particular Ben Levine and Maya Chaudhuri, for their careful editing.

TABLE OF CONTENTS

INTRODUCTION

On March 25, 2020, Jump, then one of Uber's e-scooter subsidiaries sued the Los Angeles Department of Transportation (LADOT) over a rule that requires the company to share real-time locational data about its e-scooters.[1] Jump is an e-scooter service and the rule is part of the city's licensing program for the operation of micromobility services, like e-scooters.[2] The service was available from Uber's mobile application. In the second quarter of 2020, it was acquired by Lime Scooters.[3] LADOT requests real-time information about the vehicles: how many are in use and where they are picked up and dropped off. The application also sends information about the route taken to LADOT with a within a day.[4] LADOT describes the program as "leading the way for 21st Century mobility"[5] and as allowing it to use "new technologies to provide transportation safety, happiness, sustainability, and equitable access for all."[6]

Jump argued that sharing such detailed information with LADOT puts Jump riders' personal privacy at risk.[7] In its first claim for relief it also suggested that the data collected from Jump users belongs to Jump: LADOT's requirements "operate in practice as an administrative search" because Jump has a reasonable expectation of privacy in its business records, which include "the data compelled pursuant to

1. Between the time of writing and the time of publishing, Jump was acquired by Lime Scooters, another micro-mobility company in which Uber is a main investor; Jump voluntarily dismissed the lawsuit after being bought by Lime Scooters. The American Civil Liberties Union (ACLU), however, filed a complaint on behalf of Jump's users raising similar privacy arguments. *See* Complaint, Sanchez v. L.A. Dep't of Transp., No. 2:20-CV-05044 (C.D. Cal. June 8, 2020).
2. Preetika Rana & James Rundle, *Uber Sues Los Angeles Over Data-Sharing Rules*, WALL ST. J. (Mar. 25, 2020), https://www.wsj.com/articles/uber-sues-los-angeles-over-data-sharing-rules-11585104223 [https://perma.cc/8MZU-52TD].
3. Uber is one of Lime's main stockholders. *See* Andrew J. Hawkins, *Lime Squeezes $170 Million From Uber and Alphabet as Scooter-Sharing Plummets Under COVID-19*, VERGE (May 7, 2020, 10:15 AM), https://www.theverge.com/2020/5/7/21250420/lime-funding-uber-deal-alphabet-scooter-jump-bike [https://perma.cc/QL4B-EJ5Y].
4. Seleta Reynolds, *Los Angeles Stands Firm on Mobility Data We Can Trust*, FORBES (Feb. 12, 2020, 1:06 PM), https://www.forbes.com/sites/seletareynolds/2020/02/12/los-angeles-stands-firm-on-mobility-data-we-can-trust/#37c25564570e [https://perma.cc/QQA4-F33V].
5. ASHLEY Z. HAND, LADOT, URBAN MOBILITY IN A DIGITAL AGE: A TRANSPORTATION TECHNOLOGY STRATEGY FOR LOS ANGELES (2016), https://ladot.lacity.org/sites/default/files/202003/transportationtechnologystrategy_2016.pdf [https://perma.cc/F5AQ-RULW].
6. *Id.*
7. Ruby Zefo, *Standing Up for Rider Privacy in Los Angeles*, MEDIUM (Mar. 24, 2020), https://medium.com/uber-security-privacy/ladot-mds-privacy-1eafbc412550 [https://perma.cc/2PHZ-5V3F].

the LADOT's MDS geolocation requirements."[8] According to Jump, "keeping such confidential business information from public disclosure . . . is crucial for Jump to maintain its business success."[9] Regarding users' expectation of privacy, it notes that "users expect their private information will be used only for limited purposes as outlined in Jump's privacy policy."[10] Uber's privacy policy states, however, that "Uber may share users' personal data if we believe it's required by applicable law . . . with law enforcement officials, public health officials, other government authorities . . . ."[11]

In this Essay, I examine Jump's Fourth Amendment claim over user data and argue that, though the personal privacy concerns over information sharing Jump has raised are real and important, a ruling recognizing that the data platforms collect are their property, and that all data requests are searches, would further advance our increasing tendency to isolate platforms from democratic control. Current informational capitalism[12] is characterized by rising platform power, and governmental access to some of the data these companies collect may be crucial to regulating platforms and holding them accountable.[13] Granting Uber quasi–property rights over data would also do little to address user-privacy concerns: It would still be able to use, exploit, and share user data with third parties—government included[14]—with little

