More Mobility Options, More Data: Transportation and Privacy Issues in Shared Mobility Data Use

Joint Informational Hearing
Senate Transportation Committee and Senate Judiciary Committee
State Capitol, Room 4203
Tuesday, February 25, 2020 1:30pm

BACKGROUND PAPER

I. Introduction

The purpose of this joint hearing is to explore what data is being collected by shared-mobility providers and what is being done with it. It will explore how and what those providers are sharing with government entities and academics and how those entities and academics are using shared-mobility data. Finally, the hearing will turn to crafting legislation in order to better protect the privacy of consumers while enabling transportation planning, enforcement, operations, and research. A separate hearing held on November 4, 2019 by the Senate Governance & Finance Committee and Assembly Transportation Committee addressed the balance between state and local regulations on shared mobility devices. The background paper for that hearing detailed how transportation network companies (TNCs) are regulated, the types of shared mobility devices and trends in their use, and some of their impacts on local governments.

This background paper covers:

- An overview of shared mobility data use;
- Current use of shared micromobility data by local governments;
- The governance of TNC data by the California Public Utilities Commission (CPUC) and recent developments in relevant CPUC proceedings;
- California privacy law;
- Perspectives on privacy and data management practices; and
- Recent legislation relating to shared-mobility data sharing.

II. Overview of shared mobility data use

Shared mobility is the shared use of a vehicle, bicycle, or other mode of transportation. Advances in location-based services, the Internet, and mobile technologies have recently enabled new, app-based shared mobility services.[1] These services have exploded over the last decade and are now ubiquitous in many cities throughout the state. From a meager existence in 2010, TNCs provided over 100 million trips in California between 2014 and

[1] Shaheen, S., and Cohen, A. (2019). *Shared Micromoblity Policy Toolkit: Docked and Dockless Bike and Scooter Sharing*.

2015 alone.[2] In 2018, people took 84 million rides on shared bikes and scooters (shared micromobility devices) across the country.[3] This was twice the number of shared micromobility rides taken in 2017, due in part to the deployment of shared scooters in 2018.

The proliferation of these innovative shared mobility services is transforming urban transportation, but identifying and understanding the effects and channeling this change in service of the public interest has proved difficult. What are the varied impacts of shared mobility services on vehicle miles traveled, congestion, safety, and equitable access to transportation? How can these impacts be planned for and the public right-of-way managed effectively?

The data needed to address these questions are generated through the networked nature of these services themselves, including vehicle location data. In order to regulate TNCs and make them more environmentally friendly, the CPUC requires them to provide disaggregated data on each trip in California. For their part, cities are collecting aggregated and/or disaggregated data from shared micromobility providers often using one of a handful of data specifications. This is often accomplished by implementing permitting systems that require data sharing from providers operating within their jurisdiction. In addition, academics often work with publicly available shared mobility data or negotiate access to proprietary data directly with providers. Such data enable informed planning, enforcement, and operations at the city, regional, and state level. It also enables academic researchers to analyze the effects of various transportation policies.

However, collecting shared-mobility data also raises privacy concerns and legal questions, even where information is aggregated or deidentified. Where and when individuals are traveling "provides an intimate window into a person's life, revealing not only [their] particular movements, but through them [their] 'familial, political, professional, religious, and sexual associations.'"[4] Removing a person's name from their trip data does not guarantee their movements will not be traced back to them. In one study, researchers found that only "four spatio-temporal points [were] enough to uniquely identify 95% of the [1.5 million] individuals" in the study, concluding that "human mobility traces are highly unique" and "even coarse datasets provide little anonymity."[5] Meanwhile, the Trump administration has "bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement."[6]

---

[2] CPUC. *Summary of Transportation Network Companies' Annual Reports 2014 and 2015 submissions.*
[3] National Association of City Transportation Officials. (2019). *Shared Micromobility in the U.S.:2018.*
[4] *Carpenter v. United States* (2018) ___U.S.___ [138 S.Ct. 2206, 2217], quoting concurrence by Justice Sotomayor in *United States v. Jones* (2012) 565 U.S. 400.
[5] De Montjove et al. (2013). *Unique in the Crowd: The privacy bounds of human mobility*. Scientific Reports 3, Article Number 1376. https://www.nature.com/articles/srep01376 [as of Feb. 19, 2020]. All further Internet citations are current as of February 19, 2020.
[6] Tau, B. and Hackman, M. (2020). *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*. Wall Street Journal. https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=hp_lead_pos5.

