SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

SB 1276 (Durazo)
Version: April 18, 2022
Hearing Date: April 26, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Shared mobility service data

DIGEST

This bill authorizes government entities to require shared mobility service providers to provide service data, as specified.

EXECUTIVE SUMMARY

Transportation network companies (TNCs) such as Lyft and Uber have become ubiquitous. Statistics reveal that from virtually no service in 2012, just one company, Uber, completed over 1 billion trips in the last quarter of 2020, in the midst of a global pandemic. Numerous cities in California have also witnessed the boom in shared bikes, scooters, and other transportation devices over recent years. In 2019, Americans took approximately 136 million trips on shared bikes, e-bikes, and scooters. These "shared mobility devices" have been welcomed in some areas and shunned in others. Various legal and policy questions arise around whether and how these devices and the companies providing them should be regulated.

One issue at the center of this debate is the sharing of shared mobility device information. The information is useful for greater understanding of the impacts of these near ubiquitous modes of transportation and to some extent necessary for effective regulation. However, looming behind this data collection and sharing are privacy concerns. The utility of sharing such information must be balanced against the very real concerns regarding the privacy of users, especially given the sensitivity of location data and the possibility that shared mobility information can be connected back to individual persons.

This bill authorizes government entities to require shared mobility service providers over which they have jurisdiction to provide shared mobility service data in a form that facilitates auditing. The bill places a number of obligations on these regulating agencies

in connection with this sharing, including the provision of proper notice to providers and privacy safeguards. The bill includes a number of restrictions on further disclosure of the device information.

The bill is sponsored by the California Labor Federation, United Food and Commercial Workers, and the City of Los Angeles. It is supported by a variety of groups. It is opposed by business and privacy groups, including TechNet and the Electronic Frontier Foundation.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides that a county or city may make and enforce within its limits all local, police, sanitary, and other ordinances and regulations not in conflict with general laws. (Cal. Const. art. XI, § 7.)

2) Requires any business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code § 1798.81.5.)

3) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information, as defined, from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, consent of the owner of the device, or emergency situations, as specified. (Pen. Code § 1546 et seq.)

4) Requires a shared mobility service provider, before distribution of a shared mobility device, to enter into an agreement with, or obtain a permit from, the city or county with jurisdiction over the area of use. The agreement or permit shall, at a minimum, require that the shared mobility service provider maintain commercial general liability insurance coverage with a carrier doing business in California with specified minimums that do not exclude coverage for injuries or damages caused by the shared mobility service provider to the shared mobility device user. (Civ. Code § 2505.)

5) Requires cities and counties that authorize providers to operate within their jurisdiction to adopt rules for the operation, parking, and maintenance of shared mobility devices by ordinance, agreement, or permit terms, as specified. Providers are required to comply therewith. (Civ. Code § 2505(c).)

6) Defines "shared mobility device" to mean an electrically motorized board, motorized scooter, electric bicycle, bicycle, as those terms are defined, or other similar personal transportation device that is made available to the public by a shared mobility service provider for shared use and transportation in exchange for financial compensation via a digital application or other electronic or digital platform. (Civ. Code § 2505(a)(1).)

7) Defines "shared mobility service provider" as a person or entity that offers, makes available, or provides a shared mobility device in exchange for financial compensation or membership via a digital application or other electronic or digital platform.

8) Provides that nothing in the above provisions shall prohibit a city or county from adopting any ordinance or regulation that is not inconsistent with this title. (Civ. Code § 2505(d).)

9) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

10) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

11) Authorizes the California Public Utilities Commission (PUC) to supervise and regulate every charter-party carrier (CPC) of passengers. (Pub. Util. Code § 5381.)

12) Defines a CPC of passengers as every person engaged in the transportation of persons by motor vehicle for compensation over any public highway in this state. A CPC of passengers includes any person, corporation, or other entity engaged in the provision of a hired driver service when a rented motor vehicle is being operated by a hired driver. (Pub. Util. Code § 5360.)

13) Defines a TNC as an organization, including, but not limited to, a corporation, limited liability company, partnership, sole proprietor, or any other entity,

operating in California that provides prearranged transportation services for compensation using an online-enabled application or platform to connect passengers with drivers using a personal vehicle. (Pub. Util. Code § 5431.)

