SMART ENOUGH CITIES

Governments That Seek Mobility Data Must Respect Individual Privacy

CENTER FOR DEMOCRACY & TECHNOLOGY

JUNE 2020

Smart-Enough Cities:

Governments That Seek Mobility Data Must Respect Individual Privacy

June 25, 2020

Authored by Mana Azarmi & Noah Resnick

I. Introduction

This white paper explains the growth of shared mobility services[1] such as electric scooters, dockless bicycles, and ride-sharing services like Uber and Lyft, the opportunities they provide to users, and the challenges they pose to cities. It then explores how cities have attempted to meet some of those challenges by compelling shared mobility services to, on a routine basis and for regulatory, non-criminal purposes, disclose sensitive information about how individuals use shared mobility services: trip origins, destinations, routes taken, and time of travel. It outlines the privacy, security, and legal risks (both to individuals and municipalities) of data-sharing obligations imposed by cities on shared mobility services, and then offers recommendations for how those risks could be mitigated through limitations on the types of information that can be routinely compelled from shared mobility services, and the uses to which such data can be put.

The Center for Democracy & Technology[2] believes the privacy and security risks to individuals of the compelled disclosure of information about their use of shared mobility services are clear. They largely stem from the dangers of releasing location information. This data is revealing and difficult to anonymize, raising a host of privacy issues. The risks to cities are equally great. They stem from the potential of shared mobility companies and their users challenging compelled collection of location information under privacy laws, as well as the security risks and danger of public disapproval of overly broad data collection. The goal of this paper is to help decision-makers in cities and states understand these risks and handle their responsibility as stewards of the public right of way in a privacy-respecting manner.

[1] This whitepaper uses the term "shared mobility services" to describe both rideshare services (also elsewhere labeled as services offered by Transportation Network Companies), such as Uber and Lyft, and dockless mobility platforms, such as Lime and Bird (which provide dockless, shared scooters) and JUMP (which provides dockless, shared bikes).

[2] The Center for Democracy & Technology is a nonprofit organization based in Washington, D.C., that seeks to advance individual rights in the digital age. https://cdt.org/.

II. Background

Technology is transforming the transportation options available to the public in cities across the United States. Recent years have seen a rise in shared mobility services, including app-hailing rideshares and micro-mobility options such as bicycles and electric scooters. Rideshares have experienced an explosive growth in usage over the years.[3] Electric scooters, launched in a few cities just a couple of years ago, are now in 37 states.[4] In 2018, riders took over 40 million trips on shared, dockless vehicles.[5] These services may hold the promise of making transportation faster, more accessible, and more affordable. For example, they offer a potential solution to the "first mile/last mile problem," the issue of public transportation accessibility for people who live or work far from rail and bus routes. In Sacramento, the city's regional transit agency partnered with JUMP, a dockless bike share service, to provide charging bays inside regional light rail stations.[6] The region subsequently saw an 18% increase in light rail ridership, which the agency attributed in part to its dockless mobility program.[7] These services may provide new transportation options to communities who are excluded from, or face obstacles to, accessing current offerings. While the current health crisis precipitated by COVID-19 has slowed the growth of these offerings, it is expected to continue once this health crisis passes.

But shared mobility services pose new challenges for cities and states as well. They must manage new kinds of traffic like scooters, keep streets and sidewalks safe as well as cleared and organized (a significant accessibility issue), and ensure that transportation services are equitably distributed. In order to make informed assessments of how residents are using these new services, local governments are compelling service providers to disclose records about where their users travel, when, and the routes they take. Most prominently, the Los Angeles Department of Transportation has created the Mobility Data Specification ("MDS"), a set of open-source application programming interfaces ("APIs") that enables standardized data

---

[3] *See e.g.*, Jingjing Jiang, *More Americans are using ride-hailing apps*, Pew Research Center (Jan. 4, 2019), https://www.pewresearch.org/fact-tank/2019/01/04/more-americans-are-using-ride-hailing-apps/ ("Today, 36% of U.S. adults say they have ever used a ride-hailing service such as Uber or Lyft, according to a Pew Research Center survey conducted in fall 2018. By comparison, just 15% of Americans said they had used these services in late 2015, and one-third had never heard of ride-hailing before.").

[4] Sam Sabin, *Mapping Scooters' Explosive Growth, State by State and Country by Country*, Morning Consult (Dec. 11, 2019), https://morningconsult.com/2019/12/11/mapping-scooters-explosive-growth-state-by-state-and-country-by-country/.

[5] National Association of City Transportation Officials, Shared Micromobility in the US: 2018, https://nacto.org/shared-micromobility-2018/. "Dockless here" means a mobility vehicle that does not get picked up or dropped off at docked parking stations.

[6] American Public Transportation Association, Sacramento RT and Micromobility Integration (Aug. 20, 2019), https://www.apta.com/sacramento-rt-and-micromobility-integration/.

[7] American Public Transportation Association, Sacramento RT and Micromobility Integration (Aug. 20, 2019), https://www.apta.com/sacramento-rt-and-micromobility-integration/.

sharing between shared mobility services and cities.[8] The city requires dockless mobility companies to implement MDS as a condition of operating in the city.[9] MDS is now used by a number of other cities in the United States, and over 80 cities and organizations around the world.[10] As this standard becomes more widely adopted, more information about more individuals' use of shared mobility services will be shared with local governments. While this regulatory regime has not been applied to rideshares, MDS was designed to be applied to transportation modes beyond electric scooters and other dockless vehicles, including drones and rideshares one day.[11]

CDT believes policymakers should carefully consider whether they need to compel data from shared mobility services. To the extent that they do, they should minimize the type and quantity of compelled data disclosure in order to safeguard their constituents' privacy. Additional data governance issues such as access and security must also be addressed. While the promise of location information from shared mobility services may help localities manage the challenges posed by new modes of transportation, location information can be particularly sensitive, especially when it catalogues a person's movements over time. This is why a number of recently enacted privacy laws classify geolocation information as personal information,[12] and why U.S. courts and states increasingly acknowledge the sensitivity of location information by heightening the threshold law enforcement must meet to access it.[13]

Importantly, these data-sharing obligations required of mobility service providers—imposed as a condition of operation in a particular jurisdiction—may become a model for future "smart city" ordinances. As people's lives become increasingly connected to their devices and the internet, state and local governments will have more opportunities to collect data reflecting their residents' activity. And because the data-sharing obligations discussed in this paper offer a potential template for the future, it is especially important that they are done right—with robust respect for individual privacy at their core.