At least one of the data specifications cities use to ingest shared micromobility data, the Mobility Data Specification (MDS), could be used or expanded for use with other forms of transportation, including carshare, TNCs, autonomous vehicles, microtransit, and aerial drones. Local regulations can require shared-mobility providers to provide a variety of data, including device geolocation data throughout individual trips. In the long term, there are plans to build out the data specification "into a framework for synchronizing physical systems with" detailed digital city replicas called "digital twins."[7] A city using this technology might have the ability to "begin to guarantee curb space…; react immediately to public safety issues; and explore a variety of government-to-business pricing models… Road closures can be digitally communicated to vehicles, mobility service providers, and navigation products like Google Maps and Waze."[8] Some transportation experts predict that the trends of shared mobility, automation, and electrification will eventually dominate mobility.[9] In this future, a city could have a living portal into virtually all vehicular movement.

Such a future is filled with opportunities and motivates transportation planning departments throughout the state. However, it also elicits images of Big Brother from George Orwell's strikingly prescient novel *1984*. In fact, many privacy and consumer groups have raised concerns that data specifications currently in use are not properly protecting the uniquely sensitive data at issue, including concerns with use, retention, and storage policies.[10] While the data, especially granular, individual trip data, is useful in transportation planning, enforcement, and management, its systematic collection can arguably constitute inappropriate government surveillance and put customers' personal information at risk, infringing on Californians' constitutional right to privacy if sufficient safeguards are not put into place.

Fortunately, there is not a zero-sum game between data access and respecting the fundamental right to privacy. Policy-making may support both public policy goals. The goal of this informational hearing will be to explore what the right balance may be and the role of legislation at the state level in providing proper guardrails for data sharing and use.

III. Current use of shared micromobility data by local governments

In the wake of the disruptive deployment of dockless, shared electric scooters in 2018, many local authorities, including the Los Angeles Department of Transportation

[7] Open Mobility Foundation. (2019). *Open Mobility Foundation White Paper*.
[8] Los Angeles Department of Transportation. (2019). *Technology Action Plan*. https://ladot.io/wp-content/uploads/2019/03/LADOT-TAP-v7-1.pdf
[9] Sperling, D. (2018). *Three Revolutions: Steering Automated, Shared, and Electric Vehicles to a Better Future.* Island Press.
[10] Electronic Frontier Foundation. (2019). *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification.* https://www.eff.org/document/eff-oti-letter-urgent-concerns-regarding-lack-privacy-protections-sensitive-personal-data; Center for Democracy & Technology. (2018) *Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility*, https://cdt.org/insights/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/.

(LADOT), City of Santa Monica, Oakland Department of Transportation, San Francisco Municipal Transportation Authority, and San José Department of Transportation, quickly moved to develop pilot programs or institute permanent regulations. These typically include data-sharing requirements. These entities have asserted that the data sharing requirements generally enable one or more of the following:

- Management of permittees and operating permit programs;
- Enforcement of permittees' adherence to permit terms and conditions;
- Evaluation of permit programs;
- Collection of data to support planning efforts consistent with the agency's strategic goals;[11] and
- Active management, including the use of real-time digital communications to convey mobility policies and regulation to devices using the public right-of-way.[12]

However, the regulations take many forms based on local needs, priorities, and budgets. Local authorities generally require shared micromobility providers to post data to the local authority via two main data specifications. Broadly, the General Bike Feed Specification (GBFS) offers real-time locations of available devices. MDS can capture granular data, such as in-trip data, which may be shared in real-time or after the fact. Regulations may also require regular reporting of key metrics.