8. Complaint for Injunctive & Declaratory Relief at 114, JUMP v. City of Los Angeles, No. 2:20-CV-02746 (C.D. Cal Mar. 24, 2020). LADOT's Mobility Data Specification (MDS) is the data-reporting element of Los Angeles's Transportation Technology strategy. *See infra* Part I.
9. Complaint for Injunctive & Declaratory Relief, *supra* note 8, at 114.
10. *Id.* at 115.
11. *Uber Privacy Notice*, UBER (Feb. 28, 2020), https://www.uber.com/legal/es/document/?country=united-states&lang=en&name=privacy-notice [https://perma.cc/48QH-SPE6] (requiring Jump's users to agree to Uber's privacy policy because Jump's e-scooters are available through Uber's main app, just like Uber Eats is).
12. By digital information capitalism, I refer to the economic mode of production that has evolved, largely during the last decade, out of the massification of digital technologies and data-driven analytics and that is largely intermediated by platforms. *See infra* Part II.
13. *See, e.g.*, Amy Kapczynski, *The Law of Information Capitalism*, 129 YALE L.J. 1460 (2020) (explaining how various subfields of law have contributed to isolate platform from democratic control).
14. A ruling like the one Jump seems to be seeking will do nothing to prevent voluntary data-sharing, even with government agencies including law enforcement: *Airbnb, Inc v. City of New York* was a case that involved a data-sharing ordinance for home-sharing companies, in which the court found that the requested data were part of the company's business records and that the information-sharing requirements were equivalent to an administrative search when no opportunity for precompliance review was offered. A month after the decision, New York City filed five subpoenas against Airbnb and HomeAway seeking the data of roughly 20,000 hosts whom the city had identified as having potentially violated local home-sharing rules. The City and Airbnb then reached an agreement on one of the subpoenas and a judge ordered Airbnb to comply with that agreement, which required the company to periodically hand the city information about guests and hosts for use in an investigation of illegal short-term rentals. *See*

public oversight.[15] Data-sharing programs, however, can be designed in ways that are both privacy-aware and compliant with the Fourth Amendment: They must meet an important policy interest and they must be limited to minimize possibilities of abuse and threats to privacy. Thus, even if courts find that LADOT's program is not sufficiently tailored or that it creates significant privacy risks, their decisions should be narrow so that in the future Los Angeles and other cities can use privately collected data to advance their own sustainability and equity goals.[16]

In what follows, I first present LADOT's data-sharing program, how cities have used other data-sharing programs to regulate platforms and advance equity goals, and I begin discussing the lawsuit. The second Part explains why Jump's claim is problematic from a legal and a policy perspective. The third Part examines how, why, and under what circumstances data-sharing programs between cities and platforms can be lawful under the Fourth Amendment.

I. LADOT'S DATA-SHARING PROGRAM AND OTHERS OF ITS KIND

LADOT's Mobility Data Specification (MDS) is the data-reporting element of Los Angeles's Transportation Technology strategy.[17] Per LADOT policy, companies operating shared e-scooter services are required to submit information to the city through MDS. The city requests real-time information regarding how many vehicles are in use and where they are picked up and dropped off. Information about the route taken is also sent to LADOT within a day.[18] The city uses MDS to submit information to e-scooter providers regarding limits on the number of vehicles in an area, service areas, or street closures.[19]

Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 490–93 (S.D.N.Y. 2019); *see also* Paris Martineau, *Airbnb Starts to Play Nice With Cities*, WIRED (Aug. 31, 2019, 7:00 AM), https://www.wired.com/story/airbnb-starts-play-nice-cities [https://perma.cc/T9ZQ-Z7RE] (showing that Airbnb was willing to hand in user data with cities after courts found Airbnb was subject to local municipal power to regulate short-term rentals).

15. *See, e.g.*, Jordan Abbott, *Time to Build a National Data Broker Registry*, N.Y. TIMES (Sept. 13, 2019), https://www.nytimes.com/2019/09/13/opinion/data-broker-registry-privacy.html [https://perma.cc/GX44-ABJU] (discussing the unregulated data market and the need for a supervisory regime over it, like a national data broker registry).
16. *But see* G.S. Hans, *Curing Administrative Search Decay*, 24 B.U. J. SCI. & TECH. L. 1 (2018) (arguing that the possibility of local data-sharing ordinances calls for reform of the current administrative search doctrine and proposing a narrower tailoring of the doctrine).
17. L.A. DEP'T OF TRANSP., TECHNOLOGY ACTION PLAN V 1.2, at 1, 15 (2019) [hereinafter TECHNOLOGY ACTION PLAN], https://ladot.io/wp-content/uploads/2019/04/LADOT-TAP_v1–2_Nov_FINAL.pdf [https://perma.cc/R9RC-8VBQ].
18. Reynolds, *supra* note 4.
19. TECHNOLOGY ACTION PLAN, *supra* note 17, at 27.

