The Case for Local Data Sharing Ordinances

Beatriz Botero Arcila

THE CASE FOR LOCAL DATA SHARING ORDINANCES

Beatriz Botero Arcila*

ABSTRACT

Cities in the United States have started to enact data sharing rules and programs to access some of the data that technology companies operating under their jurisdiction—like short-term rental or ride hailing companies—collect. This information allows cities to adapt to the challenges and benefits of the digital information economy. It allows them to understand what the impact of these technology companies is on congestion, the housing market, the local job market, and even the use of public spaces. It also empowers cities to act accordingly by, for example, setting vehicle caps or mandating a tailored minimum pay for gig workers. These companies, however, sometimes argue that sharing this information violates their users' privacy rights and their own privacy rights, because this information is theirs; it is part of their business records. The question is thus what those rights are, and whether it should and could be possible for local governments to access that information to advance equity and sustainability, without harming the legitimate privacy interests of both individuals and companies. This Article argues that within current Fourth Amendment doctrine and privacy law there is space for data sharing programs. Privacy law, however, is being mobilized to alter the distribution of power and welfare between local governments, companies, and citizens, within current digital information capitalism to extend those rights beyond their fair share and preempt permissible data sharing requests. This Article warns that if the companies succeed in their challenges, privacy law will have helped shield corporate power from regulatory oversight, while still leaving individuals largely unprotected and submitting local governments further to corporate interests.

INTRODUCTION

Imagine that you work for the city council of the local government of a mid-sized or large city. By now, you are almost used to seeing how technology companies

* Assistant Professor, Sciences Po Law School; Faculty Associate, Berkman Klein Center for Internet and Society at Harvard University. I thank the participants of the 2020 Big Ten & Friends Business Law & Ethics Research Seminar, the participants of the 2021 North East Privacy Scholars Conference and Yochai Benkler for their comments and feedback on this Article and previous drafts. I'd also like to thank my friends and colleagues at the Berkman Klein Center and the SJDs at Harvard Law School for the many conversations that led to this Article, and the editors of the *William & Mary Bill of Rights Journal* for excellent comments and edits. Though all of their comments made this Article better, all mistakes are mine.

coming up with new services and products change local industries and the way public spaces are used: first came ride-hailing services, then home-sharing services, and, most recently, e-scooters and delivery services. Drones and autonomous vehicles will be next. These somewhat new forms of urban services have become central to city life because they provide convenient alternatives for users and workers.[1] However, they also congest streets, contribute to rising housing prices and, often, fight to avoid regulations.[2] Many refuse to acknowledge that they offer services directly, and have instead simply labeled themselves as websites.[3] They have also refused to classify those who find jobs through them as their employees, contributing to the growth of uncertain, risk-laden work in the gig economy.[4]

As a local official, you would like reliable data in order to understand the issues raised by these new services and to regulate them effectively, as well as strengthen your decision-making ability.[5] The business model of many of these firms relies on collecting and analyzing vast troves of data and, with the help of algorithms, match demand and supply efficiently, while at the same time lowering transaction costs.[6] Much of this information says about the city what local governments are eager to

---

[1] Nestor M. Davidson & John J. Infranca, *The Sharing Economy as an Urban Phenomenon*, 34 YALE L. & POL'Y REV. 215, 218 (2016).

[2] *Study Finds Ride-Sharing Intensifies Urban Road Congestion*, MIT NEWS (Apr. 23, 2021), https://news.mit.edu/2021/ride-sharing-intensifies-urban-road-congestion-0423#:~:text=SMART%20research%20finds%20US%20road,congestion%20rose%20by%204.5%20percent [https://perma.cc/RY5N-HJ29]; Gary Barker, *The Airbnb Effect on Housing and Rent*, FORBES (Feb. 21, 2020), https://www.forbes.com/sites/garybarker/2020/02/21/the-airbnb-effect-on-housing-and-rent/?sh=2cddef422260 [https://perma.cc/7TRE-3EXS]; Nandita Bose, *Exclusive: U.S. Labor Secretary Supports Classifying Gig Workers as Employees*, REUTERS (Apr. 29, 2021), https://www.reuters.com/world/us/exclusive-us-labor-secretary-says-most-gig-workers-should-be-classified-2021-04-29/ [https://perma.cc/DW5Z-FBLD].

[3] O'Connor v. Uber Techs., 82 F. Supp. 3d 1133, 1142 (N.D. Cal. 2015).

[4] *See, e.g.*, V.B. Dubal, *The Drive to Precarity: A Political History of Work, Regulation, & Labor Advocacy in San Francisco's Taxi Uber Economies*, 38 BERKELEY J. EMP. & LAB. L. 73, 73 (2017); Benjamin Edelman & Abbey Stemler, *From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces*, 56 HARV. J. LEGIS. 141, 147 (2019); Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 98 (2016).

[5] *See, e.g.*, STEPHEN GOLDSMITH & SUSAN CRAWFORD, THE RESPONSIVE CITY: ENGAGING COMMUNITIES THROUGH DATA-SMART GOVERNANCE v (2014); Lauren Hirschon et al., *Cities, the Sharing Economy and What's Next*, NAT'L LEAGUE OF CITIES 4 (2015), https://www.nlc.org/wp-content/uploads/2015/01/Report-Cities-the-Sharing-Economy-and-Whats-Next-final.pdf [https://perma.cc/RF5S-MPLN]; FED. TRADE COMM'N, THE "SHARING" ECONOMY: ISSUES FACING PLATFORMS, PARTICIPANTS & REGULATORS 2 (2016), https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf [https://perma.cc/G6Q4-663R].

[6] *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 25 (2019); SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 25 (2019).

know: how people commute, what the emerging streets to live and eat are, where is traffic congestion occurring, and so on.[7] For instance, you want to know how to integrate new mobility alternatives into existing transportation and economic development strategies, so you want the information to build new bike lanes and streets based on actual commutes. You would also like to identify and address the social inequities and safety issues caused by these businesses by imposing vehicle caps to mitigate increases in congestion and decreases in air quality, imposing restrictions on short-term rentals that may be negatively impacting the housing market, or by mandating a minimum pay for gig workers after understanding the platform-powered word dynamics.[8]

To access this information, cities in the United States—and the world—are starting to enact data sharing rules and programs as part of the licensing requirements of these companies.[9] Many of these companies, however, often fight mandatory municipal data-requests and, in general, local regulation.[10] Ride-hailing companies aggressively lobbied states to preempt city's attempts to regulate them, while states generally seem to be increasingly hostile to local regulation across a wide range of other policy areas that threaten vested interests.[11] In court, home-sharing and dockless mobility companies have argued, first, that they are simply websites, and not direct service providers, which would put them outside of the typical city's jurisdiction.[12] They also argue, however, that sharing detailed information violates their and their users' privacy rights, and that the data they collect are part of their business records.[13] Consequently, the argument goes, mandatory data sharing rules are in practice warrantless searches and seizures that violate their Fourth Amendment rights and their rights under other privacy and security laws, like the Stored Communications Act or California's Electronic Communication Privacy Act.[14] Privacy advocacy groups have joined the companies and supported them in the first argument, as the information requested can reveal patterns of home life, mobility and other private life details of the companies' users.[15] Some District Courts have accepted these arguments and

---

[7] Hirschon et al., *supra* note 5, at 1.

[8] *See* JANETTE SADIK-KHAN & SETH SOLOMONOW, STREETFIGHT: HANDBOOK FOR AN URBAN REVOLUTION 4 (2016); *infra* Part I.

[9] Tess Hofmann, *Airbnb in New York City: Whose Privacy Rights Are Threatened by a Government Data Grab?*, 87 FORDHAM L. REV. 2589, 2589 (2019).

[10] Richard C. Schragger, *The Attack on American Cities*, 96 TEX. L. REV. 1163, 1227 (2018).

[11] *Id.* at 1165–66, 1172; KIM HADDOW ET AL., THE GROWING SHADOW OF STATE INTERFERENCE: PREEMPTION IN THE 2019 STATE LEGISLATIVE SESSIONS 4 (2019).

[12] Edelman & Stemler, *supra* note 4, at 147.

[13] Ruby Zefo, *Standing Up for Rider Privacy in Los Angeles*, MEDIUM: UBER SECURITY & PRIVACY (Mar. 24, 2020), https://medium.com/uber-security-privacy/ladot-mds-privacy-1eafbc412550 [https://perma.cc/2PHZ-5V3F].

[14] *See infra* Part I.

[15] Mana Azarmi, *Airbnb and HomeAway Challenge NYC's Mandatory Data Sharing Law*, CTR. FOR DEMOCRACY & TECH. (Oct. 9, 2018), https://cdt.org/blog/airbnb-and-homeaway

have granted preliminary injunctions blocking data sharing rules.[16] Others have rejected them, as they have found so far no significant privacy or surveillance-related harm arise from these ordinances.[17] The question is whether it should and could be possible for local governments to access that information to advance their equity and sustainability goals, without harming the legitimate privacy interests of both individuals and companies. As privacy organizations urge Appeals Courts to revive challenges against these ordinances, and several legislative bills in different states, including New York and California, propose tech companies to share some of the data, the jury is still out.[18]

This Article approaches this question by presenting some of the main data sharing programs and defining the legal regime that restricts and tolerates these companies, focusing on how that legal regime addresses (and fails to address) the privacy concerns that arise. Additionally, it presents an analysis of the way privacy laws and especially the Fourth Amendment are being mobilized to alter the distribution of power and welfare between local governments, companies, and citizens within current digital information capitalism, characterized by stark inequality—salient within large urban metropolitan areas—and corporate power concentration.[19] By doing so, the Article advances a two-pronged thesis: First, it challenges the narrow interpretation of the Fourth Amendment and existing privacy laws being put forward by some platforms and privacy advocacy groups. It shows that the goal of legal regimes that regulate surveillance, like the Fourth Amendment and its doctrine, is to ensure private actors are protected from power abuses and the information gathered about them is used with certain due-process requirements.[20] Consequently, what should be important is how the information is collected and shared and for what purposes, not specifically whether it is collected and shared, which opens space for data sharing

---

-challenge-nycs-mandatory-data-sharing-law/ [https://perma.cc/EG4Z-2G4M]; Rebecca Jeschke, *New York City Home-Sharing Ordinance Could Create Privacy Nightmare*, ELEC. FRONTIER FOUND. (Oct. 3, 2018), https://www.eff.org/deeplinks/2018/10/new-york-city-home-sharing-ordinance-could-create-privacy-nightmare [https://perma.cc/R56B-3U7D].

[16] *See* Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 490 (S.D.N.Y. 2019); Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 125 (D. Mass. 2019).

[17] *See, e.g.*, John Rossant, *CoMotion Conversations: LADOT's Seleta Reynolds on MDS' Victory in Court*, COMOTIONNEWS (Mar. 8, 2021), https://comotionnews.com/2021/03/08/comotion-conversations-ladots-seleta-reynolds-on-mds-victory-in-court/ [https://perma.cc/GTX5-9CXW].

[18] *See, e.g.*, Bennet Cyphers & Hayley Tsukayama, *Why Data-Sharing Mandates Are the Wrong Way to Regulate Tech*, ELEC. FRONTIER FOUND. (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/why-data-sharing-mandates-are-wrong-way-regulate-tech [https://perma.cc/5DLW-FYEQ]; *EFF, ACLU Urge Appeals Court to Revive Challenge to Los Angeles' Collection of Scooter Location Data*, ELEC. FRONTIER FOUND. (July 23, 2021), https://www.eff.org/pl/press/releases/eff-aclu-urge-appeals-court-revive-challenge-los-angeles-collection-scooter-riders [https://perma.cc/KY7K-GR4H].

[19] Cyphers & Tsukayama, *supra* note 18.

[20] Azarmi, *supra* note 15.

programs that are carefully tailored and include data-use provisions, despite the platforms' legal work to limit these programs. From a privacy law perspective, the Article shows that at present, consent-based regulations leave little room for actually protecting platforms' users and, as before, to protect individuals' informational self-determination rules that better define how information can be used should be advanced.[21] Second, the Article argues that if these technology companies succeed in their challenges, privacy law and constitutional law will have helped shield corporate power from regulatory oversight, advance a property-like treatment of personal data in which corporations' have an almost unrestricted right to decide who can access the information users and platforms co-produce and further submit local governments to corporate interests.[22] This would have been done while largely leaving individuals unprotected from the real risks data sharing ordinances pose.[23]

I. THE DATA SHARING PROGRAMS AT ISSUE AND GENERAL CONTEXT

Many of the technology companies providing city services are frequently described as, and describe themselves as, "platforms."[24] They provide amenities such as ride-hailing services, short-term rental services, delivery services and micro-mobility services.[25] Their platform business model relies on high-powered Internet connectivity, data collection, and a digital interface to connect and match riders with drivers, guests with hosts, pedestrians with scooters, users with applications or content, etc., through algorithmic processes that allow them to intermediate and facilitate all sorts of transactions at very low costs.[26] Central to the platform business model is an explicit attempt to build network economies and increase control over both supply and demand to achieve cost efficiencies and gain important leverage over the market overall.[27]

Popular platforms belong to what was formerly called the "sharing economy": companies that offer access to physical goods or services that have slack time, like cars, bikes, apartments or people's time.[28] Data analytics and connectivity allows these networks of goods and individuals to identify resources that are not being productive and tap that unutilized potential, and also monitor the use of resources by allowing

---

[21] *Id.*

[22] Cyphers & Tsukayama, *supra* note 18.

[23] *But see* G. S. Hans, *Curing Administrative Search Decay*, 24 B.U. J. SCI. & TECH. L. 1, 1 (2018); Hofmann, *supra* note 9, at 2589.

[24] Edelman & Stemler, *supra* note 4, at 147.

[25] *Id.* at 144.

[26] *Id.*

[27] Jack Karsten, *Sharing Economy Offers Flexibility and Efficiency to Consumers*, BROOKINGS (Jan. 9, 2017), https://www.brookings.edu/blog/techtank/2017/01/09/sharing-economy-offers-flexibility-and-efficiency-to-consumers/ [https://perma.cc/WT56-VHDY].

[28] *See* Yochai Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 YALE L.J. 273, 276–77 (2004).

people to use a car that would otherwise have been parked without the threat that it might get stolen, or run an errand at a moment they would have been doing nothing else.[29] These business models and organizational modes thrive in cities because cities are full of things with idle time, like parked cars, empty rooms, restaurant kitchens, or individuals with an hour to spare, and people with scarce time, seeking for a convenient ride, place to stay, food delivery, or people looking for jobs.[30] These needs can be efficiently placed and satisfied in the market with the aid of the digital affordances of platforms.[31]

One of the first large-scale platforms to have massive impact in cities was Uber.[32] When it first appeared in 2010, it challenged local transportation modes and regulations, and offered a very convenient new alternative. City and transportation officials all over the United States and the world called on the company to abide by existing taxi regulations, while the company argued that its service was fundamentally different.[33] By 2015, cities were already advocating for and adopting data sharing strategies to better understand the changes ride-sharing apps had brought, improve their overall planning capacity, and utilize as an important input for regulation.[34] The case was similar when Airbnb challenged the tourism industry, and contributed to the increase of housing prices in touristic city centers; Airbnb argued it was not a company offering touristic services directly, and tried to argue that tourism regulations should not apply to it.[35]

Most recently, it's been micro mobility services, and delivery services,[36] that have stormed into cities, challenged local stakeholders, offered new convenient

---

[29] M. Ritter & H. Schanz, *The Sharing Economy: A Comprehensive Business Model Framework*, 213 J. CLEANER PROD. 320, 320 (2019).