There are various categories of information local authorities may require. They may seek fleet information in order to make it possible to enforce regulations such as caps on the number of devices that can be operated; deployment or distribution requirements, such as specifying locations where scooters must be deployed at the start of each day; geographic limitations for bans on scooter use in certain districts; or requirements for utilization rates. Fleet information can include:

- Total monthly users;
- Hourly fleet utilization;
- Number of devices deployed;
- Number of trips per device;
- Real-time location of available devices; and
- Real-time location of out of service devices.

Local authorities also seek trip data, which can be used, for example, to illuminate heavily-trafficked routes suitable for bike lane upgrades or a fixed-transit route; help cities that require users to park devices at bicycle racks identify common trip end points where new bicycle racks should be installed; evaluate to what extent shared

[11] San Francisco Municipal Transportation Agency. (2019). *Powered Scooter Share Program*, https://www.sfmta.com/sites/default/files/reports-and-documents/2019/12/1._scoot_permit_and_terms_2019.pdf.
[12] LADOT. *Frequently Asked Questions.* Accessed February 20, 2020. https://ladot.io/faq/.

micromobility trips may be connecting with transit; and inform management of congestion and traffic flow. This information can include:

- Trip start and end times;
- Trip start and end locations;
- Trip costs; and
- Trip routes.

Local authorities may collect aggregated and/or disaggregated trip data. The latency between a trip and collection of information about that trip also varies among localities. Finally, local authorities may also use required information to identify safety concerns, enforce specific response times for complaints regarding improperly-parked scooters, assess environmental impacts of devices, and oversee implementation of equity objectives. Some localities contract with various private companies, such as Remix or Populus, which ingest disaggregated data and make aggregated distillations of the data available to the local authorities through a data dashboard. There are also cities that make some mobility data publically available. For example, Austin, Texas publishes mobility data including the district in which each trip starts and ends, on its "open data portal."[13]

Researchers at the University of California Institute of Transportation Studies (UC ITS) surveyed the UC ITS research network for shared mobility policy and planning questions and analyzed the data needed to address each question.[14] They found disaggregated data would benefit multiple applications. For example, evaluation of Active Transportation Program investments and modeling potential locations and dynamic pricing schemes for toll lanes. However, they noted that less accurate but still informative studies could be performed with aggregated data.

Looming behind this data collection are privacy concerns, which are exacerbated when the data collected can be connected back to individual consumers. In response, privacy advocates call for legislation restricting the sharing and use of granular trip data. One group, Electronic Frontier Foundation, supports such legislation:

> Aggregated and deidentified data can provide important insights into how Californians are using TNCs and shared mobility devices for their transportation needs. Limiting local authorities to such data strikes the appropriate balance between protecting individual privacy and ensures that local authorities have the information they need to regulate our public streets so that they work for all Californians."

[13] Data.austintexas.gov. Accessed February 20,2020. https://data.austintexas.gov/Transportation-and-Mobility/Shared-Micromobility-Vehicle-Trips/7d8e-dm7r.
[14] Matute, J., Cohen-D'Agostino, M., and Brown, A. (2020). Sharing Mobility Data for Planning and Policy Research. https://escholarship.org/uc/item/88p873g4.

LADOT established its own pilot program for shared-mobility providers that includes specific data-sharing requirements. The pilot program requires that companies transmit data on the start point and end point of each trip within five seconds of the event, and the full route of each ride within one day. One micromobility provider, JUMP (owned by Uber), has resisted these requirements citing the granularity required. After failed negotiations, Uber refused to comply, "arguing, with the backing of several data privacy organizations, that the city's policy constitutes government surveillance. With minimal analysis, they say, the information could easily reveal where people live, work, socialize or worship."[15] In response, officials have contended that "the data are necessary to figure out which companies are flouting the permit program's rules, including caps on the number of vehicles and bans on riding in certain areas" and that "the companies cannot be trusted to regulate themselves."[16]