14) Prohibits a TNC from disclosing to a third party any personally identifiable information of a TNC passenger unless one of the following applies:
    a) the customer knowingly consents;
    b) pursuant to a legal obligation; or
    c) the disclosure is to the commission in order to investigate a complaint filed with the commission against a TNC or a participating driver and the commission treats the information under confidentiality protections. (Pub. Util. Code § 5437.)

15) Establishes the California Clean Miles Standard and Incentive Program at the Air Resources Board (ARB) and the PUC to establish targets for the reduction of greenhouse gas (GHG) emissions resulting from TNC rides. The PUC must implement the targets adopted by the ARB. To support ARB's calculations of baseline TNC emissions and targets, TNCs must report at least the following data:
    a) total miles completed by drivers;
    b) percent of miles completed by qualified zero emissions transportation methods, including vehicle, walking, biking, and other modes of active transportation;
    c) miles-weighted average network-wide grams of carbon dioxide per mile to produce an estimate of the GHG emissions; and
    d) total passenger miles completed using an average passengers-per-trip estimate to account of trips where TNC does not record the exact number of passengers. (Pub. Util. Code § 5450.)

16) Requires each local transportation planning agency to adopt a regional transportation plan aimed at coordinating and balancing transportation across multiple different transportation modes. The regional transportation plan must include a policy element that describes regional transportation issues. For a transportation planning agency serving a population that exceeds 200,000 persons, the policy element of the plan may quantify a set of indicators related to specific transportation issues, including, but not limited to methods of travel and the percentage share of all trips made by specific modes of transportation. (Gov. Code § 65080.)

This bill:

1) Authorizes a regulating agency, as a term of a regulation, license, permit, or other authorization, to require a shared mobility service provider over which it

has jurisdiction to provide to the regulating agency shared mobility service data in a form that facilitates auditing. It states that this is declaratory of existing law.

2) Defines a "regulating agency" as a state, county, regional, or local government agency that issues a license, permit, or other authorization to a shared mobility service provider to operate within the governmental agency's jurisdiction or that otherwise regulates the provider.

3) Defines a "shared mobility service provider" as a person or entity that offers, provides, or makes available to the public a shared mobility service, including, a TNC and a food delivery platform, as defined. A "shared mobility service" is a service that uses an online enabled application or platform to display, offer, or make available in the public right-of-way for rent or use a shared mobility device or to provide for ordering and delivery of goods using a shared mobility device. A "shared mobility device" is a motor vehicle, bicycle, electric bicycle, electric scooter, or other device or vehicle offered for use on a platform by which a person or goods can be propelled, moved, or drawn in the public right-of-way.

4) Defines "shared mobility service data" to mean any of the following:
    a) information documenting the location, characteristics, event, or operational status or change in status of a shared mobility device or service, including locked, unlocked, accessible to people with disabilities, available for use, unavailable for use, internal combustion engine, zero-emission vehicle, and other similar characteristics or operational status;
    b) information about trips requested or completed using a shared mobility device or service, including start and end time, duration, point of origin, route, and point of conclusion; or
    c) notifications of such information provided to a regulating agency by a shared mobility service provider.

5) Permits the regulating agency to prescribe use of a particular data specification to govern submissions and may specify the time and frequency for reporting, including, if necessary to support a public purpose, requiring the submission of contemporaneous notifications about the location and operational status of shared mobility devices and services. The agency must provide the shared mobility service provider reasonable notice of the data specification and reporting requirements.

6) Requires a regulating agency imposing such requirements to protect the privacy of users by implementing all of the following policies and procedures:
    a) limiting access to shared mobility service data to employees, contractors, or agents who have an operational or regulatory need to access the data;
    b) prohibiting employees, contractors, or agents of the regulating agency from making private use of the data;

c) employing technical safeguards that prevent unauthorized access to, or inadvertent release of, shared mobility service data;
d) adopting data minimization and retention schedules under which shared mobility service data is retained only for so long as it is needed to support a public purpose; and
e) prohibiting an employee, contractor, or agent who has access to the shared mobility service data from using or disclosing the data for a commercial purpose and terminating a contractor or agent's access to shared mobility service data upon completion of work required by a contract.