[30] Davidson & Infranca, *supra* note 1, at 218.

[31] *See* FED. TRADE COMM'N, *supra* note 5, at 1; Daniel E. Rauch & David Schleicher, *Like Uber, but for Local Government Law: The Future of Local Regulation of the Sharing Economy*, 76 OHIO STATE L.J. 901, 901 (2015); Davidson & Infranca, *supra* note 1, at 218.

[32] Avery Hartmans & Paige Leskin, *The History of How Uber Went From the Most Feared Startup in the World to its Massive IPO*, BUS. INSIDER (May 18, 2019), https://www.businessinsider.com/ubers-history [https://perma.cc/5ZGA-M9ZR].

[33] Brian O'Connell, *History of Uber: Timeline and Facts*, THE STREET (Jan. 2, 2020), https://www.thestreet.com/technology/history-of-uber-15028611 [https://perma.cc/5ZTU-8AET].

[34] Hirschon et al., *supra* note 5, at 1; NAT'L ASS'N OF CITY TRANSP. OFFS. & INT'L MUNICIPAL LAWS. ASS'N, NACTO POLICY 2019: MANAGING MOBILITY DATA, https://nacto.org/managingmobilitydata/ [https://perma.cc/H2C3-VXYZ] (last visited Apr. 26, 2022).

[35] *See, e.g.*, Zoe Greenberg, *New York City Looks to Crack Down on Airbnb Amid Housing Crisis*, N.Y. TIMES (July 18. 2108), https://www.nytimes.com/2018/07/18/nyregion/new-york-city-airbnb-crackdown.html [https://perma.cc/8RUE-ZQAJ].

[36] *See* Jasper Dekker, *One Day Deliveries Are Breaking Our Cities*, FAST CO. (Dec. 23, 2019), https://www.fastcompany.com/90442742/one-day-deliveries-are-breaking-our-cities; Marc Levy, *State Senate's Lack of Action to Cap Delivery Fees Inspires Harvard Square Restaurateur to Speak*, CAMBRIDGE DAY (Sept. 8, 2020), https://www.cambridgeday.com/2020/09/08/state-senates-lack-of-action-to-cap-delivery-fees-inspires-harvard-square-restaurateur-to-speak/ [https://perma.cc/A8Y8-8A93].

alternatives, and altered how some typical urban activities are done.[37] Electric scooters, as well as docked and dockless shared bikes, are collectively called "micro mobility services."[38] The business model of micro mobility companies consists of distributing dockless e-scooters and bikes across a city and "potential riders use their smartphones to unlock and pay for" a vehicle using a mobile app.[39] Micro-mobility services are often seen as offering a solution to address the first-mile/last-mile problem, make transport more accessible for underserved communities, and replace short car trips—in the United States, more than half of the car trips annually cover less than five miles.[40] Uber and Lyft both own and have heavily invested in some of the main e-scooter companies in the United States, like Lime and Motivate.[41]

Many public planners described the storming of scooters into cities as a déja vu—a repetition of their experience with ride-hailing services disrupting local transportation systems.[42] But some cities are also now planning ahead—Los Angeles Department of Transportation, as described below, is developing a data sharing infrastructure that, according to strategy reports commissioned by the city, should help it engage and manage autonomous cars and drones in the future.[43] The city also started a foundation with many other cities from around the world to share this standard and develop more standards to manage new technology urban services.[44]

The following subsections describe three examples of mandatory data sharing programs enacted by different cities, and what the cities did with that information. These subsections also describe the strategies of some of these platforms in challenging these ordinances: through litigation, by arguing the ordinances contravene privacy

---

[37] *See* Dekker, *supra* note 36; Levy, *supra* note 36.

[38] *See, e.g.*, Rasheq Zarif et al., *Small Is Beautiful*, DELOITTE INSIGHTS (Apr. 16, 2019), https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/micro-mobility-is-the-future-of-urban-transportation.html [https://perma.cc/V9J2-VX4R].

[39] POPULUS, THE MICRO-MOBILITY REVOLUTION: THE INTRODUCTION AND ADOPTION OF ELECTRIC SCOOTERS IN THE UNITED STATES 4 (2018), https://research.populus.ai/reports/Populus_MicroMobility_2018_Jul.pdf [https://perma.cc/KV9E-PLK5].

[40] *See, e.g.*, Zarif et al., *supra* note 38. The "first-mile/last-mile" problem refers to the gap that occurs between where public transit is and where individual users need it to be—the distance between home, work, etc., and a bus stop or subway station, which may be great enough to impede use of those resources, and ultimately causing some individuals to turn away from public transit and toward private vehicles. *See id.*

[41] Megan Rose Dickey, *Lyft Outlines Bike and Scooter Plans*, TECHCRUNCH (July 16, 2018), https://techcrunch.com/2018/07/16/lyft-outlines-bike-and-scooter-plans/ [https://perma.cc/YN63-GQG2].

[42] *See, e.g.*, Zarif et al., *supra* note 38; POPULUS, *supra* note 39, at 8–9; Aarian Marshall, *Still Smarting from Uber, Cities Wise up About Scooter Data*, WIRED (Sept. 10, 2018), https://www.wired.com/story/cities-scooter-data-remix-uber-lyft/ [https://perma.cc/VRR7-N9FD].

[43] Ashley Z. Hand, URBAN MOBILITY IN A DIGITAL AGE: A TRANSPORTATION TECHNOLOY STRATEGY FOR LOS ANGELES 1 (2016).

[44] *Id.*; *FAQs*, OPEN MOBILITY FOUND., https://www.openmobilityfoundation.org/faq/ [https://perma.cc/W8TB-B7P9] (last visited Apr. 26, 2022).

and due process rights, as this Article will mostly focus on, but also alongside other strategies to avoid or preempt local regulation in general.

A. New York City's Data Sharing Program with the Ride-Hailing Industry

The first and most paradigmatic example of a mandatory data sharing program comes from New York City and its data sharing rules for ride-hailing companies.[45] New York City moved to use that data to enact minimum wage rules for ride-hailing drivers.[46] Ride-hailing companies connect drivers and passengers through an app; the best-known and largest companies in the United States are Uber and Lyft.[47] These companies offer very convenient and efficient transportation options for users, but their business models also raise questions about equity, sustainability, and safety.[48] In particular, whether and how they contribute to decreased or increased congestion, whether they compete fairly with taxi drivers (who must typically buy a medallion to operate), and the adequate classification of the drivers that work on these apps as employees or independent contractors as a means to address the precarity of their work.[49]

In 2016, the New York City's Taxi and Limousine Commission (TLC) started requiring ride-sharing companies to report the following information: pickup time and location of each trip, license numbers of the driver and vehicle performing the trip.[50] The rule was enacted following the long-established requirement for Taxis in the City to provide credit and debit card payment services for customers and transmit data, similar to TLC data, about trips made by taxi drivers gathered by a GPS installed in the card terminal.[51] Prior to the implementation of the rule, TLC required

---

[45] Aarian Marshall, *NYC Now Knows More Than Ever About Your Uber and Lyft Trips*, WIRED (Jan. 31, 2019), https://www.wired.com/story/nyc-uber-lyft-ride-hail-data/.

[46] *Id.*

[47] Janine Perri, *Uber vs. Lyft: Who's Top in the Battle of U.S. Rideshare Companies*, BLOOMBERG SECOND MEASURE (Jan. 14, 2022), https://secondmeasure.com/datapoints/rideshare-industry-overview/ [https://perma.cc/N9XK-MWP6].

[48] Dubal, *supra* note 4, at 124–25.

[49] *Id.* at 78. Their impact on the overall workforce, however, does not seem as significant as originally expected. According to the Bureau of Labor Statistics, only about 7% of the U.S. labor force are independent contractors. *See Contingent and Alternative Employment Arrangement—May 2017*, BUREAU OF LAB. STATS. (June 7, 2018), https://www.bls.gov/news.release/pdf/conemp.pdf; Sarah Holder, *There's One Thing Uber Hasn't Disrupted: Work.*, BLOOMBERG CITYLAB (June 8, 2018), https://www.bloomberg.com/news/articles/2018-06-08/a-reality-check-on-uber-s-employment-impact [https://perma.cc/VU3S-DND8].

[50] *See Notice of Public Hearing and Opportunity to Comment on Proposed Rules*, N.Y.C. TAXI AND LIMOUSINE COMM'N, https://www1.nyc.gov/assets/tlc/downloads/pdf/proposed_rule_rev_driver_fatigue_1_5_17.pdf [https://perma.cc/XYL3-8VW6].

[51] N.Y.C. TAXI AND LIMOUSINE COMM'N (Mar. 30, 2004), https://www1.nyc.gov/assets/tlc/downloads/pdf/press_releases/press_04_03_a.pdf [https://perma.cc/GHJ3-PQUQ].

drivers to provide this same information as a handwritten record.[52] The City's Department of Transportation used these data to evaluate traffic in the city, increase new pedestrian space, and improve traffic—for example, in Times Square.[53] In 2010, TLC also used the data to discover that some drivers were overcharging passengers, and used that information to revoke the permit of some of the drivers involved.[54] These ordinances were part of a wider strategy of Michael Bloomberg's tenure as Mayor—which was then followed by Mayor Bill de Blasio—that focused on harnessing the digital economy as a means for growth, loosening the City's economic dependence on the financial sector after the financial crash of 2008, using growth as a means for social policy, and modernizing the local government itself, thus making policymaking more efficient.[55]

The City had the authority to request these data under the "Vision Zero" program, a citywide initiative backed by state regulation to diminish traffic-related deaths and injuries launched in 2014.[56] The first local bills supporting the initiative sought to enhance traffic data collection, boost enforcement efforts and codify safety engineering commitments, and update the City's legal code to enhance penalties for dangerous driving.[57] Meera Joshi, who was commissioner of the TLC at the time, explained that one of the reasons behind these rules is the difficulty in regulating ride hailing companies while also understanding the impacts of the rules, because only the company knows information such as how many cars are on the streets, the length of trips taken, and what passengers pay.[58] As Joshi told the *New York Times*, "[w]ithout the ability to double check, then all the public and lawmakers are left with are unfounded statements about what happens when they pass this law."[59] At the state level, legislation was passed that empowered the City to lower citywide speed limits and increase the number of school speed zones.[60]

---

[52] N.Y.C. TAXI & LIMOUSINE COMM'N, 2014 TAXI CAB FACTBOOK (2014); Neil Thakral & Linh T. To, *Daily Labor Supply and Adaptive Reference Points*, 111 AM. ECON. REV. 2417, 2421 (2021).

[53] *See* Janette Sadhik-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. 02, 2017), https://www.nydailynews.com/opinion/uber-dishonest-data-dance-article-1.2961487 [https://perma.cc/NGK3-7LRX].

[54] Editorial Board, *Taxi Rip-Off*, N.Y. TIMES (Mar. 16, 2010), https://www.nytimes.com/2010/03/17/opinion/17wed3.html?searchResultPosition=1 [https://perma.cc/9MF2-VBVP].

[55] *See generally* SHARON ZUKIN, THE INNOVATION COMPLEX: CITIES, TECH, AND THE NEW ECONOMY (2020).

[56] *Vision Zero*, CITY OF NEW YORK, https://www1.nyc.gov/content/visionzero/pages/ [https://perma.cc/38DA-6ZJR] (last visited Apr. 26, 2022).

[57] *Vision Zero: Legislation*, CITY OF NEW YORK, http://www.nyc.gov/html/visionzero/pages/initiatives/legislation.shtml [https://perma.cc/CJM4-L4W4] (last visited Apr. 26, 2022).

[58] Shira Ovide, *An Uber Wage Experiment Worked*, N.Y. TIMES (Oct. 1, 2020), https://www.nytimes.com/2020/10/01/technology/uber-wages-new-york.html.

[59] *Id.*

[60] *Vision Zero: Legislation*, *supra* note 57.

The data requested was expected to allow the Commission to establish the maximum number of hours that licensed taxi and ride-hailing drivers could work, amidst concerns about drivers working too many hours.[61] The original proposed rule contemplated collecting only pickup time, and counting a "pickup" as one hour of work, which would be tallied against the limit.[62] According to the City's documents, several ride-hailing companies argued that it would be more accurate to use trip duration to calculate driving hours (most trips are shorter than an hour), because a calculation based on trip duration provides a more accurate way to identify drivers at risk of fatigue.[63] With the voluntarily produced trip records (which included pickup and drop-off times), in December 2016, the City proposed rules setting a cap on the amount of time per day that taxi and ride-share drivers could spend transporting passengers.[64] It also added additional trip data-reporting requirements for ride-hailing companies, as the enforcement of the proposed rules would rely on TLC's monthly review of trip records.[65]

Uber, however, launched a public campaign against the rules using the hashtag #TLCDontTrackMe, and sending its users an email warning against the privacy risks of the regulation.[66] Prominent privacy advocacy groups supported Uber's complaint and urged the Commission not to adopt these requirements, or to tailor them more narrowly.[67] The organizations highlighted that the proposed rules also could create particular risks if the data became publicly available through Freedom of Information requests, that the rules were unclear on how the information would or could be shared among city departments, and that the information could be de-identified, revealing passengers' identities.[68] They also emphasized that it was unclear how the collection of precise location information would achieve the goal of reducing the risks associated with fatigued driving, and that the agency could tailor the data collection

---

[61] *Notice of Promulgation of Rules*, N.Y.C. TAXI AND LIMOUSINE COMM'N, at 2, https://www1.nyc.gov/assets/tlc/downloads/pdf/proposed_rule_rev_driver_fatigue_2_2_17.pdf [https://perma.cc/UPE3-XURL].

[62] *Id.* at 1.

[63] *Id.* at 2.

[64] *Id.* ("Many stakeholders, including FHV bases, argued that it would be more accurate to use trip duration to calculate driving hours. TLC delayed implementation of the driver fatigue rules to explore this method for calculating driving hours as a means of establishing safe daily and weekly driving limits. In the fall of 2016, several FHV bases voluntarily produced trip records that included both pickup and drop-off times, allowing TLC to calculate trip durations. TLC then analyzed both FHV and taxi trip records and determined that a calculation based on trip duration provides a more accurate way to identify drivers at risk of fatigue.").

[65] *Id.* at 3–4.

[66] Gaby Del Valle, *Citing Privacy Concerns, Uber Fights City's Plan to Track Drivers' Trips*, GOTHAMIST (Jan. 5, 2017), https://gothamist.com/news/citing-privacy-concerns-uber-fights-citys-plan-to-track-drivers-trips [https://perma.cc/WFC2-D5HE].

[67] Letter from Ctr. for Democracy & Tech. et al. to N.Y.C. Taxi & Limousine Comm'n 1 (Dec. 26, 2016), https://fpf.org/wp-content/uploads/2016/12/TLC-Fatigue-Comments-from-FPF-CDT-EFF-Constitution-Project-and-Tech-Freedom.pdf [https://perma.cc/4VW3-9R4W].