In 2019, LADOT suspended Uber's permit to operate within the jurisdiction for failing to abide by the data sharing requirements. Uber subsequently filed an administrative appeal. A decision was recently issued, upholding the suspension. In his decision, the administrative hearing officer found weak points in both sides' arguments, writing: "JUMP offered no specific case of reidentification, although the abstract concern is real. LADOT offered no specific scenario, which 'five-second' reporting prevented or solved, even while contending that such reporting, in its administrative view, is necessary to implement" its pilot program.[17] As noted, disaggregated real-time trip data may be valuable for dynamic transportation management, but comes with serious privacy concerns.

IV. Governance of TNC data by the CPUC and recent proceeding developments

Many of the impacts of TNCs, such as congestion, greenhouse gas emissions, and diminished transit ridership fall largely to local government to address. However, the wealth of information local authorities are receiving from shared micromobility providers contrasts sharply with a dearth of information about TNCs. Local authorities do not have the authority to require a TNC to provide them data directly. The CPUC regulates TNCs in California. It has implemented substantial reporting requirements on TNCs, but keeps the data collected confidential. However, on February 7, 2020, the CPUC issued a proposed decision that would alter this policy.

---

[15] Laura J. Nelson, *L.A. suspends Uber's permit to rent out electric scooters and bikes* (Nov. 4, 2019) Los Angeles Times, https://www.latimes.com/california/story/2019-11-04/los-angeles-suspends-uber-jump-scooters-bikes-data-privacy.

[16] *Ibid*.

[17] Shapiro, D. (2020). *Social Bicycles d/b/a/ JUMP vs. LADOT: Hearing Officer's Decision;* Laura J. Nelson, *L.A. wins appeal in fight with Uber over scooter and bike data* (Feb. 11, 2020) Los Angeles Times, https://www.latimes.com/california/story/2020-02-11/uber-jump-bikes-scooters-permit-ladot-data-fight-ruling.

Confidential data collected by the TNC

In 2013, the CPUC issued a decision adopting rules and regulations for TNCs.[18] These required each TNC to obtain a permit from the CPUC, required criminal background checks for each driver, established a driver training program, implemented a zero-tolerance policy on drugs and alcohol, required specified insurance coverage, and set annual reporting requirements covering, in part:

- The average number of hours and miles each TNC driver spent driving for the TNC;
- The date and time of traffic incidents;
- The date, time, and zip code of each requested ride, including whether the ride was accepted or unaccepted by the TNC driver;
- The zip code where each ride began and ended;
- The number of miles traveled in each ride; and
- The number and percentage of their customers who requested accessible vehicles and how often the TNC was able to provide an accessible vehicle.[19]

In 2018, the Legislature passed SB 1014, the California Clean Miles Standard and Incentive Program, in order to reduce greenhouse gas emissions from TNCs.[20] SB 1014 requires the CPUC, Air Resources Board (ARB), and California Energy Commission to increase the use of zero-emission vehicles by TNCs and requires ARB to establish a baseline per-passenger, per-mile greenhouse gas emission baseline for TNC vehicles. In order to meet these requirements, the CPUC has requested additional data from TNCs including, but not limited to:

- The date, time, and latitude and longitude of each trip start;
- The date, time, and latitude and longitude of each trip end;
- The miles traveled during the trip;
- For plug-in hybrid electric vehicles only, miles traveled that were fully powered by electricity; and
- Average vehicle speed.

When the CPUC was first developing TNC regulations, TNCs argued that the annual reports should be kept confidential to protect sensitive information and to avoid placing compliant TNCs at a competitive disadvantage. For these reasons, the CPUC allowed all TNC reports to be filed confidentially.