LADOT expects to leverage the collected information to be more effective, equitable, and sustainable in its functions.[20] According to LADOT, the program also allows the city to solve a "myriad of issues" in a more cost-effective way, such as ensuring companies are complying with local rules, making sure the e-scooters are being made available to lower-income residents,[21] and addressing complaints about e-scooters blocking sidewalks and operating unsafely.[22] MDS is currently used primarily to share data from dockless and public transportation vehicles with LADOT. The agency, however, expects that in the future this kind of digital infrastructure will help it engage and manage autonomous cars and drones.[23]

Cities and transportation officials across the United States have been advocating for and adopting data-sharing strategies to improve their planning and street management capacities for some time.[24] Washington, D.C. has used a somewhat similar platform in partnership with Uber and Lyft to share anonymized rider data to redesign parking areas in Dupont Circle and decrease congestion.[25] Since 2007, New York City, a pioneer in this space, has used mobility data collected from taxis to analyze traffic patterns in the city and plan streets and bike lanes, improve traffic, and create new pedestrian space, most saliently in Times Square.[26] In 2014, the city also issued rules requiring ridesharing companies to report the pickup time and location of each trip, the license number of the driver,

20. *Id.* at 9.
21. *See* LADOT, DOCKLESS ON-DEMAND PERSONAL MOBILITY ONE-YEAR PERMIT 18 (2019), http://basic.cityofla.acsitefactory.com/sites/g/files/wph266/f/Final%20One-Year%20Dockless%20Permit.pdf [https://perma.cc/KUU8-A7Y8].
22. *See* Joseph Cox, *Scooter Companies Split on Giving Real-Time Location Data to Los Angeles*, VICE (Mar. 19, 2019, 8:43 AM), https://www.vice.com/en_us/article/yw8j5x/scooter-companies-location-data-los-angeles-uber-lyft-bird-lime-permits [https://perma.cc/UU4V-VD4Z].
23. *See* TECHNOLOGY ACTION PLAN, *supra* note 17, at 29; HAND, *supra* note 5.
24. *NACTO and IMLA Guidelines for Managing Mobility Data*, NAT'L ASS'N CITY TRANSP. OFFICIALS, https://nacto.org/managingmobilitydata [https://perma.cc/H2C3-VXYZ] (last visited May 10, 2020).
25. *See* Benjamin Schneider, *D.C. Gives Uber and Lyft a Better Spot in Nightlife*, BLOOMBERG CITYLAB (Oct. 25, 2017, 11:11 AM), https://www.citylab.com/transportation/2017/10/a-dc-neighborhood-rethinks-parking/543870 [https://perma.cc/ZN4A-DQJZ] (describing how Uber and Lyft data were used to manage pick ups in Dupont Circle as clubs let out, overall improving late-night traffic in the area).
26. *See* Janette Sadik-Khan, *Uber's Dishonest Data Dance: They Refuse to Make Available Information That the City Needs to Do Strategic Transportation Planning*, N.Y. DAILY NEWS (Feb. 2, 2017, 5:00 AM), https://www.nydailynews.com/opinion/uber-dishonest-data-dance-article-1.2961487 [https://perma.cc/6N5H-69PM] (explaining how New York City's transportation department used data from GPS in the city's yellow taxis to evaluate traffic flow after they closed Broadway through Times Square and how Uber first objected to share similar information with the city's Taxi & Limousine Commission.).

and the license number of the vehicle performing the trips.[27] In 2018, amidst local public concern over ridesharing drivers working themselves to exhaustion,[28] the New York City Council passed legislation with a minimum trip payment formula after determining that 96 percent of all app drivers were making less than the equivalent of minimum wage.[29] It also capped the amount of ridehailing cars while the city developed a longterm policy for managing congestion. The data these cities collected informed these decisions.[30]

However, since MDS in Los Angeles was announced, Uber has objected and challenged the program based on the privacy risks it represents for its users.[31] Though MDS never requests individual user information, the locational and mobility data that it requests is highly sensitive and detractors of the program argued that it could be de-identified.[32] LADOT's Data Protection Principles do say that the department will require e-scooter providers to share "data sets solely to meet the specific operational and safety needs of LADOT objectives,"[33] that where possible it will "aggregate, de-identify, obfuscate, or destroy raw data where [it] do[es] not need single vehicle data,"[34] and that "[l]aw enforcement and other government agencies . . . *will not have access* to raw trip data other