---

[8] Mobility Data Specification, Github, https://github.com/openmobilityfoundation/mobility-data-specification. An API is a computing tool that allows computer programs to communicate with one another. The MDS API allows cities to efficiently obtain vast amounts of information from shared mobility platforms. It is a more efficient alternative to a shared mobility platform recording information in a spreadsheet and sending the spreadsheet via email.
[9] Dockless On-Demand Personal Mobility One-Year Permit, Los Angeles Department of Transportation, http://basic.cityofla.acsitefactory.com/sites/g/files/wph266/f/Final%20One-Year%20Dockless%20Permit.pdf.
[10] Mobility Data Specification, Github, https://github.com/openmobilityfoundation/mobility-data-specification.
[11] Laura Bliss, T*his City Was Sick of Tech Disruptors. So It Decided to Become One.*, CityLab (Feb. 21, 2020), https://www.citylab.com/transportation/2020/02/los-angeles-transportation-data-mobility-scooter-mds-uber/606178/.
[12] California Consumer Privacy Act and General Data Protection Regulation.
[13] *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. United States*, 585 U.S. ___ 138 S. Ct. 2206; California Electronic Communications Privacy Act, Pen. Code § 1546.

In this paper, we offer an initial recommendation that localities collect only aggregated data reflecting shared mobility service usage as opposed to compelling individual trip-level data. For localities that fail to heed this advice, we offer recommendations that seek to uphold the privacy interests of consumers and mitigate the legal risks to state and local governments. Our detailed guidance covers purpose limitation, law enforcement access, data retention limits, and transparency to the public.

III. Development and Influence of the Mobility Data Standards

By dint of their operation, the new internet-based shared mobility services generate vast amounts of data about service usage. Cities have noticed and have begun to compel micro-mobility service providers to disclose data reflecting consumer usage of their services as a condition of receiving a permit to operate in their jurisdictions.[14] In addition to wholly customized data reports for each city, two data standards have become default options that are frequently adopted by cities: the General Bikeshare Feed Specification ("GBFS") and the Mobility Data Specification ("MDS").

The GBFS was developed to help end users locate available docked bikes. As compared to MDS, GBFS reveals less about the travels of individual users because the data standard emphasizes findability of available devices over granular tracking.[15] It does not reveal particularly sensitive information such as where a vehicle is at every particular moment, or the specific route the vehicle took. However, while GBFS is still used to inform the public of available devices, it has fallen out of favor because cities are seeking more granular—and more sensitive—data. Regulators argue that GBFS was not designed for the regulatory purposes cities envisioned, and therefore, recent attempts to make GBFS more privacy-preserving—for example, by rotating vehicle IDs—make individual enforcement impossible. As a result, though it is more privacy-protective, GBFS is currently not being widely considered by localities as sufficient for managing dockless scooters and bicycles. The rest of this paper focuses on MDS as the major area of concern for policymakers.

MDS was born out of the introduction of e-scooters, and the difficulty presented to cities of managing hundreds if not thousands of "dockless" transportation devices. Originally created by Los Angeles Department of Transportation ("LADOT"), its development is now tasked to the Open Mobility Foundation,[16] and is being considered a potential standard for other forms of transportation in the public-right-of way. MDS is a set of open-source application programming

[14] 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/.
[15] North American Bikeshare Association, GBFS & Data Principles, https://nabsa.net/opendata/; https://github.com/NABSA/gbfs.
[16] Open Mobility Foundation, https://www.openmobilityfoundation.org/about/ ("The Open Mobility Foundation (OMF) is an open-source software foundation that creates a governance structure around open-source mobility tools, beginning with a focus on the Mobility Data Specification (MDS).").

interfaces ("APIs") that enables standardized data sharing between shared mobility services and cities.[17] MDS is meant to facilitate access to data from providers to agencies. Importantly, it was designed to facilitate a vision of a DOT as a more proactive manager of the streets, which is reflected in its data fields.[18] Rather than narrowly tailoring a data standard to a specific purpose, as GBFS did, with the MDS LADOT aimed to first collect all sensory data generated by these devices and afterwards contemplate how to use it. Its data fields include:

- *"device_id",*
- *"vehicle_id",*
- *"trip_id",*
- *"route",*
- *"start_time", and*
- *"end_time".*

This means that for every ride taken, LADOT would receive a trip's start time, its end time, and the path it took during the ride, including where it began and where it ended. This data is potentially very revealing. For example, the data could reveal a trip that starts with a home address and ends at a shop that sells firearms or a marijana dispensary. The "route" field is even more granular and revealing, and "includes every observed point in the route, even those which occur outside the municipality boundary."[19]

MDS also offers two different types of access to data—real-time and historical. The API labels these: agency and provider. While both permit the same types of data gathering, using the agency API, the provider pushes data to the city agency continuously. This is designed for real-time data collection. Using the provider API, the agency pulls data from the provider. This is designed to provide a historical snapshot of activity.[20]

Ultimately, a uniform data standard is a likely end product in the compelled mobility space, as it is attractive to both cities and providers: cities will have some guidance on how to start their own data-driven shared mobility data program if they choose to have one, and providers only need to generate only one kind of data reporting infrastructure around the country, cutting down on resource costs. That is why it is crucial that municipalities utilizing MDS consider the privacy interests of the users of shared mobility services and adjust the standard to remove compelled individual trip-level location tracking.

[17] Mobility Data Specification, Github, https://github.com/openmobilityfoundation/mobility-data-specification.
[18] Laura Bliss, *This City Was Sick of Tech Disruptors. So It Decided to Become One.*, CityLab (Feb. 21, 2020), https://www.citylab.com/transportation/2020/02/los-angeles-transportation-data-mobility-scooter-mds-uber/606178/.
[19] Open Mobility Foundation, https://github.com/openmobilityfoundation/mobility-data-specification/tree/dev/provider#routes.
[20] Understanding MDS APIs, GitHub (last accessed April 19, 2020), https://github.com/openmobilityfoundation/mobility-data-specification/wiki/Understanding-MDS-APIs.

IV. Compelled Mobility Data Disclosure Requirements Carry Great Privacy and Security Risks

At their heart, data-sharing obligations that cities impose on shared mobility services present privacy and security risks to individuals because they can involve compelled disclosure of sensitive location information. For example, MDS allows city governments to collect detailed, individualized trip information from dockless mobility services. Through MDS, cities can collect information on individual device or vehicle IDs, trip duration, distance, and route, including all possible GPS samples collected by the service provider, trip start time and end time, and even a URL to a photo showing whether the vehicle was properly parked.[21]

Location information is a highly sensitive category of personal data. This is particularly true for GPS information collected over time. It can generally reveal one's location within 10 meters, which is often enough to locate a person to specific addresses from which their activities over time can be inferred. Supreme Court Justice Sotomayor noted that a comprehensive record of a person's movements "reflects a wealth of detail about [the person's] familial, political, professional, religious, and sexual associations."[22] It can reveal visits to abortion clinics or HIV treatment centers, churches or mosques, or visits to immigration legal clinics. Similarly, U.S. Sen. Ron Wyden has affirmed that "[l]ocation information can reveal some of the most intimate details of a person's life—whether you've visited a psychiatrist, whether you went to an A.A. meeting, [and] who you might date."[23] The Supreme Court has found that a person's location tracked over time is deeply personal information that is among the "privacies of life" protected by the Fourth Amendment.[24] When the government collects and retains this information over a lengthy period of time, the government accesses "a category of information otherwise unknowable."[25] The government gains the ability to "travel back in time to retrace a person's whereabouts[.]"[26] Thus, information about a person's location can be deeply revealing.