Reexamination of data confidentiality

In light of the "heightened interest that government entities have expressed in obtaining

[18] CPUC. (2013). *Decision 13-09-045, Decision Adopting Rules and Regulations to Protect Public Safety While Allowing New Entrants to the Transportation Industry.* Proceeding R1212011.
[19] *Ibid.*
[20] SB 1014 (Skinner, Chapter 369, Statutes of 2018)

and analyzing TNC trip data in order to gauge the TNC vehicles' environmental, traffic, and infrastructural impacts on the cities and counties in California,"[21] the CPUC began reexamining its confidentiality policy in 2017. The CPUC asked stakeholder parties to articulate the value of this data to research and government entities, and to weigh in on the ability of a CPUC-sponsored website to protect customer privacy and market-sensitive data.

On February 7, 2020, the CPUC issued a proposed ruling reversing its policy of keeping TNC annual reports confidential, laying out a number of factors for its decision, including: the public's right to information; the lack of viable competition in the TNC industry; the CPUC's adoption of stricter standards for establishing a claim of confidentiality; and heightened public interest in obtaining access to unredacted annual reports.[22]

Under the proposed ruling future annual reports would no longer be confidential by default. The burden shifts to the TNC to make the case that any information in an annual report must remain confidential. Parties will now have 30 days to respond to the decision.

Beyond confidentiality, the CPUC considered increasing the frequency of TNC reporting requirements and considered how data may be made available online or to governmental entities. These may be the subjects of future action. The CPUC is also carrying out a rulemaking process related to automated vehicle data reporting.

Publicly-available TNC data sets

TNCs have made some data available on a voluntary basis. For instance, Uber states that it provides deidentified and aggregated data on average travel times and speeds between locations through the Uber Movement website.[23] There are also examples of collaborative data sharing, notably, between Ford Motor Company, Uber, Lyft, the non-profit data platform SharedStreets, and participating cities to characterize curb-side pick-ups and drop-offs. This information could help cities determine where to place designated TNC loading zones while providing some privacy protections to the data.[24]

V. California Privacy Law

California Electronic Communications Privacy Act (CalECPA)

In 2015, the Legislature enacted the California Electronic Communications Privacy Act (CalECPA) to protect Californians from intrusive government searches in the digital

[21] CPUC. (2017). *Amended Phase III. B. Scoping Memo and Ruling of Assigned Commissioner.* Proceeding R1212011.
[22] CPUC. (2020). *Decision of Data Confidentiality Issues Track 3.* Proceeding R1212011.
[23] Uber Movement. https://movement.uber.com/?lang=en-US.
[24] NACTO. (2018), *Ford Motor Co., Uber and Lyft Announce Agreement to Share Data Through New Platform that Gives Cities and Mobility Companies New Tools to Manage Congestion, Cut Greenhouse Gases and Reduce Crashes*. https://nacto.org/2018/09/26/ford-uber-lyft-share-data-through-sharedstreets-platform/.

era.[25] Senator Mark Leno, the author of the bill, argued that clear protections for electronic communications and electronic devices needed to be codified in the face of mounting requests from law enforcement for information, including location data, from social media companies, technology companies, and telecommunications companies.[26]

CalECPA provides that a government entity shall not:

- Compel the production of or access to electronic communication information from a service provider;
- Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device; or
- Access electronic device information by means of physical interaction or electronic communication with the electronic device.

(Pen. Code § 1546.1.) CalECPA provides an exclusive list of exceptions to these prohibitions, including the issuance of a valid warrant or wiretap order.

CalECPA's applicability to shared-mobility data sharing requirements has been the source of some controversy and divergence of opinion. For instance, some government entities, including LADOT, argue that "CalECPA is limited to law enforcement access to electronic information in the course of criminal investigations" and therefore does not apply to data-sharing requirements imposed by, for example, local transportation departments.[27]

On August 1, 2019, the Office of Legislative Counsel issued a written opinion regarding the matter. The primary question presented to it was as follows:

> [W]hether the CalECPA restricts a department of a city or county from requiring a business that rents dockless bikes, scooters, or other shared mobility devices to the public . . . to provide the department with real-time location data from its dockless shared mobility devices . . . as a condition of granting a permit to operate in the department's jurisdiction."