7) Defines "deidentified shared mobility service data" as data that does not include personal information, as defined, about a driver or user. It prohibits a regulating agency from disclosing deidentified data to another public agency unless all of the following are true:
   a) the disclosure is pursuant to an agreement through which the receiving public agency agrees that it will comply with specified data security requirements;
   b) the regulating agency discloses the deidentified data at least 24 hours after the latest event or status notification included in the shared mobility data; and
   c) the purpose of the disclosure is to assist the recipient public agency with any of the following:
      i. regulation of the public right-of-way to protect public health, safety, or welfare;
      ii. transportation planning;
      iii. the design, maintenance, and operation of multimodal transportation infrastructure and services; or
      iv. any other public purpose, including an audit of a regulating agency or a shared mobility service provider.

8) Prohibits a regulating agency or recipient public agency from disclosing shared mobility service data with a local, state, or federal law enforcement agency other than as required by law pursuant to a specified warrant or through a court order, subpoena, or other legal process.

9) Prohibits, notwithstanding any other law, a regulating agency or public agency from disclosing shared mobility service data that includes location data to the public unless all of the following criteria are met:
   a) at least 24 hours have passed since the latest event or status notification included in the deidentified shared mobility service data;
   b) any location field has been redacted or the precision of data in a location field has been reduced by using any of the following methods of aggregation, obfuscation, or anonymization:

i. aggregation of records sharing a common geography, time of day, or date range to generate a sum, average, minimum, maximum, or other summary value;
ii. replacing precise latitude and longitude data with census blocks or other common geography; or
iii. using any other method reflected in an adopted industry standard or used, endorsed, or recommended by the United States Census Bureau or the National Institute of Standards and Technology; and

c) the location data does not depict a shared mobility device or service currently in use by a user.

10) Provides that it does not prohibit a public agency from disclosing to the public contemporaneous data that identifies the location of shared mobility devices or services that are currently available for public use to facilitate multimodal user access, trip planning, or trip payment.

11) Provides that it does not affect the authority of the PUC to disclose information received from PUC permittees to the public, as provided.

12) Excludes shared mobility service data from the definitions of electronic device information or electronic information in CalECPA. It states that this is declaratory of existing law.

COMMENTS

1. Shared mobility data sharing: benefits and privacy concerns

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 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. Despite the global pandemic, the usage of shared mobility services is now in the billions.

---

[1] Susan Shaheen & Adam Cohen, *Shared Micromobility Policy Toolkit: Docked and Dockless Bike and Scooter Sharing* (April 2019) UC Berkeley: Transportation Sustainability Research Center, https://escholarship.org/uc/item/00k897b5. All internet citations are current as of April 18, 2022.
[2] CPUC, *Summary of Transportation Network Companies' Annual Reports 2014 and 2015 submissions.*
[3] *Shared Micromobility in the U.S.:2018,* National Association of City Transportation Officials, https://nacto.org/wp-content/uploads/2019/04/NACTO_Shared-Micromobility-in-2018_Web.pdf.

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 relevant data is generated through the networked nature of these services themselves, including device location data. In order to regulate TNCs, the PUC requires them to provide disaggregated data on each trip in California. For their part, cities are collecting aggregated and/or disaggregated data from shared mobility 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 enables 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.

In the wake of the deployment of dockless, shared electric scooters in 2018, many local authorities, including the Los Angeles Department of Transportation (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 included 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;[4] 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.[5]

There are various categories of information local authorities 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

[4] *Powered Scooter Share Program* (2019) San Francisco Municipal Transportation Agency, https://www.sfmta.com/sites/default/files/reports-and-documents/2019/12/1._scoot_permit_and_terms_2019.pdf.
[5] *Frequently Asked Questions,* LADOT, https://ladot.lacity.org/about/faq.

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 mobility trips may be connecting with transit; and inform management of congestion and traffic flow. This information can include trip start and end times and 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.

Local authorities generally require shared mobility providers to post data to the local authority via two main data specifications. Broadly, the General Bike Feed Specification offers real-time locations of available devices. The other main data specification cities use to ingest shared micromobility data is the Mobility Data Specification (MDS). MDS can capture granular data, such as in-trip data, which may be shared in real-time or after the fact. MDS could be used or expanded for use with other forms of transportation, including carshare, TNCs, and autonomous vehicles. Some transportation experts predict that the trends of shared mobility, automation, and electrification will eventually dominate mobility.[6]

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."