27. N.Y.C. Taxi & Limousine Comm'n, *What Makes a City Street Smart?*, MEDIUM (Jan. 31, 2019), https://medium.com/@NYCTLC/what-makes-a-city-street-smart-23496d92f60d [https://perma.cc/PMG7-UHW5].
28. Ginia Bellafante, *A Driver's Suicide Reveals the Dark Side of the Gig Economy*, N.Y. TIMES (Feb. 6, 2018), https://www.nytimes.com/2018/02/06/nyregion/livery-driver-taxi-uber.html [https://perma.cc/5JXF-B4SB].
29. Laura Bliss, *New York City Just Changed the Uber Game*, BLOOMBERG CITYLAB, (Aug. 8, 2018, 1:32 PM), https://www.citylab.com/transportation/2018/08/new-york-city-moves-to-cap-uber-and-lyft/566924 [https://perma.cc/896Z-5EES].
30. *See* N.Y.C. Taxi & Limousine Comm'n, *supra* note 27.
31. *See* Cox, *supra* note 21. An interesting question that I do not address here is whether Uber has standing to assert its users' Fourth Amendment rights. For a similar discussion, see Tess Hofmann, *Airbnb in New York City: Whose Privacy Rights are Threatened by a Government Data Grab?*, 87 FORDHAM L. REV. 2589, 2612 (2019).
32. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (describing how deleting personal information like names or social security numbers from large databases does not protect individual privacy, as scientists have demonstrated that they can often "reidentify" or "deanonymize" individuals by uncovering patterns in the data).
33. LADOT, LADOT DATA PROTECTION PRINCIPLES 2 (2019) [hereinafter LADOT DATA PROTECTION PRINCIPLES], https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-Protection-Principles.pdf.pdf [https://perma.cc/37G7-GY7R].
34. *Id.* LADOT has not clarified if it uses additional mathematical methods to anonymize the data. Simply stripping data from personal information does not meet mathematical requirements to make it truly anonymous. *See* Ohm, *supra* note 32.

than as required by law . . . ."[35] The document, however, does not seem to be binding.[36]

When the program was adopted in March 2019, Uber refused to share realtime data and instead started giving LADOT data reports with a twenty-four-hour latency.[37] In October 2019, the city suspended Uber's permit, a decision that Jump appealed and lost.[38] Uber subsequently started sharing realtime data in March 2020.[39] The lawyer appointed to hear the administrative appeal found that LADOT had properly suspended Uber's permit for violating the submission rules, because Uber had applied for the permit voluntarily.[40] He also noted that just as Uber had not provided evidence that the e-scooter data had been used to personally identify a rider, the city had not successfully explained what problems could be solved with realtime data reporting.[41]

II. WHY IS JUMP'S PROPERTY-LIKE CLAIM OVER USER DATA PROBLEMATIC?

Today's informational capitalism is characterized by rising power of platforms over workers and users as these platforms become relatively insulated from democratic control.[42] The business model of these firms relies on appropriating and mobilizing vast troves of data to provide a variety of services and

35. LADOT DATA PROTECTION PRINCIPLES, *supra* note 33, at 2.
36. *Id.*
37. *See* Sasha Lekach, *Privacy Groups Actually Side With Uber in Scooter Data Fight*, MASHABLE (Oct. 29, 2020), https://mashable.com/article/uber-jump-scooter-la-data-policy/ [https://perma.cc/BR3W-HQ2G].
38. Laura J. Nelson, *L.A. Wins Appeal in Fight With Uber Over Scooter and Bike Data*, L.A. TIMES (Feb. 11, 2020, 7:13 AM), https://www.latimes.com/california/story/2020-02-11/uber-jump-bikes-scooters-permit-ladot-data-fight-ruling [https://perma.cc/9SEB-M5LU].
39. *Id.*
40. *Id.*
41. *Id.*; *see also* Bliss, *supra* note 29. LADOT's main argument regarding why it requires almost-near realtime data is that it allows it to quickly locate e-scooters in the event of a street closure or wildfire, and ensure that companies are serving transit-starved neighborhoods. Critics of LADOT's program point out that the city could meet these objectives with less intrusive measures. *Id.*
42. *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019) (comprehensively accounting the ways in which law and digital information capitalism are reshaping each other, and how law has contributed to shape platform power); *see also* SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); Kapczynski, *supra* note 13.

reduced costs while mediating and tailoring a wide range of transaction types.[43] The network effects that feed platform power create a tendency toward monopoly and winner-take-all dynamics, which has had a vast impact on the dynamics of labor, rising inequality, and the competitiveness of the market.[44] This model may even enable firms to manipulate their users.[45]

Legal scholars like Julie Cohen, Amy Kapczynski, and Yochai Benkler have pointed out that this new normal has been largely mediated by law.[46] Of particular relevance has been enabling de facto property regimes in data and algorithms.[47] Neither data nor algorithms are, however, formally property. There is no legal principle or rule that creates property rights in data:[48] Personal privacy protection laws give individuals the rights to exclude others from using certain personal information about them and even protects individual privacy from certain alleged risks, but they do so by explicitly creating inalienable rights, not by granting property rights.[49] Intellectual property law does not cover facts.[50] Copyright law provides property rights to original works;[51] patent law provides property rights to systems or methods that involve inventive uses of data;[52] and trade secret protections, which do protect certain information, do not provide exclusive rights.