Legislative Counsel first made a series of findings: (1) a department of a city or county is a "government entity" for the purposes of CalECPA; (2) a dockless shared mobility device is an "electronic device" for the purposes of CalECPA and therefore information regarding the current and prior locations of a dockless shared mobility device is "electronic device information"; (3) a dockless mobility provider is a person or entity other than the "authorized possessor" of the device during the period of the rental (the consumer is essentially the "authorized possessor" during that period); and (4) "a

[25] SB 178 (Leno, Chapter 651, Statutes of 2015), Pen. Code § 1546 et seq.
[26] Assembly Privacy and Consumer Protection Committee (2015) *Committee Analysis,* http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178.
[27] LADOT. (2019). *City of Los Angeles Inter-Departmental Memorandum: State Office of Legislative Counsel Opinion on the California Electronic Communications Privacy Act,* https://cdn.theatlantic.com/assets/media/files/17-1125-s8_rpt_dot_08-15-2019.pdf.

permitting system that imposes a real-time data-sharing requirement" constitutes the "[c]ompel[ling of] the production of or access to" electronic device information.

Legislative Counsel's legal opinion therefore concludes that "CalECPA restricts a department . . . from requiring a business that rents . . . shared mobility devices to the public to provide the department with real-time location data from its dockless shared mobility devices as a condition of granting a permit to operate in the department's jurisdiction."

California Consumer Privacy Act (CCPA)

The CCPA, enacted in 2018, creates new consumer privacy rights relating to access to, deletion of, and selling of personal information collected by businesses. These include a limited right to delete personal information held by a business and the right to opt out of the sale of the consumer's personal information. The CCPA does not apply directly to government entities. The CCPA makes clear that the obligations it imposes on businesses do not restrict a business' ability to comply with federal, state, or local laws. Consumers whose nonencrypted and nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure, as specified, are provided a limited enforcement mechanism to recover damages, injunctive or declaratory relief, and other relief deemed proper by the court.

VI. Perspectives on Privacy and Data Management Practices

Thoughtfully-crafted limitations and safeguards can mitigate the risks associated with sharing and use of shared-mobility data. Such guardrails must ensure the privacy or safety of consumers is protected, especially when that data can reveal potentially recognizable travel patterns or can be combined with other information to reveal personal identity. The probability that an individual's identity can be attributed to specific data decreases as identifying or potentially identifying information is stripped away, or as the data is more highly aggregated. For example, trip start locations averaged by zip code is more privacy-protective than trip start locations averaged by city block. However, evidence shows that even with robust deidentification, the more data points included in a data set, the easier it is to reidentify the individuals involved, especially when dealing with location information. This section extracts potential best practices from several recent reports and letters on location data management.

The National Association of City Transportation Officials' "Managing Mobility Data"[28] document sets out their perspective on "principles and best practices for city agencies and private sector partners to share, protect, and manage data to meet transportation planning and regulatory goals in a secure and appropriate manner."

[28] National Association of City Transportation Officials and International Municipal Lawyers Association. (2019). *NACTO Policy 2019: Managing Mobility Data* https://nacto.org/wp-content/uploads/2019/05/NACTO_IMLA_Managing-Mobility-Data.pdf.

Its recommendations to cities include:

- Use data sharing agreements that allow cities to own, transform, and share data without restriction (so long as standards for data protections are met);
- Treat location mobility data as they treat personally identifiable information (PII);
- Clearly outline purposes for which they are requiring shared-mobility data;
- Utilize data-sharing agreements that allow cities to own, transform, and share data without restriction (so long as standards for data protections are met);
- Set retention limits on individual trip records, and aggregate all location data before committing it to permanent storage;
- Share data publicly only in aggregate form; and
- Restrict access to sensitive data and provide specialized training for personnel handling shared-mobility data; and
- Provide sufficient oversight by employing, regulating, and enforcing IT best practices to monitor access to shared mobility data.