[68] *Id.* at 1–2.

more narrowly.[69] Lastly, they also argued that it should enact policies and procedures that detail the privacy and security protections for such sensitive data.[70]

The City adopted some of these suggestions, and the revised version of the rules did not require driver or vehicle license number, and the pickup and drop-off location data was limited to the closest intersection instead of specific addresses, and required them to indicate when trips were shared.[71] The final rule also capped taxi and for-hire vehicles from transporting passengers for more than 10 hours in any 24-hour period, and for more than 60 hours in a calendar week.[72]

Early in 2018, TLC used the data it collected from ride-hailing companies to determine that 96 percent of the 80,000 app drivers were making less than the equivalent of a minimum wage.[73] The Council voted for a one-year cap on new for-hire vehicle licenses, unless for wheelchair accessible cars, and empowered the TLC to set minimum pay rates.[74] The TLC mandated a minimum wage of $17.22 per hour for ride-share drivers ($15 minimum wage plus $2.22 they would owe in payroll taxes).[75] New York City became the first city in the world to enact pay protection for ride-hailing professional drivers, and the rule became effective in February 2019.[76] The trip pay standard took into account that ride-hailing drivers were not paid by the hour but per trip, and also established that the minimum be raised if a company could not keep drivers busy and utilize them effectively.[77] According to Joshi, the data collected allowed TLC to take into account cruise time and consider incentives in the rules to avoid oversaturation and keep their drivers busy.[78] Joshi estimated that drivers would earn about $10,000 more per year with the new standard.[79]

Lyft and Juno challenged the minimum payment rules in 2019, arguing they were biased towards Uber, because since Uber does most of the City's app-based car

---

[69] *Id.* at 2–3.

[70] *Id.* at 3.

[71] *Notice of Promulgation of Rules*, *supra* note 61, at 3–4.

[72] *Id.* at 5.

[73] Press Release, N.Y.C. Taxi & Limousine Comm'n, TLC Announces Passage of Sweeping Rules to Raise Driver Earnings (Dec. 4, 2018), https://www1.nyc.gov/assets/tlc/downloads/pdf/press_release_12_04_18.pdf [https://perma.cc/H6UD-NJLF].

[74] Andrew Millman, *Former City Taxi Commissioner on Regulating the App Companies and Saving the Yellows*, GOTHAM GAZETTE (May 13, 2019), https://www.gothamgazette.com/city/8521-former-city-taxi-commissioner-on-regulating-the-app-companies-and-saving-the-yellows [https://perma.cc/C6WN-7M5T].

[75] *Id.*

[76] N.Y.C. TAXI & LIMOUSINE COMM'N, *End of Tenure Remarks from Meera Joshi, the Outgoing Chair of the New York City Taxi and Limousine Commission, at Crain's New York Business Breakfast*, MEDIUM (Jan. 25, 2019), https://medium.com/@NYCTLC/end-of-tenure-remarks-from-meera-joshi-the-outgoing-chair-of-the-new-york-city-taxi-and-limousine-a414eb3bd7f5 [http://perma.cc/26zJ-W5ZW].

[77] *Id.*

[78] *Id.*

[79] *Id.*

rides, the procedure for calculating per trip were biased in their competitor's favor.[80] In May 2019, a state lower court upheld the rule,[81] and in December 2020, the Appellate Division affirmed.[82] The court said that TLC's rate-setting method "has a rational basis and is not unreasonable," which is the legal requirement the rule had to meet.[83] None of the challenges referred to the data-reporting element of it.[84] Despite these challenges, the New York rules have been considered an overall success; arguments from companies that passengers and drivers would wind up worse off due to increased fares and lost work have not proven true.[85] The rules have largely accomplished what they intended—paying drivers more while limiting fatigue—all while companies earned even more, because people have not been significantly discouraged from riding with ride-hailing companies despite price increases.[86] As a downside to the TLC rules, there were fewer open positions for new drivers, and not all drivers could work whenever they wanted.[87]

A December 2020 report by Dmitri Koustas, James Parrott, and Michael Reich—from the University of Chicago, the New School, and UC Berkeley, respectively—studied the bundle effects of the policies enacted by TLC (the minimum wage and the cap), plus congestion pricing introduced by New York State.[88] They found that:

> While passenger fares rose after a several month period in tandem with driver pay, passenger fares also rose by a similar amount in Chicago—in the absence of a pay standard. The observed raw fare increases in New York City may therefore not all be due to the result of the pay standard. At the same time, since prices increased, but trip volumes did not, company revenues increased.

---

[80] Brief for Petitioner-Appellant at 33–34, Tri-City, LLC v. N.Y.C. Taxi and Limousine Comm'n, 138 N.Y.S. 3d 30 (N.Y. App. Div. 2020).

[81] *Tri-City*, 138 N.Y.S. at 30.

[82] *Id.* at 31.

[83] *Id.*; Clayton Guse, *Lyft Loses Effort to Sink NYC's Minimum Wage Law for e-Hail Drivers*, N.Y. DAILY NEWS (Dec. 22, 2020), https://www.nydailynews.com/new-york/ny-lyft-minimum-wage-lawsuit-appeal-20201222-c5yaaxk4dfdh5gptcrpcw32jre-story.html [https://perma.cc/LT8V-H7Y2].

[84] *See Tri-City*, 138 N.Y.S. at 31.

[85] Ovide, *supra* note 58.

[86] *Id.* This achievement was also important, because ride-shares are both popular and beneficial, especially for the boroughs outside Manhattan. Millman, *supra* note 74. The effect on those areas was an important concern when the cap legislation was passed. *Id.*

[87] Ovide, *supra* note 58.

[88] Dmitri Koustas et al., *New York City's Gig Driver Pay Standard: Effects on Drivers, Passengers, and the Companies*, THE NEW SCH. CTR. FOR N.Y.C. AFFS. 1 (2020), https://irle.berkeley.edu/files/2020/12/NYC-gig-driver-pay-standard-December-8-2020.pdf [https://perma.cc/L6HV-ZTG7].

> Our findings here are consistent with a conclusion that New York City's driver pay standard achieved its main objectives. The standard raised driver pay without significantly dampening growth in trip volume, beyond what might be expected in a maturing market. Moreover, passenger wait times declined significantly.[89]

The latter finding was because Uber and Lyft compete by keeping passenger wait time low.[90] In a related research project, Michael Reich and coauthors found that minimum wages and earned income tax credits have a direct effect on diminishing non-substance-related suicides—so-called "deaths of despair."[91]

As of early 2020, the TLC strips the data of identifying information and makes it available to the public to "help businesses distinguish new business opportunities from saturated markets, encourage competition, and help investors follow trends."[92] In an interview, former commissioner Joshi said she hoped other cities would see the TLC's rules as a model.[93]

Starting in 2018, however, adopting such a strategy has become harder for many cities in the United States.[94] A report by the National Employment Law Project details how, around 2018, ride-sharing companies aggressively lobbied state legislators to obtain regulation that protected their interests.[95] The resulting regulations created a presumption of independent contractor status for drivers or prohibited local governments from regulating them.[96] Thirty-seven states preempted local regulation of ride-sharing companies.[97]

---

[89] *Id.* at 14.

[90] *Id.* at 10.

[91] William H. Dow et al., *Can Labor Market Policies Reduce Deaths of Despair?*, 74 J. HEALTH ECON. 1 (Dec. 2020).

[92] Today, TLC collects information on the location of pickup & drop-off of each trip, the route taken, whether the trip touches on congestion zones, date and time of pickup & drop-offs, date and time of driver's log on and off the app, driver payment, passenger fare and deductions from diver payment and vehicle and driver identifier, among others. It does not receive passenger information. As TLC notes, they "require only the data necessary to understand traffic patterns, working conditions, vehicle efficiency, service availability, and other important information." N.Y.C. Taxi & Limousine Comm'n, *What Makes a City Street Smart*, MEDIUM (Jan 13, 2019), https://medium.com/@NYCTLC/what-makes-a-city-street-smart-23496d92f60d [https://perma.cc/5GSF-A9KP].

[93] Ovide, *supra* note 58.

[94] NAT'L EMP. L. PROJECT, RIGHTS AT RISK: GIG COMPANIES' CAMPAIGN TO UPEND EMPLOYMENT AS WE KNOW IT 11 (2019), https://s27147.pcdn.co/wp-content/uploads/Rights-at-Risk-4-2019.pdf [https://perma.cc/4BEN-CQUD].

[95] *Id.* at 3.

[96] *Id.*

[97] *See* Schragger, *supra* note 11, at 1172.

Other cities have partnered with ride-hailing companies to access some of their data.[98] They have done so through voluntary agreements.[99] Washington DC has used voluntarily rendered Uber and Lyft data to redesign parking areas in Dupont Circle and decrease congestion.[100] Uber has also created its own data sharing platform called Uber Movement, yet many policymakers dislike it because the data released is too aggregated and is therefore of little use for public planning.[101]

B. New York and Boston's Data Sharing Ordinances for Short-Term Rentals

A similar data-reporting requirement has been implemented in local short-term rental regulations that were issued in response to the increase in popularity of platforms like Airbnb and HomeAway, which provide an online service where hosts and guests can offer and receive informal accommodations.[102]

Like ride-hailing platforms, short-term rental platforms provide an opportunity for individuals to earn extra income by renting their homes, and also may make travel more accessible and convenient.[103] They have become an important element of the tourism industry.[104] Their activities, however, have also raised concerns from local governments and local communities: they may often violate local zoning laws and are perceived as contributing to the rise of housing prices in many large cities.[105] When local rules provide *de minimis* exceptions for short-term rentals, hosts often

---

[98] *See* Rebecca Bellan, *Cities, Mobility Companies Agree to 7 Guidelines to Keep Rider Data Private*, TECHCRUNCH (Oct. 29, 2021, 10:35 AM), https://techcrunch.com/2021/10/29/private-and-public-sector-come-together-to-create-privacy-principles-for-mobility-data/ [https://perma.cc/9W2K-FK4Q].

[99] *Cf.* Daniel C. Vock, *4 Ways Uber is Changing the Way it Works with Cities*, GOV'T TECH. (Apr. 12, 2018), https://www.govtech.com/transportation/4-ways-uber-is-changing-the-way-it-works-in-cities.html [https://perma.cc/2RVP-ZYZC].

[100] *See* Benjamin Schneider, *D.C. Gives Uber and Lyft a Better Spot in Nightlife*, BLOOMBERG CITYLAB (Oct. 25, 2017, 2:11 PM), https://www.citylab.com/transportation/2017/10/a-dc-neighborhood-rethinks-parking/543870/ [https://perma.cc/R428-VY9K].

[101] *See* Sadhik-Khan, *supra* note 53.

[102] *See generally Reporting Law, For Hosts*, N.Y.C. OFF. OF SPECIAL ENFORCEMENT, https://www1.nyc.gov/site/specialenforcement/reporting-law/reporting-for-hosts.page [https://perma.cc/7WA8-XR5E] (last visited Apr. 26, 2022). Through their interface, the platform helps guest search for properties based on different points of information and their history using the platforms services, and help hosts describe and market their properties. Typically, the platforms limit the information hosts and guests have of each other to ensure its place as intermediating the transactions. *See* Edelman & Stemler, *supra* note 4, at 158–59.

[103] *See* Abbey Stemler, *Betwixt and Between: Regulating the Shared Economy*, 43 FORDHAM URB. L.J. 32, 48–52 (2016); CJ Arlotta, *Airbnb Continues to Dominate Short-Term Rental Market*, HOTEL BUS. (Feb. 3, 2017), http://hotelbusiness.com/Other/Airbnb-Continues-to-Dominate-Short-Term-Rental-Market/56245 [https://perma.cc/5TBU-HJBD].

[104] *See* Stemler, *supra* note 103, at 40–41.

[105] *See, e.g.*, Daniel Guttentag, *What Airbnb Really Does to a Neighborhood*, BBC (Aug. 30, 2018), https://www.bbc.com/news/business-45083954 [https://perma.cc/22BF-VW4F].

offer their properties continually, exceeding the term of the exception.[106] Similarly, many jurisdictions impose taxes on short-term rentals, yet these are largely unpaid.[107]

By 2016, however, Airbnb had challenged in court more than half a dozen local ordinances.[108] It typically argued that it was an internet intermediary and not an operator of tourism services and, thus, that it was outside of the cities' jurisdiction, so these regulations should not apply to it directly, only to its users.[109] As judges, however, started finding that the company was exercising enough control over these transactions to be operating tourism services, the company started changing its strategy.[110] As a means to facilitate the enforcement of local laws, many of these ordinances required platforms to share different types of data with the city.[111] In 2019 alone, the company settled lawsuits with three major U.S. cities—New York, Boston, and Miami Beach—and agreed to turn over much of the requested data.[112] In what follows, this Article describes the ordinances and the litigation that took place before the agreements, mainly in New York City with a brief comparison highlighting the differences with the case in Boston.

1. Local Law 146 and *Airbnb v. New York*

New York City's Local Law 146 of 2018 required home-sharing platforms to share host information with the City's Committee on Housing and Buildings.[113] The information requested included the physical address of the premises; the legal name, phone number, email, address and physical address of the host, and the URL and other identifications of the listing on the platform's website.[114] The law also contemplated

---

[106] *See* Edelman & Stemler, *supra* note 4, at 149–50; *see also* David Streitfeld, *Airbnb Listings Mostly Illegal, New York State Contends*, N.Y. TIMES (Oct. 15, 2014), https://www.nytimes.com/2014/10/16/business/airbnb-listings-mostlyillegal-state-contends.html [https://perma.cc/7KVQ-VZR7] (discussing how home rental services violate regulations).

[107] *See, e.g.*, Ann Carrns, *Lodging Taxes and Airbnb Hosts: Who Pays, and How*, N.Y. TIMES (June 16, 2015), https://www.nytimes.com/2015/06/17/your-money/lodging-taxes-and airbnb-hosts-who-pays-and-how.html [https://perma.cc/CWK2-66AV].

[108] *See* Olivia Carville, Andre Tartar & Jeremy C.F. Lin, *Airbnb to America's Big Cities: See You in Court*, BLOOMBERG (Feb. 14, 2020), https://www.bloomberg.com/graphics/2020-airbnb-ipo-challenges/ [https://perma.cc/ZA3L-VY63].

[109] *See, e.g.*, Complaint for Declaratory and Injunctive Relief at ¶¶ 43–45, Airbnb, Inc. v. City and County of San Francisco, 217 F. Supp. 3d 1066 (N.D. Ca. 2016).

[110] *See, e.g.*, Homeaway.com, Inc., v. City of Santa Monica, No. 2:16-cv-00641, 2018 WL 3013245, at *3–4 (C.D. Ca. June 14, 2018).

[111] Edelman & Stemler, *supra* note 4, at 158–59.

[112] Paris Marineau, *Airbnb Starts to Play Nice with Cities*, WIRED (Aug. 3, 2019, 07:00 AM), https://www.wired.com/story/airbnb-starts-play-nice-cities/ [https://perma.cc/BQE5-CC4J].

[113] Zoe Greenberg, *New York City Looks to Crack Down on Airbnb Amid Housing Crisis*, N.Y. TIMES (Jul. 18, 2018), https://www.nytimes.com/2018/07/18/nyregion/new-york-city-airbnb-crackdown.html [https://perma.cc/8RUE-ZQAJ].

[114] N.Y.C. ADMIN. CODE § 26-2102 (2019).

a fine of up to $1500 per listing per month if accurate information was not submitted.[115] The bill was described as part of "one of the most fractious battles in New York City to regulate companies of the so-called sharing economy,"[116] and the information was expected to facilitate the enforcing of the local provisions that limited short-term rentals in most buildings in the city, as short-term rentals were perceived as aggravating the city's housing crisis.[117]

Airbnb and HomeAway filed suit against the city, claiming that the ordinance violates the First and Fourth Amendment of the Constitution and conflicted with the Stored Communications Act (SCA).[118] This section focuses on the Fourth Amendment and SCA claims.