De-identified location information can also be easily reidentified and linked to an individual. While MDS does not require the disclosure of a rider's name or another conventional identifier such as a credit card number, location information itself can often be the identifier because it is

---

[21] Mobility Data Specification, Github, https://github.com/openmobilityfoundation/mobility-data-specification/tree/dev/provider. Many dockless mobility services, such as Lime, require users to take a photo of their scooter after they have finished using it.
[22] *United States v. Jones,* 565 US 400, 415 (2012) (Sotomayor, J. concurring). In *Jones*, the Supreme Court held that when the government attaches a GPS tracking device to a vehicle to monitor a person's car for 28 days, it is conducting a search under the Fourth Amendment. Justice Sotomayor filed a concurring opinion highlighting the privacy concerns of persistent location tracking.
[23] Jennifer Valentino-DeVries et. al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[24] *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018).
[25] *Carpenter*, 138 S. Ct. at 2218.
[26] *Carpenter*, 138 S. Ct. at 2218.

difficult to anonymize and risks being affiliated with a particular individual.[27] In a frequently cited report, researchers who studied 15 months of anonymized mobile phone location data of 1.5 million people were able to uniquely identify 95% of the individuals in their study from just four data points each.[28] This was the case even though the data relied upon in the study was less precise than the GPS location data that is required under the MDS. Additionally, *New York Times* reporters have analyzed databases of de-identified location data (location data points not directly connected to an individual's name or another conventional identifier), generated by the use of cell phones and demonstrated that the data could become reidentified.[29]

Part of what makes location information difficult to anonymize is the wealth of other information that can be combined with the location dataset.[30] For example, an anonymized route of a morning commute can reveal where the commuter likely lives and works. This information frequently uniquely describes one person and is identifiable to that person. Publicly available housing records, or online employment information can reveal the commuter's identity.[31] Bruce Schaller, a former New York City transportation official, has acknowledged that "[i]t's remarkably easy to start identifying individuals" from anonymized location data,[32] such as the anonymized GPS data New York City's Taxi and Limousine Commission publicly releases about the locations of taxicabs in the city. From one dataset released in 2013, which included

[27] Yves-Alexandre de Montjoye et. al., Unique in the Crowd: The privacy bounds of human mobility, Nature (2013), https://www.nature.com/articles/srep01376 (finding that "in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals."); DJ Pangburn, *Even This Data Guru Is Creeped Out By What Anonymous Location Data Reveals About Us*, Fast Company (Sep. 26, 2017), https://www.fastcompany.com/3068846/how-your-location-data-identifies-you-gilad-lotan-privacy (discussing research conducted by Buzzfeed's data science team).

[28] Yves-Alexandre de Montjoye et. al., Unique in the Crowd: The privacy bounds of human mobility, Nature (2013), https://www.nature.com/articles/srep01376.

[29] Jennifer Valentino-DeVries et. al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; Stuart A. Thompson and 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.

[30] For example, in the famous Netflix Prize case, Netflix published 10 million movie rankings by 500,000 customers. The data was anonymized by removing personal details and replacing names with random numbers. Researchers were able to de-anonymize some of the Netflix data by comparing rankings and timestamps with public information on IMDb. A. Narayanan and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," *2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, CA, 2008, pp. 111-125. *See also* Chris Y. T. Ma et al., Privacy Vulnerability of Published Anonymous Mobility Traces, IEEE/ACM Transactions on Networking (2013) https://www.osti.gov/servlets/purl/1095747 (finding that an adversary with a small amount of side information, i.e. information not included in the location dataset itself but rather observed from the world, can often identify a victim's "anonymous" trace in a location dataset).

[31] Jennifer Valentino-DeVries et. al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[32] Aarian Marshall, *NYC Now Knows More Than Ever About Your Uber and Lyft Trips*, Wired (Ja. 13, 2019), https://www.wired.com/story/nyc-uber-lyft-ride-hail-data/.

pickup and dropoff times and locations, as well as anonymized versions of taxi license and medallion numbers, a researcher was able to identify rides taken by specific celebrities.[33]

As applied to location data generated by the use of shared mobility services, it becomes clear how individual riders could be identified from a dataset of traveler location information. Data generated by micromobility vehicles is especially sensitive because it often involves first-and last-mile transportation—transportation directly to and from the home. For example, in its year-end report in 2018, Lime indicated that 40% of riders reported commuting to or from work or school during their most recent trip.[34] Start points and end points, if connected, reveal especially intimate and identifiable information—perhaps the most unique travel behavior of individuals—where they live and work.

People also use shared mobility services for more than just their daily commute. According to the National Association of City Transportation Officials, many rides occur in the middle of the day or on weekends, suggesting social or recreational use.[35] And again, Lime in 2018 reported that 32% of Lime riders reported traveling to or from dinner/entertainment during their most recent trip.[36] Thus, not only is shared mobility location data revealing of identity, it may be revealing of interests. Forgoing attaching rider names or ID numbers to trips, as is done with MDS. is insufficient to securely protect the identity and privacy interests of the individual.

Location information, because of its revealing nature, is especially vulnerable to official misuse and is an attractive target for malicious hackers. A 2016 Associated Press study found that law enforcement officers across the country have abused official databases (outside the location information context) to obtain information on romantic partners, business associates, neighbors, and journalists.[37] Law enforcement officers have also abused automated license plate reader technology—cameras that capture passing license plate numbers, along with the location, time, and date—to target minority and low-income communities.[38] And Uber came under scrutiny in 2014 for its since-removed "God View," which allowed Uber employees to observe the real-time locations of customers requesting rides on Uber's platform.[39] This

---

[33] *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, Neustar (Sep. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.
[34] Lime, Year End Report 2018, 8 https://www.li.me/hubfs/Lime_Year-End%20Report_2018.pdf.
[35] National Association of City Transportation Officials, Shared Micromobility in the US: 2018, https://nacto.org/shared-micromobility-2018/.
[36] Lime, Year End Report 2018, 8 https://www.li.me/hubfs/Lime_Year-End%20Report_2018.pdf.
[37] Sadie Gurman, *Across US, police officers abuse confidential databases*, Associated Press (Sep. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases.
[38] Adam Goldman & Matt Apuzzo, *With cameras, informants, NYPD eyed mosques*, Associated Press (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques; Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, Electronic Frontier Foundation (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.
[39] Brian Fung, *Uber settles FTC allegations of lax data security*, Washington Post (Aug. 15, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/08/15/uber-is-settling-with-the-ftc-in-a-major-case-

location information, which can be used to stalk and harass, is susceptible to hacking and official misuse. This is of particularly high concern for survivors of gender-based assault and hate-motivated violence.