[6] Daniel Sperling, *Three Revolutions: Steering Automated, Shared, and Electric Vehicles to a Better Future* (March 2018) Island Press.

This vision is largely driven across the country by the Open Mobility Foundation (OMF):

> [T]he Open Mobility Foundation describes itself as a "public-private forum" to help local governments gain control of their roads from private mobility companies, using big data and open-source code. A central part of OMF's mission is to govern the new mobility data standard, commonly known as MDS, unveiled by the Los Angeles department of transportation last year. Currently, MDS pulls in rich, real-time status information about dockless scooters and shared bikes. Many other cities, including Miami, Seattle, Portland, San Francisco, Austin, Minneapolis, and others that have joined OMF, have adopted it. . . . Having a virtual replica of real-world mobility flows—for scooters and bikes now, and for ride-hailing cars, AVs, and drones in the future—would allow local governments to both trace the movements of individual vehicles, and control them to some extent.[7]

One of OMF's core principles states: "As with the physical public realm, municipalities hold in the public trust and manage the digital public realm, which represents the real-time and historic state of vehicles, assets and other devices operating within the right-of-way that is managed by the city for the public good."[8] 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.[9] 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.

---

[7] Laura Bliss, *Why Real-Time Traffic Control Has Mobility Experts Spooked* (July 19, 2019) Bloomberg, https://www.bloomberg.com/news/articles/2019-07-19/why-cities-want-digital-twins-to-manage-traffic.

[8] *Bylaws* (February 2020) Open Mobility Foundation, https://www.openmobilityfoundation.org/wp-content/uploads/2020/02/OMF-Bylaws-CURRENT.pdf.

[9] Letter to Councilmember Mike Bonin, *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification* (April 3, 2019) Electronic Frontier Foundation, https://www.eff.org/document/eff-oti-letter-urgent-concerns-regarding-lack-privacy-protections-sensitive-personal-data; *Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility* (November 29, 2018) Center for Democracy & Technology, https://cdt.org/insights/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/.

2. Legislative attempts to find the right balance on data sharing

Summarizing the landscape, there are a few core issues at the center of this policy debate. This bill is only the most recent legislative attempt at finding the right balance on those issues.

a. The granularity of data

The first issue is how raw the data that is provided should be. Obviously the more granular the data the more informative it is. However, this granularity comes with privacy concerns that are exacerbated when the data collected can be connected back to individual consumers. 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.'"[10] 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."[11] Federal agencies have even "bought access to a commercial database that maps the movements of millions of cellphones in America" and has used it "for immigration and border enforcement."[12]

Researchers at the University of California Institute of Transportation Studies reported on the need and utility for various shared mobility data. Specific to this balance they found:

> Specific data needs will differ by application and geographic scale of interest. For example, state planning entities and regional planners can likely conduct most long-range planning activities with annual and aggregated data. However, city and state-level regulatory authorities could benefit from more granular route and path data for planning and policy to respond to emerging trends and challenges.[13]

Privacy advocates have called for legislation restricting the sharing and use of more granular trip data. They have urged that sharing should be limited to aggregated and

---

[10] *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.
[11] Yves-Alexandre de Montjoye, et al, *Unique in the Crowd: The privacy bounds of human mobility* (2013) Scientific Reports 3, Article Number 1376, https://www.nature.com/articles/srep01376.
[12] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement* (February 7, 2020) Wall Street Journal, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=hp_lead_pos5.
[13] Juan Matute, J., et al, *Sharing Mobility Data for Planning and Policy Research* (February 2020) University of California Institute of Transportation Studies, https://escholarship.org/uc/item/88p873g4.

deidentified data, which they argue can provide important insights into how Californians are using TNCs and shared mobility devices for their transportation needs. They argue that 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.

b. The California Electronic Communications Privacy Act (CalECPA)

Another major legal issue laying at the core of these policy debates is the application of the California Electronic Communications Privacy Act (CalECPA). In 2015, the Legislature enacted CalECPA to protect Californians from intrusive government searches in the digital era.[14] Senator Mark Leno, the author of the bill, argued that "clear warrant standards for government access to electronic information" needed to be instituted in order "to properly safeguard the robust constitutional privacy and free speech rights of Californians." He stated the case:

> SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian's personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more. The California Supreme Court has long held that this type of information constitutes a "virtual current biography" that merits constitutional protection. SB 178 would codify that protection into statute.[15]