43. *See, e.g.*, Julie Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017) (explaining patterns of legal change in the platform economy and has become the core organizational form of the emerging informational economy).
44. *See, e.g.*, Veena Dubal, *Rule-Making as Structural Violence: From a Taxi to Uber Economy in San Francisco*, LAW & POL. ECON. (June 28, 2018), https://lpeblog.org/2018/06/28/rule-making-as-structural-violence-from-a-taxi-to-uber-economy-in-san-francisco [https://perma.cc/F943-JM49] (explaining how policymakers refused to enforce existing taxi laws and regulations against so-called "ridesharing" services, contributing to create a new form of precarious work, so called gig-work); Greg Ip, *The Antitrust Case Against Facebook, Google and Amazon*, WALL ST. J. (Jan. 16, 2018, 11:52 AM), https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561 [https://perma.cc/C8JL-VZGM] (suggesting that the size and market-power of some of the main platforms could warrant anti-trust measures to break them up).
45. Kapczynski, *supra* note 13, at 1474, 1489; *see also* Yochai Benkler, Power and Productivity: Institutions, Ideology, and Technology in Political Economy 13 (Dec. 2019) (unpublished manuscript) (available at http://www.benkler.org/Benkler_Power&Productivity.pdf [https://perma.cc/J57Q-KQRE]) (arguing generally that though here is little quantitative evidence to support the claim that these technologies can effectively manipulate demand, "it is clear that their purpose is to develop such power over consumers, and that even without evidence advertisers are buying enough of the promise to obtain such power to make these technology companies the most valuable in the world").
46. Benkler, *supra* note 45; Cohen, *supra* note 42; Kapczynski, *supra* note 13.
47. Kapczynski, *supra* note 13, at 1467.
48. *See, e.g.*, Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 5 (2018).
49. *See id.* at 7; *see also* CAL. CIV. CODE § 1798.192 (West 2018).
50. *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 344, 348 (1991).
51. *See* Determann, *supra* note 48, at 18.
52. *Id.* at 16.

Rather, they are more similar to tort law, as they seek to protect the interests of corporations and individuals in information that is not generally available and known and which they have tried to keep from competitors.[53] Property law, on the other hand, grants owners the right to exclude others from their property, but does not grant rights over information about the property: A landowner cannot assert property rights to prohibit others from depicting their property on a map.[54] There is thus nothing that, a priori, turns data collectors into property owners of that information. Despite this fact, however, contract law and other bodies of law, aided by technical means that facilitate exclusion, have been mobilized to protect platform data from parties that do not contract directly with them and to legitimate patterns of appropriation and property-like regimes over data.[55]

De facto corporate rights over data help sustain and generate the dynamics of private platform power beyond what might be its fair share by, for example, expanding the main platform's power over certain business sectors. The subsequent commodification of personal data has also facilitated the emergence of largely unsupervised data markets in which participants as varied as intelligence and human resources agencies can pay for various forms of data, predictive profiling tools, and individual profiles.[56] Scholars and activists worry that too often these companies do not disclose how these profiles and data are created, nor how they are used, and that as the data become regular inputs in various forms of decision-making processes, they reinforce existing racial and social inequalities.[57] Additionally, since this is information collected by private companies, participants in these markets do not need warrants or direct consent to access this information.[58] As Kapczynsky has pointed out, the mobilization of legal resources to deem all forms of data de facto corporate property further legitimates these practices that treat data as a commodity and facilitates efforts to exclude third

53. *Id.* at 14.
54. *Id.* at 13.
55. JOSEF DREXL ET AL., DATA OWNERSHIP AND ACCESS TO DATA: POSITION STATEMENT OF THE MAX PLANCK INSTITUTE FOR INNOVATION AND COMPETITION OF 16 AUGUST 2016 ON THE CURRENT EUROPEAN DEBATE 3 (2016); Kapczynski, *supra* note 13, at 1502.
56. *See, e.g.*, Peter Waldman et al., *Palantir Knows Everything About You*, BLOOMBERG (Apr. 19, 2018), https://www.bloomberg.com/features/2018-palantir-peter-thiel [https://perma.cc/Q2U2-LW3A]; *see also supra* notes 15, 43.
57. *See, e.g.*, VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); Conor Friedersdorf, *An Unprecedented Threat to Privacy*, ATLANTIC (Jan. 27, 2016), https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/?utm_source=SFFB [https://perma.cc/8C23-2JEC].
58. *See infra* Part III; *infra* note 77.