Airbnb and HomeAway argued, first, that "the Ordinance mandates the warrantless seizure of business records protected by the Fourth Amendment, without giving the platforms—the subjects of these 'administrative searches'—an opportunity for pre-compliance review before a neutral decision-maker."[119] Second, they argued that the rule was preempted by the SCA, under which "a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service . . . to any governmental entity."[120] Within a few weeks, they moved to preliminarily enjoin the enforcement of the ordinance.[121]

Prominent privacy advocacy groups supported the platform's arguments; they said that the local law was unconstitutional and preempted, because the requested information could reveal patterns of home life, vacations, and other private details of homeowners without any allegation of wrongdoing.[122] They also emphasized that most of the hosts whose data would have to be reported were not commercial entities, but rather individuals renting out their home, that location being a "traditional bedrock of Fourth Amendment protections."[123]

---

[115] *Id.*

[116] Luis Ferré-Sadurní, *To Curb Illegal Airbnbs*, *New York City Wants to Collect Data on Hosts*, N.Y. TIMES (Jun. 26, 2018), https://www.nytimes.com/2018/06/26/nyregion/illegal-airbnb-new-york-city-bill.html?searchResultPosition=1 [https://perma.cc/NV7T-HJV6].

[117] Greenberg, *supra* note 113; Hofmann, *supra* note 9, at 2598.

[118] The lawsuits also allege violations of the First Amendment and the New York State Constitution, but those claims are beyond the scope of this Article. *See* Airbnb v. City of New York, 373 F. Supp. 3d at 476.

[119] *Id.* at 480.

[120] *Id.* at 477; 18 U.S.C. §§ 2702(a)(3), (c)(1); § 2703(c).

[121] Airbnb v. City of New York, 373 F. Supp. 3d at 474, 476. Additional similar charges are that the law violated Article 1 of New York Constitution, which also guarantees them the right to be free from unreasonable searches, seizures and interceptions, and that the law violated the platforms' First Amendment rights because it compelled them to communicate to their users that they must consent to the sharing of their data with the city. *Id.* at 477.

[122] *See* Jeschke, *supra* note 15.

[123] *See* Azarmi, *supra* note 15.

The City argued that the platforms had no protected privacy interest over the data sought by the ordinance because the data related to the users of the platforms, not the platforms themselves,[124] and that the platforms had already forfeited the right to claim privacy interests in the records, as they already alerted users that they may disclose customer information to regulators and had complied with past subpoenas.[125]

The judge, however, found that the requests were likely to abridge the platforms' Fourth Amendment rights to the privacy of their business records.[126] According to the judge, the data sharing requirement was equivalent to an untailored administrative search; the ordinance covered every booking without any factual basis to suspect that any particular listing violated other local regulations.[127] With this untailored ordinance, there was no offering of opportunity for pre-compliance review.[128] The judge relied on *City of Los Angeles vs. Patel*,[129] a 2015 decision in which the Court held that a provision of the Los Angeles municipal code requiring motel owners to keep records with specific personal information about their guests and authorized warrantless on-site inspections of those records upon the demand of any officer of the Los Angeles Police Department was unconstitutional.[130] In an en banc decision, the Ninth Circuit determined that a police officer's nonconsensual inspection of hotel records under the contested rule was a "Fourth Amendment 'search' because '[t]he business records covered . . . are the hotel's private property' and the hotel therefore 'has the right to exclude others from prying into the[ir] contents.'[131] The Supreme Court affirmed.[132]

Importantly, much of the court's reasoning in *Airbnb v. New York City* relied on the assumption that the data requested by the City were part of the company's business records.[133] Citing *Patel*, the court said that platforms have "a possessory and ownership interest" in that information, which in turn translated into a reasonable expectation of privacy.[134] Part of the court's motivation might have been the

---

[124] Airbnb v. City of New York, 373 F. Supp. 3d at 483.
[125] *Id.* at 483–85.
[126] *Id.* at 485.
[127] *Id.* at 491.
[128] *Id.* at 493–94.
[129] City of Los Angeles v. Patel, 576 U.S. 409 (2015).
[130] *See id.*
[131] *Id.* at 414.
[132] *Id.* at 414–15.
[133] Airbnb v. City of New York, 373 F. Supp. 3d at 493–84.
[134] *Id.* at 483–84 ("First, [the city] argues that the home-sharing platforms do not have a protected privacy interest in the data sought by the Ordinance, because this data largely relates to users of the platforms, not the platforms themselves. That argument is foreclosed by Patel. The data sought there by the municipal regulation . . . also largely originated with guests, not the hotel operators. But the Supreme Court in Patel implicitly recognized . . . that the records at issue were ones in which the hotel owners had a reasonable expectation of privacy. As the Ninth Circuit put the point in explaining why the Fourth Amendment protects

privacy risks sharing this information posed.[135] It noted that "the scale of the production that the Ordinance compels each booking service to make is breathtaking . . . . Had it been in effect in 2016, the Ordinance thus would have compelled Airbnb to produce user data as to each of the more than 700,000 bookings executed that year over Airbnb's platform."[136]

In any case, the court did not find that the ordinance violated the SCA.[137] As the court said, "[B]oth Airbnb and HomeAway already condition use of their services on hosts accepting privacy policies that, among other things, notify hosts that the information they provide may be disclosed to governmental authorities."[138] Lastly, the court noted that if enforcement in this area was a city priority, the City could issue more subpoenas to the platforms.[139]

About a month after the decision, the City issued five subpoenas against Airbnb and HomeAway, asking for the data of roughly 20,000 hosts identified by the City who might have violated the local home sharing rules.[140] Airbnb contested, but a judge ordered Airbnb to turn over all the data. Airbnb then reached an agreement with the City to periodically hand in anonymized information about listings, which City officials can request to be de-anonymized for use in an investigation of illegal short-term rentals.[141] The City seems to have appealed the first decision before the Second Circuit, but Airbnb seems to have reached a settlement with the City.[142]

2. Docket #0764 and *Airbnb v. Boston*

The case in Boston was somewhat different. In June 2018, Boston enacted Docket #0764, an ordinance regulating short-term rentals.[143] The ordinance limited the type of properties eligible for short-term rentals, restricted how many days per year a property may be rented through a platform, required that units register before

---

a hotel from unreasonable seizures of records that it prepares and maintains as to its guests: The business records covered by [the challenged ordinance] are the hotel's private property, and the hotel therefore has both a possessory and an ownership interest in the records.").

[135] *Id.* at 484.

[136] *Id.* at 490–91.

[137] *Id.* at 497.

[138] *Id.* at 496–97.

[139] *Id.* at 500.

[140] Sara O'Brien, *Airbnb Subpoenaed by New York City for Data on Listings*, CNN BUS. (Feb. 19, 2019), https://www.cnn.com/2019/02/19/tech/airbnb-subpoena-new-york-city/index.html [https://perma.cc/L555-UTJP].

[141] Paris Marineau, *Airbnb and New York City Reach an Agreement on Home-Sharing Data*, WIRED (May 24, 2019), https://www.wired.com/story/airbnb-new-york-city-reach-truce-on-home-sharing-data/ [https://perma.cc/KCJ2-A9LM].

[142] *See* Stipulation of Voluntary Dismissal, Airbnb v. City of New York, 373 F. Supp. 3d (S.D.N.Y. 2020) (No. 18-CV-7712-161).

[143] BOS. MUNICIPAL CODE § 9-14.11.

being listed, and established penalties for individuals and platforms who operate short term rentals that were not eligible under the ordinance.[144]

To enforce the penalties, the rule contained a "data provision," under which platforms had to provide the City with an electronic report "of the listings . . . for the applicable reporting period. The report shall include a breakdown of where the listings are located, whether the listing is for a room or a whole unit, and shall include the number of nights each unit was reported as occupied during the applicable reporting period."[145] It did not require the full legal name of the hosts, their address, or their phone number, and thus was, in its scope, less broad than the New York City ordinance.[146] Nevertheless, Airbnb sued the City in November 2018, arguing that the data provision violated the Fourth Amendment and the SCA.[147]

This time, the judge found that Airbnb had not established that all information was part of its private business records, in part because much of the information requested is publicly available online.[148] The court said that:

> To the extent the data provision compels Airbnb to provide monthly lists limited to information appearing in its public listings for Boston rental properties . . . the Court finds Airbnb has not established a likelihood that it will succeed in its SCA or Fourth Amendment challenges. Neither Airbnb nor its users can reasonably claim an expectation of privacy in information included in public listings, and Airbnb has not established that a list containing only those two categories of information is a private business record subject to Fourth Amendment protection.[149]

However, regarding the number of nights a listing was occupied in a given period (information not listed online), the court found that Airbnb had a reasonable expectation of privacy in the nonpublic usage data for its listings and would be "irreparably harmed by having to comply with an unconstitutional requirement that it disclose private business information."[150] Consequently, the court enjoined this element of the Ordinance.[151]

---

[144] *Id.*

[145] *Id.*

[146] *See supra* note 114.

[147] The lawsuits also allege violations of Section 230 of the Communications Decency Act (CDA), and the First and Fourteenth Amendment. For an analysis of the claims under Section 230 of the CDA, see Edelman & Stemler, *supra* note 4; Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 118 (D. Mass 2019).

[148] Airbnb v. City of Boston, 386 F. Supp. 3d at 124–25.

[149] *Id.* at 124.

[150] *Id.* at 125.

[151] *Id.*

As in New York, in August 2019, Boston and Airbnb reached a settlement agreement under which the platform helps facilitate the adoption of Boston's short-term rental restrictions, removes illegal listings, and shares data with the City, including the listings' unique ID/URL, submitted registration number, unique host ID, listing information, and listing zip code.[152]

C. Los Angeles and Its Data Sharing Program for Micro-mobility Services

The most recent and ambitious example of data-reporting requisites comes from the micro-mobility industry, and was developed by the city of Los Angeles.[153] Electric scooters and both docked and dockless shared bikes are collectively called "micro-mobility services."[154] Their business model consists of distributing e-scooters and bikes across a city; potential riders use their smartphones to unlock and pay for a vehicle using a mobile app.[155] Micro-mobility services are often seen as offering a solution to address the first-mile/last-mile problem, make transport more accessible for underserved communities, and replace short car trips.[156] In the United States, more than half of the car trips annually cover less than five miles.[157] Uber and Lyft both own and heavily invested in some of the main e-scooter companies in the United States, like Lime and Motivate.[158]

Despite the potential of scooters to be integrated with transportation systems, solve last-mile problems, and replace short car trips, e-scooters also raise concerns regarding the safe use of public spaces, especially sidewalks.[159] As an article from consulting firm Deloitte put it, cities were unable to know when and how these vehicles were being deployed and used, struggling to ensure that these new mobility options served broader municipal goals.[160]

1. LADOT's MDS Standard

In this context, the City of Los Angeles Department of Transportation (LADOT) announced its Shared Mobility Device Pilot Program.[161] The program, launched in

---

[152] Mayor's Office, *Airbnb Reach Agreement to Strengthen Short-Term Rental Registry, Remove Illegal Units*, CITY OF BOSTON (Aug. 29, 2019), https://www.boston.gov/news/city-boston-airbnb-reach-agreement-strengthen-short-term-rental-registry-remove-illegal-units [https://perma.cc/52AP-UYRT].

[153] LADOT, *Dockless On-Demand Personal Mobility Conditional One-Year Permit* (Dec. 1, 2018), https://ladot.lacity.org/sites/default/files/documents/final-one-year-dockless-permit.pdf [https://perma.cc/XD4D-EDB6].

[154] POPULUS, *supra* note 39, at 4.

[155] *Id.* at 5.

[156] *Id.* at 4.

[157] *See, e.g.*, Zarif et al., *supra* note 38.

[158] Dickey, *supra* note 41.

[159] *See, e.g.*, Zarif et al., *supra* note 38.

[160] *Id.*

[161] *See generally* LADOT, *supra* note 153.

the summer of 2018, recognizes that companies operating dockless on-demand mobility products have expanded significantly, and therefore need to be regulated to ensure safety, equity, and technological efficiency.[162] As part of the program, companies operating these services are required to submit information to the City through a mobility data specification interface called MDS.[163] The City requests real-time information regarding how many vehicles are in use and where they are picked up and dropped off.[164] Information on the route taken is also sent to LADOT with a 24-hour delay.[165] The City also uses MDS to submit information to e-scooter providers regarding vehicle caps, service areas or to inform them about street closures.[166]

LADOT expects to leverage the collected information to be more effective, equitable, and sustainable in its functions.[167] According to LADOT, the program allows the city to solve a "myriad of issues" in a more cost-effective way, like ensuring companies are complying with local rules, making sure the scooters are being made available to lower-income residents,[168] and addressing complaints about scooters blocking sidewalks and operating unsafely.[169] Though MDS is currently used primarily with dockless mobility, the City says this digital infrastructure will help it engage and manage autonomous cars and drones in the future.[170]

When MDS in Los Angeles was adopted in March 2019, Uber objected and challenged it based on the privacy risks the program represents for its users.[171] Jump, one of the micro-mobility services Uber owned and operated at the time, refused to share real-time data and instead started giving LADOT data reports with a 24-hour

---

[162] *Id.* at 1 ("The City of Los Angeles ("City") has seen an explosion of new mobility products and services. Acceleration of shared mobility, artificial intelligence and machine learning, electrification and solar power, GPS and big data combined to change the mobility landscape more than in the previous 40 years. The City is taking a proactive approach to integrate these technologies into the fabric of its transportation system. . . . This allows the City the tools to make informed, data-driven decisions to ensure transportation options that are safe and deliver on the City's goal of socioeconomic and racial equity.").

[163] *Id.* at 13.

[164] *Id.*

[165] *See* Saleta 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/T834-WYX5].

[166] LADOT, TECHNOLOGY ACTION PLAN V 1.2. 15, https://ladot.io/wp-content/uploads/2019/04/LADOT-TAP_v1-2_Nov_FINAL.pdf [https://perma.cc/HFW8-5AE6].

[167] *Id.* at 9.

[168] *See* Joseph Cox, *Scooter Companies Split on Giving Real-Time Location Data to Los Angeles*, VICE (March 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/UWK2-76DB].

[169] *Id.*

[170] *See LADOT's Transportation Technology Strategy*, LADOT, https://ladot.io/ [https://perma.cc/E7DD-SPML] (last visited Apr. 26, 2022).

[171] *See* Cox, *supra* note 168.

latency.[172] The other eight companies operating scooters in the City complied with the program.[173] In October 2019, the City suspended Jump's permit.[174] Jump appealed the decision and lost.[175] Jump subsequently started sharing real-time data, in March 2020.[176]

Though individual information about users is never requested, the locational and mobility data are highly sensitive and it could be potentially reidentified if cross-matched with personal data about users.[177] LADOT's Data Protection Principles say that the Department "will mandate data sets solely to meet the specific operational and safety needs of LADOT objectives,"[178] that where possible it will "aggregate, de-identify, obfuscate, or destroy raw data where we do not need single vehicle data,"[179] and that "[l]aw enforcement and other government agencies . . . will not have access to raw trip data other than as required by law."[180] The document, however, does not seem to be binding.[181] The lawyer appointed to handle the administrative appeal found that LADOT had properly suspended Jump's permit for violating the submission rules, because Jump had applied for the permit voluntarily.[182] He also noted, however, that just as Jump had not provided evidence that the scooter data had been used to personally identify a rider, the City had not successfully explained what problems could be solved with real-time data reporting.[183]

In March 2020, Jump sued the City of Los Angeles over MDS. Jump argued that sharing such detailed information with LADOT is a violation of its Fourth Amendment Rights.[184] They argued, just like Airbnb and HomeAway had, that LADOT's

---

[172] *See* Preetika Rana & James Rundle, *Uber Sues Los Angeles Over Data-Sharing Rules*, WALL STREET JOURNAL (March 25, 2020, 12:51 AM), https://www.wsj.com/articles/uber-sues-los-angeles-over-data-sharing-rules-11585104223 [https://perma.cc/8CEM-99U6].