CalECPA prohibits a government entity from the following:

- compelling the production of or access to electronic communication information from a service provider;
- compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device; or
- accessing 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. A government

[14] SB 178 (Leno, Ch. 651, Stats. 2015), Pen. Code § 1546 et seq.
[15] Senate Public Safety Committee (2015) *Committee Analysis of SB 178*.

entity may access electronic device information by means of physical interaction or electronic communication with the device under certain circumstances, including with the specific consent of the authorized possessor of the device or the owner of the device, when the device has been reported as lost or stolen. It can also be accessed if the entity has a good faith belief that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

The act defines "electronic device information" as any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device. "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof. "Specific consent" is defined as consent provided directly to the government entity seeking information.

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, have argued 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.[16]

On August 1, 2019, the Office of Legislative Counsel issued a written opinion regarding the matter.[17] The primary questions presented to it were as follows:

(1) "[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."
(2) "[W]hether, in order to constitute specific consent for purposes of the CalECPA, it is necessary for an individual to provide consent directly to a government entity seeking that individual's data."

Legislative Counsel first made a series of findings:

(1) a department of a city is a "government entity" for the purposes of CalECPA;
(2) a dockless shared mobility device is an "electronic device" and information regarding the current and prior locations of a dockless shared mobility device is "electronic device information" for the purposes of CalECPA;

---

[16] Seleta Reynolds, *City of Los Angeles Inter-Departmental Memorandum: State Office of Legislative Counsel Opinion on the California Electronic Communications Privacy Act* (August 15, 2019) LADOT, https://cdn.theatlantic.com/assets/media/files/17-1125-s8_rpt_dot_08-15-2019.pdf.
[17] Diane F. Boyer-Vine & Mariko M. Kotani, *California Electronic Communications Privacy Act - #1916004* (August 1, 2019) Legislative Counsel Bureau.

(3) a dockless mobility provider is a person or entity other than the "authorized possessor" of the device during the period of the rental;
(4) "a 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 and is restricted by CalECPA prohibition; and
(5) "an individual must provide consent directly to the government entity seeking that individual's data in order to constitute 'specific consent' within the meaning of CalECPA."

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."

The applicability of the law to shared mobility device data was recently thrust into the courts.

In response to the sudden arrival of electric scooters, LADOT established a program for shared-mobility providers that includes specific data-sharing requirements and the use of MDS. According to the LADOT website:

> [T]he Mobility Data Specification (MDS) gives cities an elegant and cost effective tool to actively manage private mobility providers and the public right-of-way. MDS allows cities to collect valuable insights through a shared data vocabulary and to communicate directly with product companies in real time using code. Today, it enables cities to manage dockless scooters, bikes, taxis, and buses. Tomorrow, that could be autonomous cars, drones, and whatever else the future may hold.
>
> . . . In Los Angeles, permitted shared use mobility providers (like scooters and bikes) must provide real-time information about how many of their vehicles are in use at any given time, where vehicles are at all times, and the physical condition that vehicles are in. Additional information includes:
> - parking verification
> - operating cost
> - customer cost
> - vehicle utilization
> - percent battery charge
> - start trip data
> - end trip data[18]

[18] *Mobility Data Specification* (October 31, 2018) LADOT, https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf.

On June 8, 2020, Justin Sanchez and Eric Alejo, represented by the ACLU and the Electronic Frontier Foundation, sued the city, claiming that MDS violated their rights under the Fourth Amendment of the United States Constitution, the California Constitution, and CalECPA.[19] The United States District Court granted LADOT's motion to dismiss all claims. Relevant here, the court found that the provision of CalECPA that allows an individual to bring a cause of action to enforce CalECPA did not provide these plaintiffs standing in the particular instance before the court:

> Plaintiffs purport to sue under Section 1546.4(c), which provides:
>
> > An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter . . . may petition *the issuing court* to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter . . . [emphasis added].
>
> This Court is not the "issuing court" of any warrant, order, or process by which the City collects the MDS data. Section 1546.4(c) gives standing to a person whose information has been targeted pursuant to a court order, warrant, or process to challenge that order, warrant, or process before that same court *in the same proceeding*. It does not allow the person to initiate an entirely new civil action before another, unrelated tribunal.
>
> By contrast, Section 1546.4(b) allows the Attorney General to "commence a civil action to compel any government entity to comply with the provisions of this chapter" (emphasis added).[20]