An additional risk to privacy arises as a result of state public records disclosure laws, which provide members of the public a means of requesting records in the possession of government agencies, which might include compelled mobility data. In these cases no theft or official misuse would occur. Instead, sensitive data would be released as a result of a lawful request. For example, in 2012 privacy advocates filed a request under the California Public Records Act seeking one week of automatic license plate reader data held by the Los Angeles Police Department (LAPD).[40] While the California Supreme Court ruled that the LAPD had to anonymize the records before disclosing them, effective anonymization is difficult to achieve because state and city governments will have to anticipate the various means by which the specific data being released could be reidentified.[41]

V. Compelled Disclosure of Mobility Data May Also Carry Legal Risks

Compelled data disclosures between cities and shared mobility services may violate the Fourth Amendment, the Stored Communications Act, and state privacy laws such as the California Electronic Communications Privacy Act. Companies, individual users, and drivers have important privacy interests embedded within mobility data. Governments that narrowly tailor their data-sharing requirements reduce the risk of a legal challenge. For example, in response to LADOT's decision to pursue granular data disclosures, JUMP filed suit against LADOT for warrantlessly seizing the company's business records in violation of the Fourth Amendment, the California Constitution, and the California Electronic Communications Privacy Act (CALECPA).[42] Riders of electric scooters in Los Angeles also challenged the compelled disclosure of mobility data, alleging that LADOT is violating their rights under the Fourth Amendment, the California Constitution, and CALECPA.[43]

---

over-privacy-and-security/. As a result, the company now operates under strict conditions of an FTC consent order that requires it to maintain a comprehensive data privacy program to protect user data. See, Press Release: Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims, FTC (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

[40] Automated license plate readers (ALPRs) are high-speed camera systems that can be mounted to street poles or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time, and including photographs of the vehicle and sometimes the driver and any passengers. For more information on the case, see *Automated License Plate Readers- ACLU of Southern California & EFF v. LAPD & LASD*, Electronic Frontier Foundation (last accessed April 19, 2020), https://www.eff.org/cases/automated-license-plate-readers-aclu-eff-v-lapd-lasd.

[41] *American Civil Liberties Union Foundation v. Superior Court*, 3 Cal. 5th 1032 (2017).

[42] Ruby Zefo, *Standing Up for Rider Privacy in Los Angeles*, Uber Security (March 24, 2020), https://medium.com/uber-security-privacy/ladot-mds-privacy-1eafbc412550.

[43] *Sanchez v. LADOT,* CASE NO: 2:20-cv-05044 https://www.eff.org/document/sanchez-v-ladot-complaint.

Companies have privacy interests in their user-related records. A city that obtains user-related records pursuant to an ordinance that compels a company to provide those records may be conducting a search under the Fourth Amendment.[44] The Fourth Amendment requires that a non-criminal government search be supported by: (1) an administrative warrant or subpoena; (2) individualized justification for the search; and (3) an opportunity for pre-compliance review.[45] None of these criteria is met when a city compels a shared mobility service to provide it with location data as a condition of operating in the city. Compelled disclosure of data under the MDS standard can be quite broad. It applies to all location data, covering all users at all times. Its "universality," "volume," and "infinite time horizon" likely makes it the "antithesis" of a limited administrative subpoena for business records.[46] Moreover, blanket compelled data disclosure does not provide shared mobility services with an opportunity for pre-compliance review. Unlike a subpoena for specific records, the validity of which can be challenged in court, shared mobility services have no way of challenging the compelled disclosure of specific location information. Thus, compelled disclosure, without legal process, of trip data from shared mobility services could well violate the Fourth Amendment rights of providers and individual users, which could be pursued by providers on behalf of those users.

Individual users of shared mobility services may also have another Fourth Amendment interest at stake. In *Carpenter v. United States*, the Supreme Court held that an individual had a reasonable expectation of privacy in a comprehensive record of his movements, as revealed by seven days or more of historical cell-site location data, in part because of the sensitive and revealing nature of the data.[47] Similarly, here, the location data held by shared mobility services is among the most intimate kinds of location data. In the case of dockless mobility services, it

---

[44] *Airbnb v. City of New York*, 373 F.Supp.3d 467, 482 (S.D.N.Y. 2019); see also *Patel v. City of Los Angeles*, 135 S. Ct. 2443, 2453 (2015) (applying Fourth Amendment protections to business records). Whether a business has a privacy interest in its records that is protected by the Fourth Amendment warrant requirement can turn on whether the business is closely regulated. Shared mobility services probably do not operate in an industry so closely regulated that they have no expectation of privacy in their records. The Supreme Court has only recognized four closely regulated industries, companies in which hold no expectation of privacy in their records: mining, firearms, liquor sales, and automobile junkyards. See *Airbnb v. New York*, 373 F.Supp.3d at 485 (compiling cases). The shared mobility service industry does not have a history of as pervasive regulation; nor does it involve inherently dangerous operations. Rideshare services, in particular, present the closest call because their pre-technology analogue, taxi services, have traditionally been regulated by the state. But so have hotels, and the Supreme Court in *Los Angeles v. Patel* (2015) rejected the argument that hotels were so closely regulated so as to deprive hotel proprietors of a reasonable expectation of privacy in their guest records. See *Patel*, 135 S. Ct. at 2454–56. The same should apply to rideshare services.

[45] *Airbnb*, 373 F.Supp.3d at 488. This is not a case of "special needs," in which the warrant and probable cause requirements are impracticable. Examples of "special needs" cases include some searches inside of schools, *New Jersey v. TLO*, 469 US 325 (1985), government workplaces, *O'Connor v. Ortega*, 480 US 709 (1987), and highway safety checkpoints, *Michigan v. Sitz*, 496 US 444 (1990).

[46] *Airbnb*, 373 F.Supp.3d at 391.

[47] *Carpenter*, 138 S. Ct. at 2217 (holding that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI).

CENTER FOR DEMOCRACY & TECHNOLOGY

relates to first-and last-mile transportation, as well as other transportation uses, through which information about the individual's home, workplace, and identity can be easily ascertained. Thus, even though shared mobility data is not as all-encompassing as cell-site location data, shared mobility users likely retain a legitimate expectation of privacy in their movements as revealed by that data. The compelled disclosure of location information that can be identified to an individual frequent user of shared mobility services could trigger the Fourth Amendment.

While the legal questions are more complicated, users of shared mobility services may also have statutory privacy rights. Under federal law, electronic records and communications may be protected by the Stored Communications Act ("SCA"), which prevents certain network service providers from disclosing information to the government without sufficient legal process or user consent.[48] It is unclear whether shared mobility services, in their various contexts and use cases, fall under the SCA.[49] But even assuming that they do, user consent may vitiate the SCA's disclosure prohibitions. *Airbnb v. New York City* involved an ordinance that required homeshare companies to provide host information to the city. The court found that hosts had consented to compelled disclosure of host information to the city when the hosts agreed to the homeshare platforms' terms and conditions.[50] To the extent shared mobility services contain similar notices in their terms of use,[51] drivers and users may also be deemed to have consented under the SCA to disclosures of information in the shared mobility context as well.