[173] Cox, *supra* note 168.

[174] Laura J. Nelson, *L.A. Wins Appeal in Fight with Uber Over Scooter and Bike Data*, L.A. TIMES (Feb. 11, 2020), https://www.latimes.com/california/story/2020-02-11/uber-jump-bikes-scooters-permit-ladot-data-fight-ruling [https://perma.cc/9SEB-M5LU].

[175] *Id.*

[176] Kirsten Errick, *Jump Sues Los Angeles for Requiring Real-Time Geolocation Data*, LAW STREET MEDIA (March 25, 2020), https://lawstreetmedia.com/news/tech/tech-policy/jump-sues-los-angeles-for-requiring-real-time-geolocation-data/ [https://perma.cc/FK9W-JS7U].

[177] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[178] City of Los Angeles, *LADOT Data Protection Principles* 2 (Apr. 12, 2019), https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-Protection-Principles.pdf.pdf [https://perma.cc/37G7-GY7R].

[179] *Id.*

[180] *See id.*

[181] *Id.*

[182] Petitioner's Complaint for Injunctive and Declaratory Relief at 13, JUMP v. City of Los Angeles (C.D. Cal, Mar. 24, 2020) (No. 2:20-CV-02746) [hereinafter Petitioner's Complaint for Relief].

[183] *Id.* at 12–13.

[184] *See* Zefo, *supra* note 13.

requirements operated "in practice as an administrative search," because Jump has a reasonable expectation of privacy in its business records, which includes "the data compelled pursuant to the LADOT's MDS geolocation requirements."[185] According to Jump, keeping "such confidential business information from public disclosure . . . is crucial for maintain[ing] its business success."[186] Regarding the users' expectation of privacy, they noted that "[u]sers expect their private information will be used only for limited purposes as outlined in Jump's privacy policy."[187] Second, Jump argued that MDS violates and is preempted by the California Electronic Communications Privacy Act (CalECPA), because it generally "prohibits any government entity from compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device."[188]

In May 2020, Lime, another e-scooter company in which Uber was a main investor, acquired Jump as part of the deal in a $170 million funding round let by Uber.[189] Lime withdrew the lawsuit.[190] The ACLU, however, filed a complaint on behalf of e-scooter users raising the same Fourth Amendment arguments.[191]

2. The Open Mobility Foundation and Communities Against Rider Surveillance

In the meantime, more than 50 cities in the United States and abroad (including Seattle, Providence, Austin, Louisville, Dublin, Ireland, and Bogota, Colombia) have partnered with Los Angeles to create a non-profit called the Open Mobility Foundation (OMF) in order to use the MDS standard to solicit and organize information about shared scooters.[192] The Foundation seems to be only starting, but its primary objective is the governance and development of open-source software and related APIs, not only for scooters but for other services such as online shopping and

---

[185] Petitioner's Complaint for Relief, *supra* note 182, at 114.

[186] *Id.*

[187] *Id.* at 115.

[188] *Id.* at 132; *see* CAL. PENAL CODE § 1546.1(a)(2).

[189] Andrew J. Hawkins, *Lime Squeezes $170 Million from Uber and Alphabet as Scooter-Sharing Plummets Under COVID-19*, THE 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].

[190] *See generally* Petitioner's Complaint for Relief, *supra* note 182.

[191] *See* Plaintiff's Complaint, Sánchez & Alejo v. City of Los Angeles (C.D. Cal. June 8, 2020) (No. 2:20-CV-05044).

[192] Aarian Marshall, *These Cities Will Track Scooters to Get a Handle on Regulation*, WIRED (June 25, 2019), https://www.wired.com/story/these-cities-will-track-scooters-handle-regulation/ [https://perma.cc/8G3V-5LH2]; David Zipper, *Cities Can See Where You're Taking That Scooter*, SLATE (Apr. 2, 2019), https://slate.com/business/2019/04/scooter-data-cities-mds-uber-lyft-los-angeles.html [https://perma.cc/VK4H-SKAS]. *See generally*, *Who Is Using MDS*, OPEN MOBILITY FOUND., https://www.openmobilityfoundation.org/mds-users/ [https://perma.cc/D9LH-WLKH] (last visited Apr. 26, 2022).

new vehicles that use the existing public right-of-way.[193] According to the OMF's website, the advantage of MDS is that:

> [c]ities are accountable to the public, and have an interest in making sure that their residents are being served in a way that is safe and equitable, and improves their quality of life while protecting individuals' privacy rights. With new challenges and new tools around mobility technology emerging in cities across the country, municipalities are well-positioned to collaborate and convene stakeholders in order to find technology solutions that serve the public good.[194]

The Foundation foresees creating a Privacy, Security and Transparency Committee in the near future.[195]

At the same time, various non-profits and privacy advocacy groups have joined an organization called Communities Against Rider Surveillance, which is largely backed by Uber.[196] Some left, however, when they discovered the company was involved.[197]

D. Summary of This Section

This section presented three data sharing ordinances, their overall objectives, how the data has been used, and how they have been challenged—or not—by platforms offering city services. It showed that enhanced access to data collected by these companies enhance cities' power to regulate and engage with them, which can lead to equality enhancing measures.[198] Larger platforms, on their side, seem to behave strategically when faced with these data sharing ordinances, depending on the cities' formal authority to regulate these companies.[199] In the ride hailing example in New York, platforms were still willing to render *more* data if this meant that the city would calculate the work time for drivers in a more accurate way, one which would, ultimately, allow them to pay drivers per actual time working and not per a lengthier estimated time working.[200] Similarly, Airbnb dropped its lawsuits

---

[193] *Id.*

[194] *FAQS*, OPEN MOBILITY FOUND., https://www.openmobilityfoundation.org/faq/ [https://perma.cc/S7WC-7Q2N] (last visited Apr. 26, 2022).

[195] *Id.*

[196] *About Our Coalition*, COMMUNITIES AGAINST RIDER SURVEILLANCE, https://stopridersurveillance.com/about-cars/ [https://perma.cc/U2FA-JHVX] (last visited Apr. 26, 2022).

[197] Aarian Marshall, *Uber Quietly Recruits Allies to Battle Cities Over User Data*, WIRED (July 9, 2020), https://www.wired.com/story/uber-moves-stealthily-gain-allies-fight-cities/ [https://perma.cc/93J2-MYZE].

[198] *See, e.g.*, Marineau, *supra* note 141.

[199] *See* Marshall, *supra* note 197.

[200] *See, e.g.*, N.Y.C. TAXI & LIMOUSINE COMM'N, *supra* note 51.

against data sharing ordinances when it became clear that it was nevertheless going to be regulated by local governments, and thus it made more sense to cooperate.[201] This is not to say that companies always try to mobilize the legal system against cities. Lime, for example, dropped the LADOT lawsuit when it acquired Jump, even before it had complied with the regulation and was a part of anti-regulation lobbying efforts.[202] Cooperating can be a choice for cities and companies too.

At the same time, these data sharing ordinances are situated in broader political economy contexts in which platforms work to preempt local regulation by lobbying states or challenging these ordinances using federal law, in these cases on privacy grounds.[203] The next section discusses the privacy concerns these ordinances raise from a legal and regulatory perspective.

It argues, in general, that current privacy laws frameworks offer weak protections to data collected "in public," such as on streets, online, or that which is freely rendered to service providers. Thus, cities should include privacy safeguards in their data sharing programs that mitigate these risks. It would also be ideal, however, that eventually across-the-board privacy frameworks are developed that allow cities to have access to this data while at the same time regulating and limiting some of the riskiest uses of sensitive information.

II. THE LEGAL ISSUES RAISED BY PLATFORMS AGAINST LOCAL DATA SHARING PROGRAMS

In the cases above, short-term rental platforms and micro-mobility companies argue that local governments cannot enact data sharing rules, like the ones New York, Boston, and Los Angeles have, because the bulk of data they collect from their users is part of their business records.[204] Thus, the argument goes, they have a business, ownership, and possessory interest in that information and data sharing ordinances are warrantless administrative searches, which must include an opportunity for pre-compliance review.[205] They also argue that the ordinances work against their user's privacy interests.[206] Their arguments mainly rely on the protections granted to them and their users by the Fourth Amendment and other data security

---

[201] Sylvia Shalhout, *Airbnb, New York City Settlement Over Host Data*, MASHVISOR (June 18, 2020), https://www.mashvisor.com/blog/airbnb-new-york-city-settlement/ [https://perma.cc/PX5H-EN49].

[202] *Court Dismisses Lawsuit Against Micromobility Data-Sharing*, BICYCLE RETAILER AND INDUS. NEWS (March 2, 2021), https://www.bicycleretailer.com/industry-news/2021/03/02/court-dismisses-lawsuit-against-micromobility-data-sharing#.YfBEhFjMK3I [https://perma.cc/D2FJ-G58N].

[203] *See* COMMUNITIES AGAINST RIDER SURVEILLANCE, *supra* note 196.

[204] Petitioner's Complaint for Relief, *supra* note 182, at 10.

[205] *Id.* at 15.

[206] *Id.* at 50.

and privacy laws, like the Stored Communications Act (SCA) and California's Consumer Privacy Act (CCPA).[207]

Data sharing ordinances raise privacy concerns from a user perspective when the information local governments request is mostly about them or is information that could be linked to them.[208] This is the case for mobility data, which is very sensitive because it is highly unique and can be linked back to individuals, even if no other personal information is requested.[209] Similarly, these ordinances raise privacy concerns from the platform's perspective because this data often reveal important information about their business's operation.[210]

Present privacy frameworks, however, are rather unfit to prevent some of the privacy risks of this information age. This is not a new phenomenon: privacy as a normative concept and as a body of law and legal protection is deeply intertwined with the history of technology.[211] The ubiquitous collection of information by smart city technologies and other service providers, like platforms, represents arguably another historic inflection point in privacy, just like the telegraph in the late nineteenth century, and the computer in the early 1970s.[212] Consequently, the European Union and the State of California have sought to update their privacy frameworks and introduce new information privacy norms for this new context.[213] At the same time, however, platforms and other actors are mobilizing their own resources to ensure their interests are or remain protected, as in the challenges I described in the previous section.[214]

This section shows how platforms are mobilizing Fourth Amendment doctrine to entrench property-like rights over the data they collect from users while, in the

---

[207] *California Consumer Privacy Act (CCPA)*, CAL. OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/K2MV-4EFT]; 18 U.S.C. § 2703.

[208] Thus, for example, it is unlikely that the data sharing that takes place between TLC and ride-hailing companies in New York raises Fourth Amendment concerns, at least from the user's perspective, because aggregated data is at stake.

[209] *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/CEB3-RAD4].

[210] *Id.*

[211] URS GASSER, FUTURING DIGITAL PRIVACY: REIMAGINING THE LAW/TECH-INTERPLAY 2 (Cambridge Univ. Press 2021) (ebook).

[212] *Id.* at 5.

[213] *See European Union—Data Privacy and Protection*, EUR. UNION COUNTRY COM. GUIDE, https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection#:~:text=The [https://perma.cc/UM7E-DJFX]; *The OECD Privacy Framework*, ORG. FOR ECON. COOP. & DEV. (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf; Commission Regulation 2016/679, 2016 O.J. (L 119) 1; OBAMA WHITE HOUSE, *Administration Discussion Draft: Consumer Privacy Bill of Rights Act*, OBAMA WHITE HOUSE ARCHIVES (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf; *California Consumer Privacy Act (CCPA)*, *supra* note 207.

[214] *See* Zefo, *supra* note 13.

meantime, trying to limit cities' power to access and use that data to regulate them and advance equity related goals. It first, analyzes these challenges and, second, situates them within the current political economy of rising platform power and their efforts to shape the law in their favor.

A. The Fourth Amendment Argument Raised by Platforms

The legal arguments that short-term rental platforms and micro-mobility companies are making are basically the following: first, local governments can't enact data sharing rules like the ones New York, Boston and Los Angeles have, because the bulk of data they collect from their users is part of their business records. Thus, the argument goes, they have a business, ownership, and possessory interest in that information and data sharing ordinances are warrantless administrative searches, which must include an opportunity for pre-compliance review.[215] Second, these ordinances violate their user's privacy interests. These arguments mainly rely on the protections granted to them and their users by the Fourth Amendment, and other data security and privacy laws like the Stored Communications Act (SCA) and California's Consumer Privacy Act (CCPA).[216]

In *Airbnb v. New York City* and *Airbnb v. Boston*, the courts agreed with much of the platform's Fourth Amendment arguments, though in the Boston case, the court found that the platforms had no protected privacy interest on the information that it listed online—it did not seem to worry much about the privacy interests users could have on that same information.[217] The courts found that the claims under the SCA were unlikely to succeed, mainly because platforms already require users to consent to their information being shared.[218] If confirmed, this reasoning would make it harder for local governments to issue ordinances that mandate platforms to share information with them and, as both the New York and Boston cases show, it would instead precipitate a situation where platforms and cities bargain over data with little democratic oversight.[219] The ACLU, as Jump had done before, is seeking a similar ruling that would prevent LADOT from requesting data from scooter services by local ordinance.[220]

The legal question at stake is thus the following: are the protected privacy interests of a platform that requires local permission to operate, or the interests of

---

[215] *See* Petitioner's Complaint for Relief, *supra* note 182; *supra* notes 204–06 and accompanying text.

[216] *See California Consumer Privacy Act (CCPA)*, *supra* note 207.

[217] *See* Airbnb v. City of Boston, 386 F. Supp. 3d 113, 125 (D. Mass. 2019); Airbnb v. City of New York, 373 F. Supp. 3d. 467, 467 (S.D.N.Y. 2019).

[218] *See* Airbnb v. City of Boston, 386 F. Supp. 3d at 113.

[219] *See* Airbnb v. City of New York, 373 F. Supp. 3d at 501; *see also* Airbnb v. City of Boston, 386 F. Supp. 3d at 125.

[220] *Court Dismisses Lawsuit Against Micromobility Data-Sharing*, *supra* note 202.

said platform's users, infringed by local ordinances or licensing requirements that include a duty to share information with the local government about how its users use its services?