Therefore, the claim was dismissed for lack of standing rather than on a finding that the permitting system did not constitute a violation of CalECPA. The case is currently pending on appeal in the United States Court of Appeals for the Ninth Circuit.

c. Previous legislative attempts to strike the balance

One of the first attempts at directly addressing the sharing of data from shared mobility devices was AB 1112 (Friedman, 2019). Although later amended out of the bill before dying in the Senate Transportation Committee, it originally sought to limit 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 have permitted 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

---

[19] *Sanchez v. L.A. DOT* (C.D.Cal. Feb. 23, 2021) No. CV 20-5044-DMG (AFMx), 2021 U.S. Dist. LEXIS 34711, at *1.
[20] *Id.* at *14-15.

engaged by a user), and (2) trip data that is deidentified and aggregated. "Deidentified data" was defined to mean data that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular user, provided that an entity that uses deidentified data meets all of the following criteria:

> (1) Has implemented technical safeguards that prohibit reidentification of the user to whom the data may pertain.
> (2) Has implemented business and security processes that specifically prohibit reidentification of the data.
> (3) Has implemented business and security processes to prevent inadvertent release of deidentified data.
> (4) Makes no attempt to reidentify the information.

The bill would have prohibited a local authority from requiring disaggregated "individual trip data" including location, time stamp, or route data that are not deidentified and aggregated. It died in the Senate Transportation Committee.

AB 1142 (Friedman, 2019) dealt with TNC data and would have required the CPUC to reflect certain government entities' need for data in carrying out their specified responsibilities, including their obligation to analyze and plan for the impacts of TNCs on local, regional, and state transportation systems and networks and make informed decisions regarding infrastructure investment. It required that the CPUC provide only deidentified and aggregated data. However, in order to ensure the data would address the specified needs, AB 1142 would have 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.

AB 859 (Irwin, 2021) would have authorized a public agency to require shared mobility operators to periodically submit to the public agency anonymized trip data, defined as aggregated and deidentified data pertaining to a user's trip. The bill would have deemed trip data as personal information for purposes of the California Consumer Privacy Act (CCPA) and would have provide that a public agency is prohibited from obtaining trip data except as provided in CalECPA. This bill died in the Assembly Appropriations Committee. AB 3116 (Irwin, 2020) was identical to AB 859 and was held on the Assembly Appropriation committee's suspense file.

Thoughtful policy-making is required to find the proper balance between data access and respecting the fundamental right to privacy. To effectuate this, regulation in this area must ensure that any data sharing laws and regulations make sufficient data available without placing personal information at risk. At the very least, experts urge that this must involve various levels of aggregation, deidentification, encryption standards, data minimization principles, and standards and protocols for transmission,

use, sharing, and retention. Appropriate guardrails must be in place. This is especially true when dealing with more granular trip data that could reveal Californians' every movement on these increasingly relied upon modes of transportation.

3. Enabling regulating agencies to require data and restricting further disclosure

The author states the intent of the bill:

> A growing number of digitally operated mobility devices have proliferated across California, saturating city streets and when left unregulated, endangering the public right of way. For regulatory agencies to support innovation and meet their obligations to protect critical policy goals like public safety, accessibility, sustainability and equity, they need accurate and timely information about the use and disbursement of mobility devices. SB 1276 affirms a regulatory agency's ability to require data from permitted companies in order to fulfill its responsibility to protect the public right of way. By codifying best practices on how agencies collect this data, we will ensure there are stringent individual privacy protections in place that expressly prohibit the ability of law enforcement entities to access this data absent a robust legal process.

The bill explicitly authorizes regulating agencies to mandate shared mobility service providers operating within their jurisdiction to provide shared mobility service data in a form that facilitates auditing. Shared mobility service providers are individuals or entities that offer, provide, or make available to the public shared mobility services. The definitions are broad and include not only data relating to shared bikes and scooters, but also TNCs and food delivery platforms. "Shared mobility service data" includes location data and information documenting characteristics, availability, and operational status. The data that can be required also includes information about trips requested or completed, including start and end time, duration, point of origin, route, and point of conclusion.