State privacy laws are more likely to operate to protect this data. In particular, the California Electronic Communications Privacy Act ("CalECPA") restricts government entities from "compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device."[52] And California's Legislative Counsel Bureau, a nonpartisan public agency that prepares legal opinions for the California Legislature, concluded that CalECPA's prohibition restricts a department of a city or county from imposing real-time data-sharing requirements on a dockless mobility provider as a condition of granting a

---

[48] 18 U.S.C § 2703. See *Telecommunications Regulatory Board of Puerto Rico v. CTIA*, 752 F.3d 60, 68 (1st Cir. 2014) (Puerto Rico's Registry Act was preempted by the SCA because it would have required cellular service providers "to disclose their prepaid customers' names, addresses, and phone numbers to a governmental entity without a subpoena—or any process whatsoever).

[49] The SCA applies to electronic communications services ("ECS") and remote computing services ("RCS"). A single service can be an ECS, an RCS, both, or neither, in different contexts. For example, rideshare services may act as an ECS with respect to their drivers because drivers use the in-app messaging features provided by the rideshare services. Rideshares may also act as an RCS with respect to their drivers because drivers likely use the services' apps to store their trip records—in order to account for their hours worked or miles driven, potentially vital information for driver safety and car maintenance.

[50] *Airbnb*, 373 F.Supp.3d at 496–97.

[51] Uber Privacy Notice, Uber (Dec. 12, 2019), www.uber.com/global/en/privacy/notice; Lyft Privacy Policy, Lyft (Jan. 1, 2020), https://www.lyft.com/privacy#privacy-how-we-share-your-information; Privacy Notice, Lime (Jan. 1, 2020), https://www.li.me/privacy.

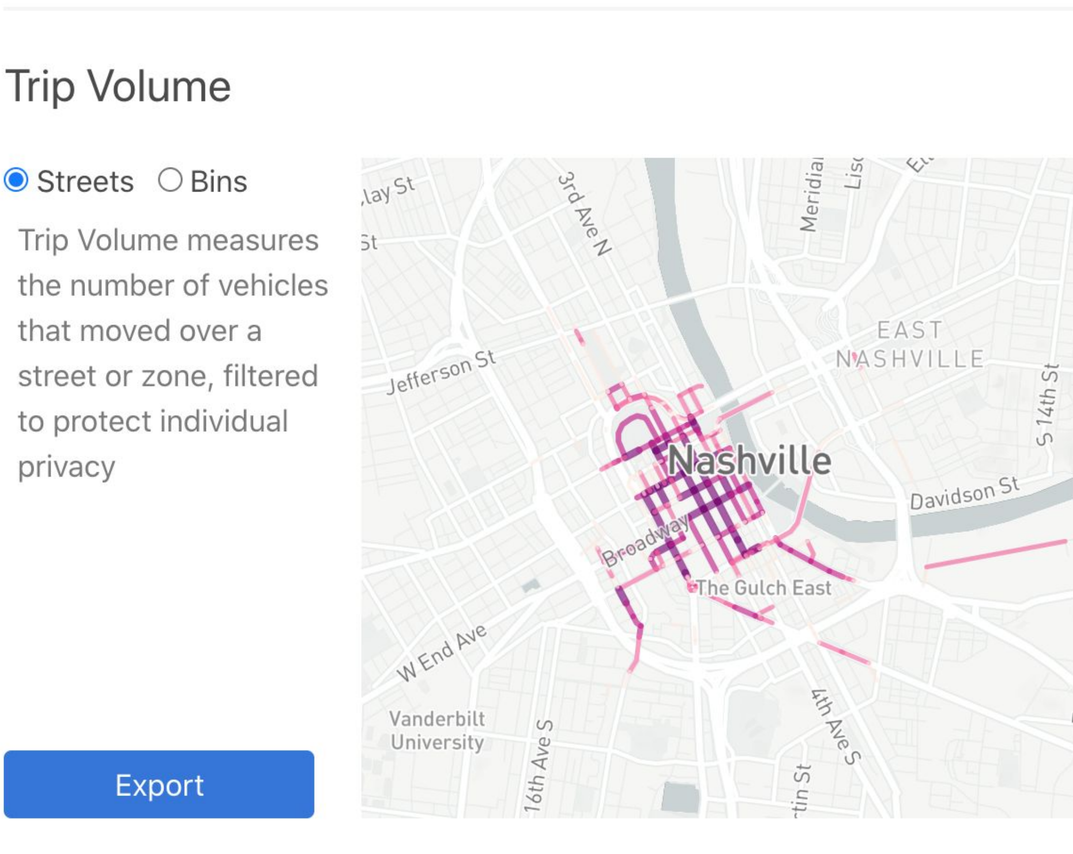
[52] CA Pen. Code § 1546.1(a)(2).

permit.[53] Other states, such as Montana and Maine, have similar privacy-protective laws that may also apply.[54]

VI. Recommended Privacy and Security Safeguards

This paper outlined the attendant prevalent privacy impacts on individuals and legal risks to cities and state governments in requiring, without legal process, shared mobility services to produce service usage data. Cities and states that compel such data from service providers can mitigate those risks by adopting privacy and rights-respecting policies.

As an initial matter, we urge localities to resist compelling two classes of particularly sensitive data: individual trip data and real-time data. These records are very sensitive, and alternatives to disclosure of this information can achieve the goals for which this information is sought.



Example of aggregate usage data from SharedStreets Mobility Metrics. Screenshot taken [2020-06-24](#).

[53] Legislative Counsel Bureau, California Electronic Communications Privacy Act - #1916004 (Aug 1, 2019), https://cdn.theatlantic.com/assets/media/files/calecpa_dockless_mobility_provider_lc_opinion_(2).pdf.
[54] Montana House Bill No. 603, https://leg.mt.gov/bills/2013/billhtml/HB0603.htm; Maine Public Law, Chapter 409, http://www.mainelegislature.org/legis/bills/bills_126th/chapters/PUBLIC409.asp.

Instead of raw trip data, localities should instead request providers disclose aggregated usage data, which serves the dual purposes of preserving individual privacy and providing insights to guide planning purposes. Aggregating data is the process of grouping data and generating statistical summaries for those groups.[55] While steps must be taken to ensure the aggregation sufficiently masks identity, this type of disclosure can serve both privacy and governmental interests.[56] Instead of receiving individual trip data, governments could receive insights in the form of heat maps to show which regions have relatively high volumes of trip traffic, or at what times generally ridership is great. This data still provides useful patterns of location information, allows governments to better distribute vehicles, design and update traffic infrastructure, and organize the streets. Shared mobility service providers have the ability to do this without adopting MDS through the use of internal or external tools.[57] If cities are concerned about the reliability of aggregated data, there are technical solutions available to audit data's integrity.[58]

One of the most alarming elements of MDS is the fact that it facilitates real-time location disclosures. There is no city planning purpose that justifies the collection of consumers' real-time location information while a consumer is mid-ride. Additionally, enforcement of permitting requirements can and should be achieved through more tailored requests, or occasional auditing. Real-time location information is much more sensitive than historical location information. It is much closer to the type of ubiquitous surveillance associated with surveillance states. It also means that criminals and others who wrongly access information will have a much greater range of options for harm. Stalkers can intercept a rider. Thieves can know whether an individual is at home. While accessing real-time rider information does not allow for the type of ubiquitous surveillance that access to some types of information (such as real-time cell phone information) does, it raises real risks. Those risks simply aren't offset by commensurate agency benefits or interests. For this reason, we strongly disfavor the adoption of the agency API and collection of real-time information.