This Article argues that these data sharing requirements do not infringe on such protected privacy interests. Current Fourth Amendment doctrine does not recognize that individuals or companies have "no reasonable expectation of privacy in public" or in information that has been willingly shared with third parties. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[221] According to a famous test articulated by Justice Harlan in *Katz v. United States* (1968), in order to succeed in Fourth Amendment challenges, plaintiffs need to prove that they have a reasonable expectation of privacy on the information sought, and that that expectation is one that is protected.[222] The third-party doctrine and the rule of "no reasonable expectation of privacy in public" can also be traced back to *Katz v. United States*.[223] In *Katz*, FBI agents had listened to and recorded a petitioner's conversation in a telephone booth without a warrant.[224] The Court famously distanced itself from the previously prevalent theory that the Fourth Amendment protected only interests tied to property, and declared that "the Fourth Amendment protects people, not places."[225] Consequently, the Court declared that the intrusion had been an unconstitutional search, because in the booth Katz had a reasonable expectation of privacy and electronic intrusions could constitute a violation of privacy.[226]

The decision might have hinted at a nuanced understanding of when a person had a reasonable expectation of privacy, but both statements are contradictory and the concept of "publicness" is indeterminate.[227] In practice, courts, including the Supreme Court, have treated freely accessible information rather binarily and considered all forms of information that is freely accessible or available in public spaces as "public."[228] In *United States v. Knotts*,[229] decided in 1983, the Court found that the warrantless use of an electronic tracking device—a beeper used to track a vehicle in traffic—did not violate the Fourth Amendment.[230] The Court reasoned that the

---

[221] U.S. CONST. amend. IV.

[222] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[223] *Id.* at 362; *see also* Lucas Issacharoff & Kyle Wirsha, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 988 (2016).

[224] *Katz*, 389 U.S. at 348.

[225] *Id.* at 351.

[226] *Id.* at 359.

[227] *Compare id.* at 351 ("[T]he Fourth Amendment protects people, not places."), *with id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

[228] Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 474 (2019).

[229] 460 U.S. 276 (1983).

[230] *Id.* at 285.

information the police obtained using the device was almost public, as they could have obtained it from simply following the subject, which would not have required a warrant.[231]

More recently, the Washington Supreme Court even held that people had no reasonable expectation of privacy in very personal information "left behind," like fingerprints:

> Police may surreptitiously follow a suspect to collect DNA, fingerprints, footprints, or other possibly incriminating evidence, without violating that suspect's privacy. No case has been cited challenging or declaring this type of police practice unreasonable or unconstitutional. People constantly leave genetic material, fingerprints, footprints, or other evidence of their identity in public places. There is no subjective expectation of privacy in discarded genetic material just as there is no subjective expectation of privacy in fingerprints or footprints left in a public place. Physical characteristics which are exposed to the public are not subject to Fourth Amendment protection.[232]

Similarly, the third-party doctrine stems from cases that came in the years that followed *Katz*.[233] Some scholars have noted that the Court tried to reconcile an individual's reasonable expectation of privacy with cases in which undercover agents or informants gathered private information through different means, which led to the development of the third-party doctrine.[234] Regarding what a reasonable expectation of privacy is, in *Couch v. United States*[235] and *United States v. Miller*,[236] the Court found that the defendants did not have a reasonable expectation of privacy in records they had given to an accountant and a bank, respectively.[237] In 1979, in *Smith v. Maryland*, the Court expanded this doctrine, moving beyond business records and admitting into trial data from a pen register (a device that keeps track of dialed numbers) obtained without a warrant.[238] It held that because the defendant had voluntarily conveyed the numbers to the telephone company, he could claim no legitimate expectation of privacy.[239] These are all cases in which customers of companies, like

---

[231] *Id.*

[232] State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

[233] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (holding that warrants are needed for gathering information from wireless carriers that comes from personal cell phones because a cell phone is "a feature of human autonomy.").

[234] *See* Issacharoff & Wirsha, *supra* note 223, at 988.

[235] 409 U.S. 322, 335–36 (1973).

[236] 425 U.S. 435, 442 (1976).

[237] *See Couch*, 409 U.S. at 335–36; *Miller*, 425 U.S. at 442.

[238] *See* Smith v. Maryland, 442 U.S. 735, 735–36 (1979).

[239] *See id.* at 743.

platform users, were denied privacy protections after having surrendered information that was necessary for the provision of the service at hand.[240]

The Court had largely and consistently affirmed these doctrines until *Carpenter v. United States* in 2018.[241] In *Carpenter*, the FBI had obtained the defendant's cell phone records from a telecom company based on a court order under the Stored Communications Act (SCA).[242] Carpenter was charged based on the records requested and, prior to trial, he argued that the government's seizure of the records "violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause," a higher threshold.[243] The government argued that Carpenter lacked a reasonable expectation of privacy because he had shared that information with the wireless carriers; however, the Supreme Court disagreed and did not extend the third-party doctrine "to cover [these] novel circumstances."[244] In the majority opinion, Justice Roberts stated that the premise underlying the third-party doctrine—knowingly and voluntarily sharing information[245]—didn't hold up when it came to cell-site location information:

> After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements . . . [c]ell phone location information is not truly "shared" as one normally understands the term. . . . [C]arrying one is indispensable to participation in modern society.[246]

---

[240] *See, e.g.*, *id.* at 743, 745–46.

[241] *See Carpenter*, 138 S. Ct. 2206, 2220, 2223 (2018). *Jones v. United States* in 2012 was another related decision in which the mobility information of someone was also at stake: police officers attached a Global Positioning System (GPS) device to a vehicle and used it to monitor an individual's movements without a valid warrant. The Court didn't address the relevance of the third-party doctrine or whether the information at stake had been "public"—as in *Knotts*—because the majority found that this was a search or seizure within the meaning of the Fourth Amendment because the government had physically occupied private property. Justice Sotomayor, however, signaled in her concurrent opinion a bit of a movement towards a more nuanced understanding of privacy in public: the Fourth Amendment was not concerned only with trespassory intrusions of property. Given the unique attributes of GPS technology, it could be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties or members of the public. *See* 565 U.S. at 402, 417–18 (Sotomayor, J., concurring).

[242] *Carpenter*, 138 S. Ct. at 2221.

[243] *Id.* at 2212.

[244] *Id.* at 2217.

[245] *Id.* at 2222.

[246] *Id.* at 2217, 2220.

The decision was considered a landmark.[247] Many scholars agree that in the digital information economy, consent-based privacy protections do not reflect the reality of how we interact with data-enabled services.[248] Nevertheless, the ruling was narrow: it explicitly did not "call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information."[249] The third-party doctrine and the lack of expectation of privacy in public remains, thus, the general rule.[250]

Consequently, the standard in *Carpenter* does not seem to apply to the data collected by the platforms at issue here.[251] Services like e-scooters or short-term rentals are not as essential as using a cellphone, and the Court almost explicitly excluded business records that revealed incidental location information.[252] The standard in *Carpenter* seems higher, and the underlying assumption of the third-party doctrine, that individuals willingly and voluntarily share their information, is likely to hold.[253] If users do not have protected privacy interests under the Fourth Amendment, the arguments brought by platforms will not protect them; platforms will still be able to share or sell their data downstream.[254]

---

[247] *See* Adam Liptak, *In Ruling On Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, N.Y. TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html [https://perma.cc/L9PT-8WTS].

[248] *See* Issacharoff & Wirsha, *supra* note 223, at 987, 999–1008.

[249] *Carpenter*, 138 S. Ct. at 2220; making a similar point, see Ira S. Rubinstein, *Privacy Localism*, 94 WASH. L. REV. 1963 at 1979. In their dissents, however, Justices Thomas, Alito and Kennedy reasserted the property-based concepts that "have long grounded the analytic framework" that pertains to the Fourth Amendment protections, and argued that customers do not own, possess, control or use the business records from businesses they contract services from. Consequently, the relevant question necessary to decide was whether the Government searched anything of Carpenter's, and the answer was no. *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J. dissenting).

[250] *See, e.g.*, Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

[251] *See Carpenter*, 138 S. Ct. at 2220.

[252] *See also id.*

[253] *Cf.* 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/3MAE-99LM].

[254] Other reasons why data sharing ordinances are not like *Carpenter* include the following: first, the information at stake is not sufficiently pervasive about an individuals' life to be as telling as the cell-site location the Court considered in *Carpenter*. It would be rare that an individual uses e-only scooters or only ride-sharing services to move around. The mobility data of scooters and even ride-sharing companies seems to be more similar to the information at stake in *Knotts* than in *Carpenter*, and the Court explicitly did not overrule *Knotts.* The same is true about information about one's home. In this latter case, additionally, the platforms often share information about the host's home online and the Fourth Amendment does not protect information that is in plain sight. Similarly, if as in Boston and New York City hosts are only allowed to offer their properties for short-term rentals a few months or weeks a year, the

Therefore, the next question is whether the platform's privacy interests are protected. This Article argues in the negative, that platform's interests are unprotected. Platforms claim they have a protected privacy interest on the data they collect from their users because it is sensitive user information and because that information is part of their business records. According to the test from *Katz*, they should be able to show, first, that they have exhibited a subjective expectation of privacy on the information sought and, second, that the expectation is one that society is prepared to recognize as "reasonable."[255]

Platforms argue that they have a reasonable privacy expectation for the data being requested in data sharing ordinances because it is part of their business records, and consists of sensitive information relating to their users as well as confidential commercially sensitive information about their businesses, which is important to keep from competitors.[256]

The Fourth Amendment protections on business records are, however, not absolute. They have not been defined in the abstract by the Court and vary greatly on a case-by-case basis.[257] "Business records" is, indeed, a broad term that encompasses all sorts of files and physical papers: contracts, correspondence, registries, licenses, etc.[258] In the previous subsection, we saw that the Fourth Amendment does not protect information that is publicly available, even if it is part of what a platform could consider its business records.[259] Accordingly, in *Airbnb v. Boston,* the Court did not find that Airbnb and HomeAway could assert that they had a privacy interest on the information that they make publicly available on their website.[260]

How to determine what the protected interests on a company's business records are also complicated. Throughout history, the Court has found that a company's privacy interests in its business records are not determined by other rights; a company's Fourth Amendment protections are not determined by the Fifth Amendment right to not self-incriminate, and they must comply with regulations and reporting obligations under the law.[261] Thus, in *Hale v. Henkel*,[262] a 1906 case, the Court found

---

information shared would partially only reflect those few transactions. Other information—address, zip code, name, and so on—remains the same, but it is also information regarding the owner of a property the city already has. Second, users willingly and voluntarily decide to use these services and participate in the kind of platform examined here. We even sign terms of services and privacy policies in which they agree to our data being shared with public entities. *See supra* Part I.

[255] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[256] *See* Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 486–87, 499 (S.D.N.Y. 2019).

[257] *See* Morton Salt v. United States, 338 U.S. 632, 654 (1950).

[258] *See Hearsay—The Business Records Exception to the Hearsay Rule*, MARTINDALE, https://www.martindale.com/legal-news/article_the-clinton-law-firm_1258444.htm.

[259] *See* discussion *supra* Part II.

[260] Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 125 (D. Mass. 2019).

[261] Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 196 (1946).

[262] 201 U.S. 43 (1906).

that Hale could not assert his privilege against self-incrimination on behalf of his employer to refuse an order to produce some documents for a Court.[263] Similarly, in *Oklahoma Press Publishing Co. v. Walling*,[264] decided in 1946, the Court found that the rights guaranteed by the First Amendment to newspapers do not create an exception for newspapers and publishing companies regarding the application of rules that allow regulators to issue subpoenas requesting documents to ensure that these companies are complying with their obligations.[265] In that case, which concerned the enforcement of a provision of the Fair Labor Standards Act, the Court noted that "[w]hat petitioners seek is not to prevent an unlawful search and seizure. It is, rather, a total immunity to the Act's provisions"[266] that the requirement of reasonableness of the Fourth Amendment "comes down to specifications of the documents to be produced adequate, but not excessive for the purpose of the relevant inquiry."[267] In another decision in 1950, the Court even considered that the collective impact corporations have on society and their privilege of acting as artificial entities carried with them an enhanced measure of regulation.[268] The Court said that "law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest."[269]

Another illustrative decision is *Dow Chemical Co. v. United States*, decided in 1986.[270] In *Dow Chemical*, the Court stressed that a company's interest in not disclosing information to competitors did not define the limits of its Fourth Amendment rights, as government actors requested information to regulate them and not to compete with them.[271] In the case, Dow had denied a request by the Environmental Protection Agency (EPA) for an on-site inspection and the government decided instead to employ a commercial aerial photographer to take photographs of the facility.[272] Dow argued that trade secret laws protected it from aerial photography.[273] The Court disagreed and held that the fact that such photography might be barred by state law with regard to competitors, was irrelevant to the questions presented in the case: "[s]tate tort law governing unfair competition does not define the limits of the Fourth Amendment . . . [.] The Government is seeking these photographs in order to regulate, not to compete with, Dow."[274]

As in *Dow Chemical*, in the data sharing cases reviewed above, platforms argue that they have a protected interest in the data requested because the information is

---

[263] *Id.* at 58, 77.
[264] *Okla. Press Publ'g*, 327 U.S. 186.
[265] *Id.* at 193–94.
[266] *Id.* at 196.
[267] *Id.* at 209.
[268] Morton Salt v. United States, 338 U.S. 632, 652 (1950).
[269] *Id.*
[270] 476 U.S. 227 (1986).
[271] *Id.* at 238.
[272] *Id.* at 242.
[273] *Id.* at 230.
[274] *Id.* at 232.

crucial for their business models.[275] Consequently, if the law governing unfair competition does not define the limits of the Fourth Amendment, this argument should also not lead to preempt local governments from asking platforms for user data or data regarding their operations. If a particular data sharing ordinance does pose a protected competitive threat to a platform—for example, because a competitor could access information that is protection under trade secrecy via freedom of information requests—what local governments should do, and courts should demand, is that the data are labeled as confidential, so that they will not be shared under FOIA requests. Indeed, local governments are requesting that information to regulate platforms not compete with them, so that they may enforce local laws that are not related to criminal law in order to bring about better public policy implications.[276] Additionally, quite often, some of that information is available online, as the court in *Airbnb v. City of Boston* noted, could be considered, as in *Knotts*, public, because city officials could obtain it by monitoring city streets more thoroughly.[277] Since platforms cannot assert their privilege against self-incrimination to oppose inspections and data sharing requests, it would be unreasonable to recognize that platforms can assert the Fourth Amendment to seek immunity from local regulation or keep verifiable information from city officials or local authorities regarding how they are abiding to local laws.

According to the *Katz* test, the next step is to examine whether the data requests are reasonable.[278] In *Airbnb v. City of New York*, the court granted the preliminary injunction to Airbnb because, according to it, platforms have a reasonable expectation over their business records and the data requested is part of their business records.[279] The ordinance on its face lacked a mechanism for pre-compliance review.[280] In its decision, the New York court relied on *City of Los Angeles v. Patel*, a case Uber cites to as well in its lawsuit against LA.[281] In what follows, the Article briefly presents *City of Los Angeles v. Patel*, and the Court's jurisprudence on the constitutionality of warrantless searches.

City of Los Angeles v. Patel, however, does not deal with information requests that are not intended to facilitate criminal law investigations.[282] In *Patel*, motel owners challenged a provision that both required them to keep records with specific personal information about their guests, and authorized warrantless on-site inspections of those records upon the demand of the Los Angeles Police Department.[283]

---

[275] *See id.* at 250; Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 486–87, 499 (S.D.N.Y. 2019).

[276] *Id.* at 232.

[277] *See* Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 124 (D. Mass. 2019).

[278] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[279] *See* Airbnb Inc. v. City of New York, 373 F. Supp. 3d. 467, 501 (S.D.N.Y. 2019).

[280] *Id.* at 496.

[281] City of Los Angeles v. Patel, 576 U.S. 409, 428 (2015).

[282] *Id.* at 420.

[283] *Id.* at 413.