parties from accessing or knowing how these profiling and data-sets are built and work, further insulating platform power from democratic control.[59]

Indeed, the increasing information intensity of these industries has created a vast technical challenge for regulators: Kapczynski asks, "How do you detect discrimination, manipulative marketing, or regulatory evasion when so much is buried in intricate decisions made by data-gatherers, software, and hardware?"[60] Cohen suggests that "regulators will need to engage more directly with practices of data-driven, algorithmic intermediation and their uses and abuses."[61] Decisions that recognize property-like rights over information for platforms, however, might undermine such efforts. Kapczynski points to decisions in which the U.S. Supreme Court held that trade secrets constituted property subject to protection under the Takings Clause, which lower courts then read broadly to, for example strike down a state law that required disclosure of ingredients to state regulators who could then disclose the ingredients to the public if they found that doing so could lead to public health benefits.[62] In *Philip Morris v. Reilly*, the First Circuit Court of Appeals dismissed the idea that the state's public-health interest in disclosure justified such a move without compensation,[63] despite the fact that the goal of trade secret law is not to help companies keep information secret, but rather to protect business integrity from unfair misappropriation of valuable confidential information.[64] Kapczynski worries that "companies like Google, Facebook and Palantir will surely argue that their data . . . qualify as trade secrets, meaning that any attempt to render them public, or to give access to competitors, will likely face a constitutional challenge."[65] Uber's claim is not so different: It asserts property-like rights over the data it collects, a claim that could unduly insulate the company from democratic control if successful.[66]

III. DATA-SHARING PROGRAMS IN THE LIGHT OF THE FOURTH AMENDMENT

Despite the policy and fairness arguments against granting Uber property-like claims over the data it collects from users, the legal question begs discussion:

59. Kapczynski, *supra* note 13, at 1508.
60. *Id.* at 1491.
61. Cohen, *supra* note 42, at 200.
62. Ruckelhaus v. Monsanto Co., 467 U.S. 986, 1003 (1984); Kapczynski, *supra* note 13, at 1508, 1509.
63. Kapczynski, *supra* note 13, at 1509 (citing Philip Morris, Inc. v. Reilly, 312 F.3d. 24, 28–29 (1st Cir. 2002)).
64. *See, e.g.*, Determann, *supra* note 48, at 15.
65. Kapczynski, *supra* note 13, at 1510.
66. *See also supra* note 14.

Are a platform's Fourth Amendment rights infringed by an ordinance that requires it to share information about how its users use its services?[67]

Not necessarily. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[68] Uber cites *Jones v. United States*,[69] *Carpenter v. United States*,[70] and *City of Los Angeles v. Patel*[71] to convey the sensitivity of geolocational data, to claim that it has a reasonable expectation of privacy in its business records—by which it means the data it collects from users—and, finally, to argue that it should have been given an opportunity to obtain precompliance review before a neutral decisionmaker.[72] These cases, however, dealt with information requests that were intended to facilitate criminal investigations unlike the requests at issue in *Jump*, and they did not address questions about property-like entitlements to the information a company collects from its users.

Here, I show that courts do not need to resolve or adjudicate questions about property-like rights to decide the constitutionality of LADOT's or other data-sharing programs. Rather, they should evaluate whether these programs are reasonably designed to meet an important policy interest, identified and authorized by statute, while at the same time limiting the possibilities of abuse and mitigating threats to protected privacy interests.[73]

In *Jones*, police officers attached a GPS to a vehicle and used it to monitor an individual's movements without a valid warrant. The Court held this was a search within the meaning of the Fourth Amendment because the government had physically occupied private property.[74] In her concurrence, Justice Sotomayor argued that the trespassory test applied by the majority did not reflect how GPS technology bore on reasonable societal expectations of privacy.[75] In 2018, the Court moved a tiny bit in that direction in *Carpenter*: There, the FBI had obtained the defendant's cell phone records from two telecommunications companies without a warrant and the government argued that he lacked a reasonable expectation of privacy because he had shared that information with the wireless