Should localities wish to move beyond collection of aggregate historical information in some cases, below we highlight some best practices to mitigate the privacy, security, and legal risks discussed in this paper. The theme of these recommendations is that a city can deliver services efficiently without being all-knowing: being "smart enough" is all that is needed.

---

[55] For a series of examples *see*, Mana Azarmi & Andy Crawford, *Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies*, Center for Democracy & Technology, (May 29, 2020), https://cdt.org/insights/report-use-of-aggregated-location-information-and-covid-19/.
[56] Morgan Herlocker, *Aggregating trip data using k-anonymization*, Medium (Nov. 6, 2019), https://medium.com/sharedstreets/aggregating-trip-data-using-k-anonymization-727d5a6413f3.
[57] *See e.g.*, Shared Streets, Mobility Metrics (last accessed April 19, 2020), https://sharedstreets.io/mobility-metrics/.
[58] *See e.g.*, EFF/OTI letter to LADOT, 13, https://www.eff.org/files/2019/04/03/eff_oti_letter_re_ladot_mds_privacy_concerns_april_3_2019.pdf.

A. Articulate Clear, Limited Purpose for Data Collection and Collect Only for That Purpose

Governments that collect mobility data must articulate clear, limited purposes for doing so. Such purposes may include assessing how shared mobility services can better integrate with existing transportation options, identifying needed transportation infrastructure improvements such as where and how to place bike lanes, and where to locate dockless mobility infrastructure. For example, the city of Alexandria, VA, conducted a "dockless mobility pilot" in which the city evaluated the use of shared mobility services, in particular electric scooters, within the city and sought data from service providers.[59] Alexandria used the data from this pilot to identify areas in which high ridership rates warranted installing parking corrals to keep sidewalks free of scooters, and also established areas in which scooters could not be ridden.[60] Another clear, limited purpose for collecting mobility data is to promote equitable distribution of shared mobility services. Ensuring the distribution scooters at the start of every day to otherwise underserved locations and the provision of incentives to promote such distribution are clear, specific purposes for mobility data collection—and don't require invasive information like real-time data transfer.[61]

Once a municipality has articulated these purposes, it should collect only the data necessary to achieve those purposes. This process can help a government identify privacy issues that must be mitigated. For example, a number of cities recognize that their city planning needs do not necessitate collecting data that can be readily associated with a particular traveler.[62]

In our view, it is never necessary for cities to obtain or compel specific trip route data for city planning purposes. For example, if a city's goal is to ensure equitable distribution of dockless mobility vehicles, the city need not collect location information on every single device over a lengthy period of time. An occasional daily or weekly sampling of dockless vehicle locations may be sufficient. Or, if a city wants to know where it needs to build a new bike lane or adjust traffic lights, the city can collect aggregated rideshare data to determine which routes are most popular at various times. In both scenarios, the city achieves its goals and the risks to individual privacy are mitigated.

---

[59] City of Alexandria, Alexandria Dockless Mobility Pilot Evaluation, (Nov. 2019), https://www.alexandriava.gov/uploadedFiles/tes/info/EvaluationReportReducedSize.pdf.

[60] City of Alexandria, Alexandria Dockless Mobility Pilot Evaluation, 11 (Nov. 2019), https://www.alexandriava.gov/uploadedFiles/tes/info/EvaluationReportReducedSize.pdf.

[61] *See e.g.*, Chicago, *E-Scooter Share Pilot Program*, https://www.chicago.gov/city/en/depts/cdot/supp_info/escooter-share-pilot-project.html.

[62] For example, Baltimore's ordinance regulating the use of shared mobility devices acknowledges the sensitivity of the data at issue, and specifies that the data providers reporting data "may not include information that can reasonably be used to contact or distinguish a person." https://transportation.baltimorecity.gov/sites/default/files/cc19-0324~CommReprint(3).pdf.

Unfortunately, some cities have taken a more expansive approach to data collection. Some compel *all* the raw data provided through MDS, including, but not limited to, collecting real-time location data and displaying it in real time to the public. The thinking behind an expansive approach is to collect as much data as possible, figure out what is useful, and then later tailor the collection.[63] Such an expansive approach exacerbates the privacy risks to individuals and the legal risks to cities highlighted above. In contrast, a narrow data collection approach mitigates the potential privacy harms individuals face, while still allowing cities to achieve their policy objectives.

B. Institute Appropriate Data Access Controls

Once a government obtains data it must still carefully control access to it. In the shared mobility space, two actors warrant special attention: law enforcement and third-party data aggregators and data analysts.

Law Enforcement

The Fourth Amendment was crafted in response to "the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[64] General purpose access to an individual's location history without suspicion of criminal wrongdoing raises a similar concern today. While the requisite level of legal process for data collection can vary in the non-criminal context, when law enforcement seeks precise location information over time for criminal investigation, a warrant is required. Moreover, outside of the Fourth Amendment, many state laws that protect location data also explicitly prohibit warrantless law enforcement collection.[65] Finally, absent strong access controls with respect to law enforcement, many riders may be deterred from using shared mobility services, particularly those from communities with strained relationships with law enforcement or concerns about data sharing with immigration enforcement. Thus, it is especially important to bar law enforcement from direct access to data collected for other purposes.

Many cities have already adopted this practice. The data-sharing obligations in Austin and the District of Columbia, for example, both specify their cities' departments of transportation as the

---

[63] 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 (When asked for examples of policy decisions that require individual trip data instead of aggregated data, Reynolds demurs. "If data is aggregated before I touch it, I lose options of what to do or analyses to run," she says. "Talk to me in two months after the system is in operation, and I might have decided I really don't need the disaggregated data. . . . That's why MDS is open and versioned. We're learning a ton as we iterate.")
[64] *Riley v. California,* 134 S.Ct. 2473, 2494 (2014).
[65] E.g. Utah H.B. 57, https://le.utah.gov/~2019/bills/static/HB0057.html.

recipients of shared mobility data.[66] Santa Monica and Chicago, meanwhile, only specify the "city" as the recipient.[67] A model obligation would delineate the city's department of transportation as the only recipient of shared mobility data.

Law enforcement officers seeking location data generated by operation of a shared mobility service should generally be required to seek to compel its disclosure from the service provider using proper legal process (usually, a warrant), as opposed to seeking it on a less formal basis from a city's department of transportation or state regulators.[68] Such informal arrangements risk massive privacy invasion, and consumer backlash when it becomes public. Shared mobility services operate at arm's length from law enforcement, and are therefore better situated to protect individual users' privacy interests. Unlike most city departments of transportation, shared mobility services have sophisticated processes for dealing with law enforcement data requests.[69] As such, they are better able to assess the sufficiency of legal orders and are more likely to challenge insufficient or overbroad demands in court, upholding user privacy.[70] Shared mobility services also have a greater incentive to provide user notice of a law enforcement data demand, and where permitted, such notice can enable a user to challenge the sufficiency of the legal process being used.