Writing for the Court, Justice Sotomayor held that such a requirement was unconstitutional *because* the alleged government interest at stake—to facilitate criminal investigation and ensure compliance with the record-keeping requirement—did not meet the strict requirements for allowed warrantless searches.[284] 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.[285]

Historically, however, the Court has carved out a variety of exceptions where the primary purpose of the search is distinguishable from crime control.[286] Warrantless searches known as "administrative searches" are, as a matter of black letter law, an exception, but are actually very common.[287] Sobriety checkpoints, drug tests and business searches are all administrative searches.[288] Typically, subjects of administrative searches must be afforded an opportunity to obtain pre-compliance review before a neutral decision maker.[289] Yet, an exception to the warrant requirement also exists for closely regulated businesses, like the liquor store industry, pawnshops, junkyards, and the mining industry.[290] These warrantless searches are permissible where "regulatory inspections further urgent federal interest, and the possibilities of abuse and the threat to privacy are not of impressive dimensions, the inspections may proceed without a warrant where specifically authorized by statute."[291] State

---

[284] *Id.* at 421, 427–28.

[285] *See* Katz v. United States, 389 U.S. 347, 347, 351 (1967).

[286] *Patel*, 576 U.S. at 421.

[287] *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255 (2011).

[288] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000); *see also* G. S. Hans, *Curing Administrative Search Decay*, 24 B.U. J. SCI. & TECH. L. 1 (2018); Hofmann, *supra* note 9, at 2601.

[289] These exceptions date back to the late 1960s and early 1970s. In two decisions decided on the same day, *Camara v. Municipal Court* and *See v. City of Seattle*, the Court created the administrative search exception. *Camara* involved a local ordinance that allowed inspections on buildings to determine compliance with the city's Housing Code. Camara argued that those were warrantless inspections that violated his Fourth Amendment rights. The Court found that administrative inspection programs were intrusions upon the interests protected by the Fourth Amendment, and that city officials required a warrant if the homeowner didn't consent to the inspection. In doing so, it explicitly distanced itself from previous doctrine in which it had allowed warrantless inspections for administrative purposes However, given that the inspections were "neither personal in nature nor aimed at the discovery of evidence of crime" the reasonableness standards for obtaining such a warrant was lower, and where considerations of health and safety were involved, the test of "probable cause" could take into account the nature of the search that was being sought. Similarly, in *See*, the plaintiff had been convicted for refusing to allow a city official to enter his commercial warehouse without a warrant. The Court extended its reasoning in *Camara* to commercial premises. *See* Camara v. Mun. Ct., 387 U.S. 523, 537 (1967); See v. City of Seattle, 387 U.S. 541, 541; *Patel*, 576 U.S. at 10.

[290] *See* Colonnade Catering Corp. v. United States, 397 U.S. 72, 72 (1970); United States v. Biswell, 406 U.S. 311, 311 (1972); New York v. Burger, 482 U.S. 691 (1987); Donovan v. Dewey, 452 U.S. 594 (1981).

[291] *Biswell*, 406 U.S. at 317.

and lower federal courts have found many other industries to be "pervasively regulated"; these include the medical profession, the food industry, daycares, as well as nursing homes, banking, and commercial trucking, among many others.[292]

Consequently, it does not appear that courts need to decide that all data sharing ordinances are unconstitutional. Fourth Amendment scholars tend to agree that the doctrine regarding administrative searches is a little messy, and some have pointed out that what is important is whether the information requests are reasonable.[293] This is an ambiguous standard, but in *Patel* the Court found that the ordinance was unreasonable because of its goal and the risks it posed; the purpose of the search was not distinguishable from criminal control,[294] and "[a] hotel owner who refuses to give an officer access to his or her registry can be arrested on the spot . . . . [T]he ordinance creates an intolerable risk that searches authorized by it will exceed statutory limits, or be used as a pretext to harass hotel operators and their guests."[295] Consequently, even after *Patel* and in light of Fourth Amendment doctrine on administrative searches and the closely regulated industry exception, what is crucial is not that local governments should not have access platforms "records" without an opportunity for pre-compliance review. Rather, it is that the particular kind of records requested are necessary to meet a particularly important governmental interest that is not related to crime control and that the data sharing ordinance or program is so tailored that it does not create intolerable risks of abuse or harassment for either the platforms or their users.[296] Local governments can achieve this by explicitly including binding rules in their data sharing programs regarding how the information can be used and by whom, for how long it will be kept, and by explicitly excluding criminal-control-related uses. The last section of this Article will further discuss these kinds of measures.

---

[292] *See* Desilva v. State Med. Bd., No. 1:09cv683, 2010 U.S. Dist. LEXIS 40059, at *26 (S.D. Ohio 2010); United States v. Montrom, 345 F. Supp. 1337, 1340 (E.D. Pa. 1972), *aff'd without opinion*, 480 F.2d 919 (3d Cir. 1973); Med. Soc'y of N.J. v. Robins, 729 A.2d 1056, 1059 (N.J. Super. Ct. App. Div. 1999); United States v. Bus. Builders, Inc., 354 F. Supp. 141, 143 (N.D. Okla. 1973) ("It would be an affront to common sense to say that the public interest is not as deeply involved in the regulation of the food industry as it is in the liquor and firearms industries."); Rush v. Obledo, 756 F.2d 713, 720 (9th Cir. 1985); People v. Firstenberg, 155 Cal. Rptr. 80, 84–86 (Cal. Ct. App. 1979); United States v. Chuang, 897 F.2d 646, 651 (2d Cir. 1990); United States v. Delgado, 545 F.3d 1195, 1201–02 (9th Cir. 2008) (finding commercial trucking to be pervasively regulated and citing similar holdings from the First, Fifth, Sixth, Eighth, and Tenth Circuits); *see generally Patel*, 576 U.S. at 435 (Scalia, J., dissenting).

[293] *See, e.g.*, Primus, *supra* note 287; Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757–58 (1994).

[294] *Patel*, 576 U.S. at 420.

[295] *Id.* at 421.

[296] *See* Beatriz Botero Arcila, *Jump v. Los Angeles: Removing Platforms Further from Democratic Control?*, 68 UCLA L. REV. DISC. 160, 163–64 (2020) (arguing that a ruling in favor of Jump would have seemed to recognize property rights ruling over the data requested, creating additional hurdles to regulate platform power).

B. The Privacy Law Argument Raised by Platforms

Lastly, platforms also argue that laws governing electronic communications, like the Stored Communications Act (SCA) and the California Electronic Communications Privacy Act (CalECPA), preempt data sharing ordinances.[297] These claims did not succeed in the cases regarding short-term rentals and are not likely to succeed in the case regarding micro-mobility data because these acts condition the legality of data sharing on user consent, and as shown above, users typically agree to privacy policies that warn that their data might be shared with governmental agencies.[298]

The SCA and CalECPA are information security laws that rely on personal authorizations to authorize the collection and disclosure of personal information.[299] In *Airbnb v. New York* and *Airbnb v. Boston*, HomeAway and Airbnb raised this argument regarding the SCA.[300] The SCA is part of the Electronic Communications Privacy Act and governs the disclosure of communications and records by providers of digital technology services.[301] It states that a provider may not disclose "a record or other information pertaining to a subscriber or customer of such service . . . to any governmental entity."[302] However, Section 2702 of the SCA also provides that providers can disclose information to the government "with the lawful consent of the customer or subscriber"[303] and allows governmental entities to mandate disclosure of information if, among other processes, the governmental entity has the consent of the subscriber or customer to such disclosure.[304] In *Airbnb v. New York*, the court did not find that claim was likely to prevail because platforms "*already* condition use of their services on hosts accepting privacy policies that, among other things, notify hosts that the information they provide may be disclosed to governmental authorities."[305]

In its lawsuit against Los Angeles, Uber argues that LADOT's program is preempted by CalECPA because the statute generally prohibits any government entity from "compel[ling] the production of or access to electronic device information from any person or entity other than the authorized possessor of the device."[306] Like the SCA, however, the statute also provides that the government may compel

---

[297] *See* Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 477 (S.D.N.Y. 2019).

[298] *See Uber Privacy Notice*, UBER (Dec. 22, 2021), https://www.uber.com/legal/en/document/?name=privacy-notice&country=united-states&lang=en [https://perma.cc/BZW8-73F7].

[299] *See* Airbnb v. City of New York, 47 F. Supp. 3d at 495–96 (describing the Stored Communications Act); Cal. Penal Code § 1546.1 (2021) (which incorporates CalECPA).

[300] *See* Airbnb v. City of New York, 373 F. Supp. 3d at 496; Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 118 (D. Mass. 2019).

[301] *See* Airbnb v. New York, 373 F. Supp. 3d at 495.

[302] *See* 18 U.S.C. § 2702(a)(3).

[303] *Id.* § 2702(a), (c)(2).

[304] *Id.* § 2703(c)(1)(C).

[305] Airbnb v. City of New York, 373 F. Supp. 3d at 496–97.

[306] *See* Botero Arcila, *supra* note 296, at 46; CAL. PENAL CODE § 1546.1(a)(2).

production of or access to data in specific circumstances, including consent of the device's "authorized possessor."[307]

It is very unlikely these claims will succeed.[308] Users willingly and voluntarily decide to use these services and participate in the kind of platform examined here.[309] They even sign terms of services and privacy policies, in which they agree to terms such as the following:

> When you use [platform name], you trust us with your personal data. . . . [platform name] may share users' personal data if we believe it's required by applicable law, regulation, operating license or agreement, *legal process or governmental request*, or where the disclosure is otherwise appropriate due to safety or similar concerns. This includes sharing personal data with law enforcement officials, public health officials, other government authorities, airports (if required by the airport authorities as a condition of operating on airport property).[310]

Many scholars agree that in the digital information economy, consent-based privacy protections do not reflect the reality of how consumers interact with data-enabled services.[311] Others have pushed against the binary distinction between public and private, because it is rather blurry and indeterminate, and utilized for a variety of purposes, including facilitating various forms of surveillance.[312] Modern digital surveillance has as a central feature not only data gathering, but identifying individuals, correlating their information and profiles with other larger datasets, and deciding, based on those correlations, what services individuals are offered, how trustworthy they are, what opportunities they have access to, and so on.[313] Technology firms, such as Google and Facebook, and data-brokers that buy and sell data use this information to target advertising, search results, construct risk management tools, and authenticate individuals to access a variety of services.[314] Government agencies also benefit, as they can access this information in the same private markets that private companies do, even if they don't have the basis for obtaining a warrant.[315]

---

[307] CAL. PENAL CODE § 1546.1(b)(3), (c)(4).

[308] Airbnb v. City of New York, 373 F. Supp. 3d at 496–97.

[309] *Id.*

[310] *See Uber Privacy Notice*, *supra* note 298.

[311] *See* Richards & Hartzog, *supra* note 250, at 1463.

[312] *See* Hartzog, *supra* note 228, at 459, 471; *see also* Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1916.

[313] Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privac250.html.

[314] *Id.*

[315] *See, e.g.*, Cohen, *supra* note 312, at 1916.

Much of this market is enabled by protections that consider that individuals have few rights over the data about them once the information is given away or made publicly available.[316] Consent-based regulations, however, remain the general rule.[317]

C. The Political Economy Context of the Platforms' Challenges

It is important to note that arguments are not raised in an institutional vacuum. The digital information economy is characterized by stark inequality, especially in the United States.[318] It is also characterized by the power of platforms over workers, users, and markets, while at the same time, platforms remain relatively isolated from democratic control, especially local control.[319] Additionally, the current rules and structure of the digital economy favor almost monopolistic power over the market, and data and network economies that allow rather few players to dominate vast industries, and many of the platforms challenging these ordinances are dominant actors in the industries in which they operate.[320] Enhanced access to data by other actors can be a way to curb some of their power because much of their dominance is enabled in large part by the vast troves of data that they collect about their users and the services they provide, and their ability to almost exclusively control that information.[321] Control over data allows those who have it to train better algorithms and gain a competitive advantage, but also tailor and influence transactions with little oversight, in ways that can also result in racial or socioeconomic discrimination, price discrimination, manipulative marketing, and regulatory evasion.[322]

The present form of the digital information economy and city-powerlessness is neither necessary nor natural; it is shaped by the market, norms, ideology, and institutions, of which, crucially law is one.[323] Recall that thirty-seven states preempted

---

[316] *See* Hartzog, *supra* note 228, at 459, 464.

[317] *See* Section II.A. It could be different in cases in which some platforms provide the main source of income for some workers, for example, or other more comprehensive platforms, but that is not examined here.

[318] *See* Yochai Benkler, *Power and Productivity: Institutions, Ideology, and Technology in Political Economy*, *in* A POLITICAL ECONOMY OF JUSTICE 27, 28 (Danielle Allen et al. eds., Univ. of Chi. Press 2022).

[319] *See id.*; Britton-Purdy et al., *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784, 1830 (2020); Cohen, *supra* note 312, at 1913–14. *See also* ZUBOFF, *supra* note 6, at 8; Amy Kapczynski, *The Law of Information Capitalism*, 129 YALE L.J. 1460, 1462, 1514–15 (2020).

[320] *See* Kapczynski, *supra* note 319, at 1467, 1489.

[321] *See id.* at 1472, 1489.

[322] Lina Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 981 (2019) ("Dominant digital platforms passively capture highly precise and nuanced data on their business customers, information that they can exploit when competing against those same customers."); *see also* Cohen, *supra* note 312, at 1916, 1930; Kapczynski, *supra* note 319, at 1478–79.

[323] *See* GERALD FRUG, CITY MAKING: BUILDING COMMUNITIES WITHOUT BUILDING WALLS 5, 24(1998).

local regulation of ride-sharing companies,[324] and how short-term rental platforms tried to label themselves as websites to avoid local regulation.[325] At the same time, contract law, privacy law and trade-secret law, assisted by technical means, have aided in de facto commoditizing data and structuring who has control over data.[326] Through notice and consent privacy agreements, platforms obtain from individuals the right to manufacture, use, and share or sell the data about them at will or require that data be kept secret or not shared.[327] Scholars like Julie Cohen and Amy Kapczynski have shown that technology companies have actually mobilized several bodies of law to protect their ownership and possessory interests over information; these interests are reason enough to characterize trade secrets and data as forms of property.[328] They have done so to seek protection from "takings" and from government disclosures;[329] in *Ruckelshaus v. Monsanto Co.*,[330] the Supreme Court held that trade secrets constituted property that could be protected by the Takings Clause and that could be required if there was interference with "investment-backed expectations."[331] Lower courts have read the decision broadly. For example, in *Philip Morris v. Reilly*, the First Circuit struck down a Massachusetts law that required disclosure of all cigarette ingredients to state regulators, who were then empowered, if they found that public health could benefit, to make them public.[332] As Kapczynski points out in the wake of these decisions:

> [C]ompanies have begun to argue that a wide range of laws that seek to disclose corporate information would violate takings law. . . . Companies like Google, Facebook, and Palantir will surely argue that their data, algorithms, and processing techniques used by companies qualify as trade secrets, meaning that any attempt to render them public, or to give access to competitors, will likely face a constitutional challenge.[333]

"On this theory," she emphasizes, "trade-secrets law stands as a profound impediment to democracy."[334]

---

[324] *See* Schragger, *supra* note 11, at 1172; *Cities, the Sharing Economy, and What's Next*, NAT'L LEAGUE CITIES: CTR. FOR CITY SOLS. & APPLIED RSCH. (Jan. 30, 2022), https://www.nlc.org/resource/cities-the-sharing-economy-and-whats-next/ [https://perma.cc/KG4Z-D4BD].