Recommendations have also been put forth by privacy and consumer groups, including the Electronic Frontier Foundation and Center for Democracy & Technology[29] including:

- Establish a clear mobility data management policy that explicitly states how high level privacy principles will be implemented;
- Cease collecting geolocation data on shared-mobility trips until adequate safeguards are implemented;
- Establish clear guidelines on data retention;
- Outline and limit the specific purposes for which geolocation data will be used;
- Commit to requiring a warrant before sharing location data with law enforcement;
- Implement data cybersecurity measures, including data encryption during transmission and password protection while in storage;
- Subject government entities collecting this information to the requirements of the CCPA; and
- Limit sharing with third parties, update sharing agreements and provide transparency as to their provisions, and ensure they include necessary data safeguards, such as prohibitions on commercial use.

Finally, the UC Davis Policy Institute for Energy, Environment, and the Economy has suggested establishing publicly held big-data repositories to securely hold mobility data and provide structured access to states, cities, and researchers, managed by an appropriate third party such as a university or national laboratory.[30]

[29] Electronic Frontier Foundation. (2019). *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification.* https://www.eff.org/document/eff-oti-letter-urgent-concerns-regarding-lack-privacy-protections-sensitive-personal-data; Center for Democracy & Technology. (2018) *Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility*, https://cdt.org/insights/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/;

[30] D'Agostino, M., Pellaton, P., and Brown, A. (2019). Mobility Data Sharing: Challenges and Policy Recommendations. https://escholarship.org/uc/item/4gw8g9ms

Ultimately, some expressing concerns for consumers' constitutional right to privacy believe that legislation should restrict the sharing of individual trip data and instead provide government entities, and others, with aggregated and deidentified trip data. However, some government entities contend this would hamper their planning efforts and ability to manage transportation in the digital age.

VII. Recent Legislation

AB 1112 (Friedman, 2019) deals with shared-mobility devices and limits the data a local authority may require a shared-mobility device provider to provide the local authority as a condition of operating in its jurisdiction. Specifically, AB 1112 would permit a local authority to require (1) data related to the general status of shared-mobility fleets (e.g. number of devices deployed and location of devices not engaged by a user), and (2) trip data that is deidentified and aggregated. It would prohibit a local authority from requiring disaggregated "individual trip data" including location, time stamp, or route data that are not deidentified and aggregated. Finally, AB 1112 clarifies that CalECPA applies to individual trip data. This bill also provides that a local authority may enact reasonable regulations on shared mobility devices and providers within its jurisdiction. AB 1112 is a two-year bill and is currently in the Senate Transportation Committee.

AB 1142 (Friedman, 2019) deals with TNC data and would have required the CPUC to reflect certain government entities' need for data in carrying out their responsibilities to (1) analyze and plan for the impacts of TNCs on local, regional, and state transportation systems and networks and make informed decisions regarding infrastructure investment, (2) prepare SB 375 sustainable communities strategies and meet the goals of those strategies, and (3) comply with federal air quality conforming mandates in a manner that effectively reflects the role of TNCs. It required that the CPUC provide only deidentified and aggregated data. However, in order to ensure the data would address the specified needs, this bill also limited how highly the data could be aggregated. For example, trip start and end locations would not be aggregated beyond the ZIP Code or census block level. This bill also authorized larger metropolitan planning organizations to include TNC data in their regional transportation plan policy element. AB 1142 was held on suspense in the Senate Appropriations Committee.

VIII. Policy Considerations

In the course of the hearing and as legislation on shared-mobility data is considered by the Legislature, the Committees may wish to consider the following questions:

- What responsibilities do local governments have in overseeing the transportation system, and what data is necessary to support carrying out that responsibility?
- What limits should be placed on the types of shared-mobility data government entities may require providers to share as a condition of operating in their jurisdictions?

- What required safeguards should be put in place for shared-mobility data that is transferred from providers to government entities?
- What TNC data should be made publicly available or available to government entities and under what conditions?
- What entities should have the ability to collect and store sensitive shared-mobility location data?
- What policies should entities storing sensitive shared-mobility location data put in place to ensure the data is managed securely?