67. Complaint for Injunctive & Declaratory Relief, *supra* note 8, at 114.
68. U.S. CONST. amend. IV.
69. Jones v. United States, 565 U.S. 400 (2012).
70. Carpenter v. United States, 585 U.S. ___ (2018).
71. City of Los Angeles v. Patel, 576 U.S. 409 (2015).
72. *See* Complaint for Injunctive & Declaratory Relief, *supra* note 8, at 4, 36, 41.
73. *See, e.g.*, United States v. Biswell, 406 U.S. 311, 314 (1972).
74. *Jones*, 565 U.S at 402.
75. *Id.* at 417–18 (Sotomayor, J., concurring).

carriers.[76] The Court disagreed and declined to extend the third party doctrine[77] "to cover [these] novel circumstances."[78] Justice Roberts, writing for the majority, stated that the premise underlying the third party doctrine—voluntary exposure—did not apply in the case of cell site location information, observing that "[c]ell phone location information is not truly 'shared' as one normally understands the term" and that "carrying one is indispensable to participation in modern society."[79] The ruling was narrow, however, as it did not "call into question conventional surveillance techniques and tools, such as security cameras." Nor did it "address other business records that might incidentally reveal location information."[80]

Patel addressed the privacy interests of a business in its records—its private property—and the reasonableness of government searches. There, motel owners challenged a provision that required them to retain records containing specific personal information about their guests and authorized warrantless onsite inspections of those records at the behest of the Los Angeles Police Department. Writing for the Court, Justice Sotomayor held that such a requirement was unconstitutional: The alleged government interests at stake—to facilitate criminal investigations and ensure compliance with the recordkeeping requirement—did not meet the strict requirements for permissible warrantless searches.[81]

Indeed, the Fourth Amendment requires that searches and seizures be reasonable, which ordinarily requires a court-issued warrant that guarantees a legal justification for the search.[82] When the primary purpose of the search is distinguishable from crime control, however, warrantless searches known as administrative searches are sometimes allowed.[83] Administrative searches are very common, even if they are exceptional as a matter of black letter law.[84] Sobriety checkpoints, drug tests, and business searches are all administrative searches.[85] These searches do not require particularized suspicion of misconduct but they

76. *Carpenter*, 585 U.S. at 3–4.
77. According to the third party doctrine, a person has no protected privacy interest in information it voluntarily gives to a third party. *See Carpenter*, 585 U.S. at 9; Katz v. United States, 389 U.S. 347, 357 (1967).
78. *Carpenter*, 585 U.S. at 11.
79. *Id.* at 17.
80. *Id.* at 18.
81. City of Los Angeles v. Patel, 576 U.S. 409, 420 (2015) (citing City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000)).
82. *Katz*, 389 U.S. at 357.
83. *See, e.g.*, Hans, *supra* note 16, at 4.
84. *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255 (2011).
85. *Edmond*, 531 U.S. at 37; *see also* Hans, *supra* note 16; Primus, *supra* note 84.

must be appropriately limited,[86] they must be reasonably conducting towards meeting a government interest,[87] and "the possibilities of abuse and the threat to privacy" must not be "of impressive dimensions."[88] Additionally, subjects of administrative searches must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker.[89]

In *Patel*, one of the Court's main worries was that the purpose of the search was not distinguishable from crime control.[90] Additionally, because the law provided that "[a] hotel owner who refuses to give an officer access to his or her registry can be arrested on the spot," the Court found that "the ordinance create[d] an intolerable risk that searches authorized by it w[ould] exceed statutory limits, or be used as a pretext to harass hotel operators and their guests."[91] The holding, however, was narrow: Nothing in the Court's opinion questioned the requirement that hotels maintain guest registries. It held "only that a hotel owner must be afforded an opportunity to have a neutral decisionmaker review an officer's demand to search the registry before he or she faces penalties for failing to comply. Actual review need only occur in those rare instances where a hotel operator objects to turning over the registry."[92]

After considering the caselaw raised by Jump, it is possible to draw some conclusions about the conditions data-sharing programs like LADOT's should meet to be constitutional. First, *Patel* demonstrates that businesses can be asked to share the information they collect to meet important policy goals. Such requests do not require suspicion of misconduct but must be limited and reasonable to meet the policy goal in question,[93] the possibilities of abuse and the threat to privacy must not be "of impressive dimensions,"[94] and they cannot be related to crime control.[95] Second, *Carpenter* demonstrates that though cell site location information is more intimate than e-scooter data, individuals can reasonably be said to have heightened expectations of privacy regarding their geolocational and mobility data if this information can be traced back to them, even if it is in the possession of third parties.[96] There is, however, nothing impeding programs in which companies are required to first collect and keep this information and then