[325] *See* Edelman & Stemler, *supra* note 4, at 148, 161–62, 194–95.

[326] Kapczynski, *supra* note 319, at 1502.

[327] *Id.* at 1502.

[328] *Id.* at 1509.

[329] *Id.*

[330] 467 U.S. 986, 1003 (1984).

[331] *Id.* at 1005.

[332] 312 F.3d 24, 28–29 (1st Cir. 2002).

[333] Kapczynski, *supra* note 319, at 1510.

[334] *Id.* at 1509.

If the companies succeed, the same could hold true about the Fourth Amendment. Thus, besides the fact that the law is unclear and courts do not need to decide in favor of platforms, the policy argument is that the platforms' legal arguments should not succeed, because granting them absolute protection over the data they co-produce with individuals in city spaces would, as said, significantly impede the efforts of cities to use this same data to improve their policymaking in ways that can be equality enhancing.[335] Their efforts to advance this outcome should also be received with skepticism if one of the reasons why platforms were raising these issues is to avoid regulation or to protect business models that are grounded in noncompliance with applicable laws.[336] Accepting the companies' view could also backfire: it would still not solve the many ways in which user data can be abused both by platforms and governmental actors, mainly because platforms remain free to share and sell user data.[337]

D. Partial Conclusion to This Section: Individuals' Privacy Interests and the Limits of Consent

The main goal of this section was to present the formal legal regime governing data sharing ordinances from a privacy law and Fourth Amendment perspective, given that this is how platforms are challenging and framing these ordinances.[338] It showed, first, that platforms' users are relatively unprotected by existing Fourth Amendment doctrine and privacy laws. Under Fourth Amendment doctrine, once individuals surrender their personal information to another party, they lose almost all their protected privacy interests in it.[339] Similarly, even progressive privacy laws—like CalECPA—give people a bundle of rights to notice, access, and consent regarding the collection, use, sharing and disclosure of personal data, and seem to presume that users will be able to weigh the costs and benefits of their decisions regarding their data and decide accordingly.[340] The Supreme Court has started to recognize that the ubiquity of the digital information economy may make it impossible for individuals to opt out of data management practices that can result in harmful practices.[341] Using Airbnb or e-scooters seems far from the necessity standard devised by the Court in *Carpenter*.[342] Thus, individuals are still left unprotected in

---

[335] *See* Edelman & Stemler, *supra* note 4, at 157, 169, 170–72.
[336] *See id.* at 159.
[337] *See* Carpenter v. United States, 138 S. Ct. 2206, 2212, 2225 (2018).
[338] *See id.* at 2214–16, 2221, 2223.
[339] *See id.* at 2208–10.
[340] *See id.* at 2208, 2216, 2259, 2263; CAL. PENAL CODE § 1546.1 (2021) (incorporating CalECPA).
[341] *See Carpenter*, 138 S. Ct., at 2220.
[342] *See id.* at 2208, 2216–17.

many circumstances where they engage in voluntary transactions with platforms as mere consumers or service providers.[343]

Second, and most importantly, this section argued that companies' protected interests over the information they collect and produce, which may be considered part of their business records, are not absolute.[344] These interests have been, and can be, constrained by other interests of the general public, such as when regulation of these companies is necessary, or particularly important, non-crime control governmental interests are at stake.[345] This is not to say that platforms should have no protected privacy interests over all the data they collect. My objective is, rather, to show that how these limits are set is a policy question that needs to be seen as such, and to highlight the political and distributional implications of the exact opposite statement—that they should have a protected privacy interest over all the data they collect.

Given the political economy of the present digital information economy, challenges against local data sharing platforms can be framed as part of a larger effort to give corporate actors vast rights to exclude access to the data they produce from users, and, in doing so, protect their power and shield them from democratic control.[346] As technology companies accrue vast power to influence our societies and markets, it should be a central substantive interest of governments to supervise and regulate platforms and, consequently, to request from them that they share with local governments the information that is necessary to regulate them.[347] The following section thus proposes a framework for planning and assessing data sharing programs and, more broadly, city-data governance strategies.

III. A FRAMEWORK FOR ASSESSING AND DESIGNING DATA SHARING PROGRAMS

Central to the discussion of data sharing ordinances should be the broader question of data democracy and questions about the kind of powers local governments should have to govern technology companies that operate within their jurisdiction. It is important, however, to discuss too how local power should be limited, especially when data that can be traced back to individuals is at stake.

---

[343] Relatively recent scholarship has also pointed out that individual consent is particularly unusual in various cases because information is embedded in society and is usually collective in its nature. Thus, for example, while consenting to give one's own personal information it is almost impossible not to give away someone else's information—for example a sibling's genetic information. *See* Carisa Véliz, *Privacy Is a Collective Concern*, NEW STATESMAN (Oct. 22, 2019), https://www.newstatesman.com/science-tech/privacy/2019/10/privacy-collective-concern [https://perma.cc/MSD6-BF8V].

[344] *See id.*; Airbnb, Inc. v. City of New York, 373 F. Supp. 3d. 467, 493–94 (S.D.N.Y. 2019); Airbnb, Inc. v. City of Boston, 386 F. Supp. 3d 113, 124–25 (D. Mass. 2019).

[345] *See* Véliz, *supra* note 343.

[346] *See* Botero Arcila, *supra* note 296, at 163, 169–70.

[347] *See id.* at 163, 175.

The presentation of Fourth Amendment doctrine and the claims under privacy law in Part II provide some preliminary answers: the Fourth Amendment ultimately protects legal subjects from unreasonable government intrusions.[348] What "an unreasonable government intrusion" is, is largely indeterminate and courts have interpreted it differently throughout history, influenced by the ideas at the time about the importance of curbing both state coercion power and private power, though it has been, perhaps until some of the examples raised here, typically deferential to state power.[349] Nevertheless, current Fourth Amendment doctrine does seem to offer key guidelines regarding what unreasonable privacy risks are: mainly that data sharing requests must be limited,[350] they must be reasonable to meet a government interest,[351] and "the possibilities of abuse and the threat to privacy are not of impressive dimensions."[352] Privacy laws, on the other hand, generally seek to protect individuals from unjustified harms that can result from certain uses or revelations from information that can be connected to them, which in turn can hamper trust in institutions, self-determination, and other rights, like due process.[353]

A. What Courts Should Do

Given the nature and urgency of checking the kind of surveillance and algorithmic power that is enabled by exclusionary entitlements over data in the digital information economy, this Article suggests that courts should be skeptical of cases in which platforms raise user-privacy arguments to avoid regulatory oversight. Rather, courts should consider seriously the argument made by a variety of scholars and policymakers that platforms increasingly exercise vast surveillance and algorithmic power in our societies—at the market and individual level—that they increasingly provide key services that are at the backbone of our digital age, and that they do so largely unsupervised.[354] Thus, it is only reasonable that such platforms be closely supervised and perhaps regulated. Courts should therefore be prepared to uphold data sharing ordinances and programs when they are tailored and limited, and do not pose a threat to user privacy of impressive dimensions. The analysis in Part II offers a roadmap of what that could mean; however, most courts could apply the following kind of guidelines.

1. What Should User's Protected Privacy Interests Be?

Regarding a user's legitimate privacy interests, as the Supreme Court explained in *Carpenter*, the Fourth Amendment seeks, at its core, "to secure the privacies of

---

348 *See supra* Part II.
349 *Id.*
350 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).
351 *See, e.g.*, Illinois v. Lidster, 540 U.S. 419, 424–25 (2004).
352 *See* United States v. Biswell, 406 U.S. 311, 314 (1972).
353 *See* Richards & Hartzog, *supra* note 250, at 1469–72.
354 Kapczynski, *supra* note 319, at 1472, 1501–03.

life against arbitrary power," and to place an obstacle to permeating police surveillance.[355] Though ride-hailing, home-sharing, and similar platforms are not essential services of modern life, they are increasingly common and part of city life.[356] Courts could thus recognize that users have heightened protected interest in information they share with platforms freely when two requirements are jointly met: first, when these platforms provide a somewhat "infrastructural" service as part of contemporary city life,[357] and, second, when the information is sought for criminal law purposes pertaining to individuals.[358]

This heightened interest should not, however, translate into an overall ban on sharing or collecting that information. Rather, to protect individuals from arbitrary government power while still permitting more democratic uses of platform-collected data, courts should not tolerate warrantless data sharing ordinances or programs that are meant for criminal enforcement or investigation purposes.[359] Courts should also extend such protections to cover instances in which this information is used for criminal law enforcement purposes, even if it was collected to meet planning or regulatory goals.[360]

Conversely, if data sharing programs and ordinances are designed to meet goals that are different from criminal law enforcement, such as improving the regulatory or planning capacity of a local government, and the programs include provisions that ban criminal law enforcement agencies and authorities from accessing that information without a valid warrant,[361] courts should hold that such ordinances do not involve a legitimate user privacy interest. Similarly, courts should favor ordinances that include rules and mechanisms intended to ensure that the information will be used only in these ways that do not result in unjustified privacy harms.

2. What Should Platform's Protected Privacy Interest Be?

The Fourth Amendment seeks to protect corporations from arbitrary power and, especially, police surveillance.[362] Consequently, data sharing programs should include clear guidelines that guarantee that the information shared cannot be used for purposes related to crime control or investigations against the platform or its employees without a warrant.[363]

---

[355] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[356] *See supra* Part I.

[357] *See supra* Part I.

[358] *See supra* Part II.

[359] *Id.*

[360] This would echo the exclusionary rule that prohibits the use at trial of illegally seized evidence.

[361] *See supra* Part II.

[362] *See* Carpenter v. United States, 138 S. Ct. 2206, 2213, 2218 (2018).

[363] *See supra* Part II.

B. What Local Governments Should Do

Local governments interested in implementing data sharing ordinances or programs should be mindful of the risks these programs pose for citizens and should also be strategic and adjust their programs to the requirements and expectations of Fourth Amendment doctrine and, in general, the objectives and concerns that inspire privacy law, as described in Part II. Since not all local governments have privacy frameworks of their own, nor are they bound by state privacy laws, data sharing ordinances and programs must therefore (1) be designed to meet a local government goal, (2) ensure that this goal is not related to criminal law enforcement, and (3) include mechanisms that limit how the data can be used and by whom, and preempt the agencies from receiving de-identifiable data or personal data from third parties, especially criminal law enforcement agencies, but from also other uses that can result in unjustified harms.[364] Additionally, based on the privacy concerns raised by some of the interventions highlighted here, there are best practices that can be adopted to ensure the privacy and security of the information requested. This Article suggests four.

First, when shared data is sensitive and can hypothetically be traced back to individuals, the local government should implement measures that guarantee confidentiality about the information shared with them. One way this can be done is by marking the data as confidential.[365] Similarly, the U.S. Census Bureau provides strong protections for the information it collects from individuals and business, and makes it against the law for any Census Bureau employee to disclose or publish any census information that identified individuals or businesses, even for inter-agency communications.[366] Local governments should label or format the de-identifiable data in such a way that it will not be made public under freedom of information laws and requests.[367]

Second, all forms of data gathering and storage create security risks that can take the form of data breaches or hacking attacks. Thus, local governments should also ensure within their data sharing programs that the requested information will be stored according to the highest security standards, especially if it is de-identifiable, and should also have a policy regarding for how long de-identifiable data will be stored.[368] In

---

[364] *See supra* Part II.

[365] *See Rules and Policies—Protecting PII—Privacy Act*, U.S. GEN. SERVS. ADMIN., https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act [https://perma.cc/97L2-AL8E].

[366] *See, e.g.*, *History: Privacy & Confidentiality*, U.S. CENSUS BUREAU, https://www.census.gov/history/www/reference/privacy_confidentiality/ [https://perma.cc/N4XH-BHRY].

[367] *See, e.g.*, NAT'L ASS'N CITY TRANSP. OFFS. & INT'L MUNICIPAL LAWS. ASS'N, *supra* note 34. *See also* Christopher Morten & Amy Kapczynski, *The Big Data Regulator, Rebooted: Why and How the FDA Can and Should Disclose Confidential Information on Prescription Drugs*, 109 CALIF. L. REV. 493 (2021) (explaining how data use agreements that are legally binding would allow research organizations to access some information regarding FDA data).

[368] *See* Jeschke, *supra* note 15.

all cases, local governments should also adopt binding protocols addressing how the data shared will be retained, stored, indexed, accessed, and used.[369]

Third, local governments should also be realistic and aware about the popularity of many of these platforms and the convenience of the services they provide. Platforms also have often mobilized their user base to oppose local regulation.[370] A local government seeking to request data from platforms and regulate them should thus be transparent and communicate with its constituents about the importance, welfare-enhancing nature, and prudence of such programs.

Finally, local governments could include in their data sharing programs fiduciary duties over the information collected, as privacy and technology scholars have proposed in recent years technology companies should do.[371] These duties would include a duty of confidentiality and care, to keep personal or all re-identifiable information confidential and secure with few exceptions—for example, to share with research institutions under binding and limited use agreements.[372] These responsibilities would also include a duty of loyalty that would entail that the local government agency in charge of the data sharing program cannot share that information further nor use it to manipulate end-users or the companies, or betray their trust.[373]

CONCLUSION

A paradoxical reality of our current digital information capitalism is that unlike cities, corporations have been often granted vast powers to pursue their own interests, with far less consideration of how corporate power affects, and may harm, others.[374] Yet, like all forms of power, unchecked and concentrated corporate power is prone to enhance the prosperity of those within the circle of power—property owners or shareholders—regardless of how this affects the general economy or society, and especially those left behind.[375]

Given the vast influence platforms have today in our societies and the fact that exclusive entitlements over data largely empower them to exercise that power beyond what seems their fair share, platform power should be checked too.[376] Cities are at the heart of our increasingly urban and digital present, and our concern about

---

[369] *See, e.g.*, SEATTLE, WASH. ORDINANCE 124142 (Mar. 18, 2013) (codified at Seattle, Wash. Mun. Code § 14.18); N.Y. Police Dep't, Public Security Privacy Guidelines (2009). Note, however, that the NY guidelines don't address data sharing arrangements.

[370] *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 17 (2020); Del Valle, *supra* note 66.

[371] *See* Balkin, *supra* note 370, at 11.

[372] *See* Morten & Kapczynski, *supra* note 367.

[373] *See* Balkin, *supra* note 370, at 14.

[374] *See* Kapczynski, *supra* note 319, at 1467, 1472, 1489.

[375] *See* FRUG, *supra* note 323, at 18–19, 62–63, 358.

[376] *See* Kapczynski, *supra* note 319, at 1472, 1489.

inequality in digital information capitalism, which plays out acutely between and within cities could be alternative power sites to check some of that power. Questions of data and democracy should be central to how we imagine city power for a digital age. Local data sharing ordinances are an important step in that direction.[377]

It is certainly urgent, too, to make long-term structural shifts that protect individuals in the data-economy, such as creating better social safety nets and enacting privacy laws that are not "consent-based," just as it is important that data sharing ordinances are rightly tailored.[378] Such broader provisions should work to limit what both state and private parties can do with de-identifiable information and should enhance the bargaining power of individuals in the digital information economy.

Many cities right now are, however, trying to address that issue correctly by implementing data sharing programs that could allow their constituents at large to benefit from the data we all collectively manufacture.[379] Yes, cities must tailor these ordinances and laws to prevent misuses of data and possibilities of abuse, but courts and states should also let them.

---

[377] *See* Balkin, *supra* note 370, at 14.

[378] *Id.*

[379] *Id.*