---

[66] Director Rules for Deployment and Operation of Shared Small Vehicle Mobility Systems, Austin Transportation Department, http://austintexas.gov/sites/default/files/files/Transportation/Dockless_Final_Accepted_Searchable.pdf; Terms and Conditions for the Public Right-Of-Way Occupancy Permit, DC Department of Transportation, https://ddot.dc.gov/sites/default/files/dc/sites/ddot/2019.11.6%20Shared%20dockless%202020%20Terms%20and%20Conditions%20scooter.pdf.

[67] Shared Mobility Device Pilot Administrative Regulations, City of Santa Monica, https://www.smgov.net/uploadedFiles/Departments/PCD/Transportation/SM-AdminGuidelines_04-19-2019_Final.pdf; Requirements for Scooter Sharing Emerging Business Permit Pilot Program, City of Chicago, https://www.chicago.gov/content/dam/city/depts/cdot/Misc/EScooters/EScootersPilotProgramTerms_06-07-19.pdf.

[68] This is no hypothetical. Law enforcement has already sought this data from local departments. California Joint Hearing Senate Transportation and Senate Judiciary Committee, Tuesday February 25, 2020, at 1:20:26 https://www.senate.ca.gov/media/joint-hearing-senate-transportation-senate-judiciary-committee-20200225/video.

[69] *See e.g.*, Guidelines for United States Law Enforcement, Uber (Jan. 16, 2020), https://www.uber.com/legal/en/document/?name=guidelines-for-law-enforcement&country=united-states&lang=en.

[70] If a city wants to allow law enforcement to collect shared mobility data from its department of transportation, it is especially important for the city to have a brief data retention policy (discussed in the following section). The department of transportation should require a warrant, supported by probable cause, before releasing location data to law enforcement. And law enforcement should provide simultaneous notice to the relevant shared mobility service and individual when it makes such a request, so that the shared mobility service or individual can challenge the validity of the request in court.

Third Party Data Aggregators and Analysts

Not all cities have the technical capacity to operate the MDS internally because of its complex design, and the need to develop infrastructure to request and store the data. As such, some cities hire third parties to digest and make sense of the data compelled from mobility service providers. Third-party aggregators can be hired to anonymize, aggregate, and display mobility data in a privacy-protected way.[71] But cities should exercise caution in compelling providers to share raw location data with third parties (and we have a stronger preference for the aggregation to happen on the provider side). First, cities should make sure that third-party partners have proper privacy and security policies in place to handle data safely. And second, cities should enter into use-limiting contracts with third parties to ensure that data is not used for commercial purposes, or abused for personal purposes. And finally, cities that enter into agreements with third-party entities have an obligation to audit the companies to ensure that they are complying with these policies.

C. Promptly Delete Unneeded Data

A third key protection is that cities should only retain data as long as is required to achieve the purposes for which it was collected. Lengthy retention periods of historical location information present potentially significant privacy harms to individuals. Cities can avoid these harms by setting brief retention periods and clear deletion schedules. To date, this has not become common practice. Los Angeles announced a retention policy of "no less than two years," but it has not articulated any retention limits or deletion requirements.[72] Other cities, such as Chicago and Austin, fail to reference data retention or deletion at all in the data-sharing policies announced through their cities' permit applications.[73]

Data deletion is an important element of both safeguarding individual privacy and protecting cities. A breach of raw data would undermine user trust. It might also be costly. Under many state data breach laws, municipalities must report when they lose data. This can be a cumbersome and expensive process. In fact, the average cost of a data breach incident for companies in the United States is $3.92 million.[74] A model data-sharing obligation should specify a brief retention period and frequent deletion requirements. Data deletion

[71] Shared Streets, https://sharedstreets.io/; Ride Report, https://www.ridereport.com/; Remix, https://www.remix.com/; Populus, https://www.populus.ai/.
[72] LADOT Guidelines for Handling of Data from Mobility Service Providers, City of Los Angeles, https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-Protection-Principles.pdf.pdf.
[73] Director Rules for Deployment and Operation of Shared Small Vehicle Mobility Systems, Austin Transportation Department, http://austintexas.gov/sites/default/files/files/Transportation/Dockless_Final_Accepted_Searchable.pdf; Requirements for Scooter Sharing Emerging Business Permit Pilot Program, City of Chicago, https://www.chicago.gov/content/dam/city/depts/cdot/Misc/EScooters/EScootersPilotProgramTerms_06-07-19.pdf.
[74] *Cost of a Data Breach Study*, IBM (last accessed Jun. 1, 2020), https://www.ibm.com/security/data-breach.

requirements and data retention limits should also extend to third-party data aggregators. For more information on best practices for data deletion, please see CDT's white paper on the issue, "The Legal, Policy, And Technical Landscape Around Data Deletion."[75]

D. Focus on Collecting Aggregate Information

As discussed above, we urge municipalities to rely exclusively on aggregated data. We simply do not believe there is any city planning purpose for which the mass collection of granular individual trip-level data is necessary to collect and retain. But even if municipalities are collecting some raw data, aggregation should be a central component of any data-sharing obligation between cities and shared mobility services because it is a much more privacy-protective approach while still providing significant benefit for municipal regulators.[76] For example, in Sacramento, City of Transportation officials use aggregated data to inform city planning needs.[77] The city collects the number of trips, the number of active vehicles, total distance, and trip time, all in aggregated form. Sacramento uses Shared Streets to aggregate the data for the city to identify high-volume areas of usage for city planning.[78] It collects start and end data which is not connected to route data in order to identify parking needs.

Another solution that is inferior to pure aggregation but provides some security benefit is for cities to process the data they collect in a way that masks identifiable information. Minneapolis offers a model example. In its pilot program, the city did not store any raw location data, instead processing all location data in memory (where it was quickly overridden with new data).[79] Minneapolis then discarded the hashed vehicle IDs assigned by the companies and replaced them with new IDs from the city, making it more difficult to link back to the original source.[80] Finally, the city adjusted trip start and end times to the nearest half hour, or classified them within time blocks, and adjusted trip start and end points to an average of the nearest three

---

[75] Michelle De Mooy et. al., *Should it Stay, or Should it Go?*, Center for Democracy and Technology (Feb. 2017), https://cdt.org/wp-content/uploads/2017/02/2017-02-23-Data-Deletion-FNL2.pdf.

[76] Note that in cases where a provider is unwilling or unable to provide aggregate information, cities can take in raw data themselves, aggregate the data to further their policy goals, and then delete the raw data. This solution is disfavored because it requires more transfer of data (increasing security risks) and relies on municipalities to promptly and completely purge data.

[77] Statement of Jennifer Donlan Wyant, California Joint Hearing Senate Transportation and Senate Judiciary Committee, Tuesday February 25, 2020, at 1 hour 58 to https://www.senate.ca.gov/media/joint-hearing-senate-transportation-senate-judiciary-committee-20200225/video.