86. *Edmond*, 531 U.S. at 37.
87. *See, e.g.*, Illinois v. Lidster, 540 U.S. 419, 424–25 (2004).
88. Biswell v. United States, 406 U.S. 311, 314 (1972).
89. City of Los Angeles v. Patel, 576 U.S. 409, 423 (2015).
90. *Id.* at 420.
91. *Id.* at 420–21.
92. *Id.* at 421.
93. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).
94. Biswell v. United States, 406 U.S. 311, 314 (1972).
95. *Patel*, 576 U.S. at 420.
96. *See, e.g.*, Carpenter v. United States, 585 U.S. ___, 17 (2018).

give it to regulators when there is a particular need to access granular data, as long as they—and perhaps users themselves—are afforded an opportunity to have a neutral decisionmaker review particular requests.[97] Third, *Patel* demonstrates that corporations may have a protected expectation of privacy if the data they collect could potentially be used to harass them or their users. Thus, programs should have clear and binding rules regarding how and for what purposes the requested information can be used so that abuse can be prevented.[98] Finally, current Fourth Amendment caselaw does not seem to cover information that cannot be traced back to a particular vehicle's movements or that reveals sensitive information about the working of the business. Thus, data-sharing requests over information that is either aggregated mobility data[99] or data made truly anonymous via mathematical methods like differential privacy should not raise Fourth Amendment concerns[100] Tailoring data-sharing ordinances in this manner does not require recognizing quasi–property rights over information.

CONCLUSION

LADOT's Shared Mobility Device foresees that companies operating dockless on-demand mobility products and services (like e-scooters, bicycles, and cars) need to apply for a permit from the city. One of the requirements to obtain the permit is to send LADOT data via MDS. As LADOT's general manager describes it:

> MDS is a straight forward [sic] tool. Shortly after a rider unlocks a scooter, its location and status is automatically sent to our system. Then, after the trip ends, that location is sent again. Within a day, our system receives the route taken . . . . The system is built to process only the minimum amount of vehicle data needed to fulfill our responsibilities to the public. Information about the rider is never requested . . . . With tens of thousands of scooters in operation in unconventional locations, traditional policy and enforcement measures like parking tickets, or speeding tickets, or people with paper

97. *See Patel*, 476 U.S. at 419–20.
98. *Id.* at 425–26; *see also* Hans, *supra* note 16, at 36.
99. *See, e.g.*, N.Y.C. Taxi & Limousine Comm'n, *supra* note 27.
100. Differential privacy is the mathematical definition of privacy in which additional data—often referred to as "noise"—is inserted in a data set in a manner that doesn't affect the general conclusions that can be drawn from that data set but it is impossible to tell whether any individual's data was included in the original dataset or not. *See Differential Privacy*, HARV. U. PRIVACY TOOLS PROJECT, https://privacytools.seas.harvard.edu/differential-privacy [https://perma.cc/4QA7-S7WW] (last visited May 27, 2020) (follow Harvard.edu hyperlink; then follow dropdown menu, "What is Differential Privacy").

> and pen are simply inadequate to address challenges with new mobility devices and providers.[101]

Jump argues that such a program in an unreasonable, untailored warrantless administrative search, and it suggests that the data it collects from its users is its quasi-property.

In *Jump v. Los Angeles*, LADOT will have to show that its MDS program is appropriately tailored and that the information it is asking for is necessary to meeting its policy goals. If, as it seems, LADOT's Data Protection Principles are not binding and LADOT does not prove it is preventing future abuse, courts may find that LADOT's MDS program as it exists today is not sufficiently tailored and may be creating significant risks regarding how the collected data could be used in the future.[102]

What is most important, however, is that the decision should not expand platforms' property-like entitlements over the information they collect from users, hindering future uses of privately collected data that enhance public welfare. Data-sharing programs can be legally and technically tailored to protect individuals' interests in their mobility data, platforms' most sensitive business information, as well as their interest in not being "harassed" by authorities. Uber and other platforms have voluntarily shared and complied with requests to share data before, and cities have used the data to advance equality-enhancing goals while at the same time holding platforms to reasonable controls.[103]

It is not enough, however, that platforms are sometimes willing to collaborate with regulators. If our current era of informational capitalism is characterized by rising concentrated platform power beyond what seems their fair share, it is crucial that governments retain the power to hold platforms accountable. It is also important that just as platforms and consumers benefit from data collection and analytics because it allows platforms to provide ever-more efficient and convenient services, the public in general should benefit too. Giving cities access to some of the quality data platforms collect, while limiting how and why it can be used, is important for that goal. In *Jump v. Los Angeles*, this is at stake.

101. Reynolds, *supra* note 4.
102. *See supra* note 33.
103. *See* Zefo, *supra* note 7.