[78] Morgan Herlocker, *Citizen Privacy and City Oversight Needs Are Compatible: Our views from the California Senate Hearing*, SharedStreets (Feb. 26, 2020), https://medium.com/sharedstreets/citizen-privacy-and-city-oversight-needs-are-compatible-26fb262cc7a.

[79] Mobility Data Methodologies and Analysis, Minneapolis, http://www.minneapolismn.gov/www/groups/public/@publicworks/documents/webcontent/wcmsp-218311.pdf.

[80] Mobility Data Methodologies and Analysis, Minneapolis, http://www.minneapolismn.gov/www/groups/public/@publicworks/documents/webcontent/wcmsp-218311.pdf.

center points on a street.[81] Each of these steps made the location information less identifiable, and thus more protective of individual privacy.

Another privacy-protecting solution is for cities to not collect route start and end points at all. For example, shared mobility services could cut off route information one to four blocks from the start and end of each trip. The services could then provide cities with two forms of data: one map highlighting routes, with their start and end points removed, and one map detailing static vehicle location data. Routes would be less personally identifiable, but cities would still receive sufficient data to manage infrastructure updates and equitable distribution. This solution would not be privacy-protective in all scenarios—for example, if someone lives and travels to an isolated area—so it is less preferable to aggregation, but it could still protect privacy in many high-traffic locations.

E. Cities Must Secure the Data They Possess

Cities must be responsible stewards of traveler mobility data. We strongly urge localities that choose to store raw data to purge it quickly. While retaining data, they should ensure that the location data that they collect is encrypted, both in transmission to and on their servers. Some municipalities have already begun to take these measures. Los Angeles has designated MDS data as "confidential" under the city's data handling guidelines, which means that the data must be encrypted in transmission, password-protected in storage, and not subject to disclosure under open records laws.[82] Cities should also classify the raw location data that they collect as "personal information" and beyond the reach of open records laws. As noted earlier, even "de-identified" location data can be easily traced back to an individual, thus, cities should also ensure that any stored data is obfuscated to protect against potential breaches. In their data-sharing obligations, cities should specify the methodologies they plan to use to obfuscate the identity of individuals.

F. Be Transparent About Policies and Changes

When dealing with the collection of information related to an individual's activity, including sensitive location information, government agencies have a duty of transparency. They should provide clear, public notice to users that data reflecting their usage of shared mobility services is being collected by the providers and shared with a government agency. Governments should detail the kinds of data that they are collecting and the ways in which they plan to use that data, and do so in a manner that is easy for users and the public to find and understand. Such documentation must not be hidden in ancillary policy documents or advisory opinions, but

---

[81] Mobility Data Methodologies and Analysis, Minneapolis, http://www.minneapolismn.gov/www/groups/public/@publicworks/documents/webcontent/wcmsp-218311.pdf.
[82] LADOT Guidelines for Handling of Data from Mobility Service Providers, City of Los Angeles, https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-Protection-Principles.pdf.

rather displayed prominently with the data-sharing obligations themselves. Cities should also permit shared mobility services to report government disclosure obligations to their users.

Cities should also promote or facilitate community involvement in developing their data-sharing policies, and organizational accountability in monitoring those policies. As an analogue, the movement for Community Control Over Police Surveillance (CCOPS) has led some cities to pass laws requiring community involvement and oversight of city purchasing of surveillance technology.[83] As part of CCOPS, city governments that seek to purchase and use surveillance technologies are obligated to craft privacy impact assessments, released to the public and city council, that account for data management and privacy risks.[84] The public and city council then assess whether the city has done a sufficient job planning for its proposed use of the new technology. The same should apply here. Changes to MDS, for example, should not just be made to the code base, out of view to most residents. Same with any agency decisions to change the data they seek from providers.[85] The community must be provided some opportunity to meaningfully engage with jurisdictions about whether the proposed collection of data is necessary for government objectives and sufficiently protective of user privacy. Finally, cities should release privacy impact assessments addressing the privacy risks associated with each change, and the planned course of action to address each risk.[86]

These steps are important to preserve community trust and to eliminate unwarranted suspicion. Without such measures, individuals could be chilled from using shared mobility services due to fear of unwarranted surveillance, particularly those communities with whom relationships with law enforcement or immigration enforcement are strained. These are often the same communities that would benefit most from new modes of transportation.

---

[83] *See e.g.*, CB 118930, An Ordinance relating to The City of Seattle's acquisition and use of surveillance technologies, https://www.eff.org/files/2018/05/17/seattleccops.pdf.

[84] Community Control Over Police Surveillance + Militarization (CCOPS+M) Model Bill, ACLU, https://www.aclu.org/other/community-control-over-police-surveillance-militarization-ccopsm-model-bill; Draft Anticipated Impact Report, Oakland Department of Transportation (May 31, 2019), https://www.documentcloud.org/documents/6158513-DataSharing-Anticipated-Impact-Report-DRAFT-5-31.html.

[85] For example, a change to DC's permit requirements was made without notice to the public. *See* CDT's Letter to the District DOT Regarding Mobility Data, Center for Democracy & Technology (march 20, 2020), https://cdt.org/wp-content/uploads/2020/03/2020-03-20-CDT-Letters-to-DDOT-LADOT-regarding-mobility-data.pdf.

[86] For example, the City of Oakland adopted a Surveillance and Community Safety Ordinance in 2018, their version of a CCOPS ordinance. In compliance with this ordinance the City's Department of Transportation approached the civilian operated Privacy Advisory Commission to develop a surveillance use policy and privacy impact assessment for the proposed mobility data program. These documents were approved by the City Council on September 17, 2019. See approval and discussion of the DOT's outreach to the public and privacy groups at https://oakland.legistar.com/LegislationDetail.aspx?ID=4121230&GUID=C30FD950-CE2D-47B1-A95E-F703D0B99070&Options=&Search=. Privacy Impact Assessment found here, https://cao-94612.s3.amazonaws.com/documents/DataSharing_Anticipated-Impact-Report_DRAFT_5-31.pdf.

VII. Conclusion

The increasing use of shared mobility services has resulted in increased demands for disclosure to cities of very granular and personal information about such uses. The information that cities seek includes detailed trip information that can reveal a person's sensitive activities and interests, including those being pursued in real time. Moreover, the adoption in many localities of the Los Angeles DOT's Mobility Data Specification reduces the friction that would otherwise slow disclosure of this sensitive information.

Compelled disclosure of mobility data carries significant legal risks for cities, but those risks can be mitigated if they choose to be "smart-enough." Cities can rely on aggregated data disclosed by the mobility service provider, rather than individualize data compelled disclosure of which carries legal risk. To the extent cities compel disclosure of disaggregated data, they should protect user privacy by limiting their collection of data to that which is necessary to achieve a clear and narrowly stated purpose, controlling the flow of such data to law enforcement entities and third-party aggregators, deleting unneeded data and securing the data that is needed, and by being transparent about the data they are collecting and the uses to which it is being put.