The bill defines "shared mobility service provider" to mean a person, corporation, partnership, association, joint venture, or other private entity that offers, provides, or makes available to the public a shared mobility service, including, but not limited to, a transportation network company and a food delivery platform, as those terms are defined. However, it specifically exempts a public agency or its contractors or agents acting on behalf of the public agency from this definition, and by extension, from the data sharing requirements of the bill. Arguably, if a government agency meets the definition of a provider, it should be held to the same regulatory oversight and potential data sharing requirements as any other provider. For instance, if LADOT contracted with a company to provide TNC services, any regulating agency should be able to similarly seek data in order to provide the same level of oversight as other companies are subjected to. The author may wish to remove this exemption.

After providing reasonable notice, a regulating agency can also dictate a particular data specification, such as MDS, and specify the time and frequency for reporting. This can include *contemporaneous* notifications about the location and operational status of shared mobility devices and services if necessary to support a public purpose. However, what constitutes a public purpose is not defined in the bill.

To take advantage of the imposition of these data reporting requirements, an agency must implement certain policies and procedures to protect users' fundamental right to privacy. Agencies must limit access to shared mobility service data to employees, contractors, or agents who have an operational or regulatory need to access the data. These individuals must be prohibited from making private use of the data and from using or disclosing it for a commercial purpose. Technical safeguards that prevent unauthorized access to, or inadvertent release of, shared mobility service data must also be implemented. Agencies must also adopt data minimization and retention schedules under which shared mobility service data is retained only for so long as it is needed to support a *public purpose*. Again, what is sufficient grounds to be deemed a public purpose is not laid out.

To make clear that no disclosure or other use of this data is authorized, except as specifically provided in the bill, including disclosure by the regulating agency itself, the author has agreed to amend the bill to state:

> Amendment
>
> Amend Section 1798.78.2 as follows:
>
> (E) Prohibiting a regulating agency, an employee of the regulating agency, a contractor, or an agent who has access to the shared mobility service data from using or disclosing the data for a commercial purpose and terminating a contractor or agent's access to shared mobility service data upon completion of work required by a contract.
>
> (c) A regulating agency, an employee of the regulating agency, a contractor, or an agent who has access to the shared mobility service data, shall not disclose shared mobility service data except as provided by sections 1798.78.3 and 1798.78.4.

The bill also lays out guidelines for when shared mobility data can be shared with other public agencies and the public. The bill requires any data that is disclosed externally must be deidentified. "Deidentified shared mobility service data" is data that does not include personal information, as defined in the Information Practices Act, about a driver or user.

The definition of personal information here is extremely narrow and fails to recognize the sensitivity of information outside of name, social security number, address, and the like. The author may wish to consider relying on the definitions of personal information and "deidentified" in the CCPA/California Privacy Rights Act instead. The City of Los Angeles, a sponsor of the bill, states that "none of the data required by these programs is personal." Therefore, a switch to these definitions should not impact the utility to other public agencies and the public. Given that the regulating agencies are not even limited to deidentified data, and can require providers to disclose personal information under the bill, the change to the definition of "deidentified shared mobility service data" does not impact them directly at all and therefore would not hinder their ability to regulate these providers.

On this point, the Electronic Frontier Foundation highlights concerns:

> The bill describes deidentified data as information that is stripped of identifiers, using the definition from the state Information Practices Act, which defines the term as: "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history."3 This is simply not enough to guarantee that information—particularly information companies may be required to collect under the Mobile Data Specification developed by the City of Los Angeles4—is anonymous. Location data can easily, for example, reveal a person's home address without having recorded it as such. A system that logs where an individual may return to each night around the same time would sufficiently provide this information. The MDS system is designed to collect granular location data.

The author has agreed to remove one part of a finding and declaration that is arguably not supported by existing practices:

> Amendment
>
> (f) ~~In contrast, public agencies are able to fulfill most responsibilities related to shared mobility providers without any of the personal information maintained by shared mobility service providers. Rather, most data generated by shared mobility services is deidentified and does not contain personal information related to drivers or users.~~ Deidentified data documenting the status and availability for hire of devices or vehicles and supporting user trip planning is essential to the development of multimodal transportation services, equity analysis, and the development of innovative programs and services to support decarbonization of the transportation sector.

The bill does allow for the sharing of deidentified data to another public agency if a series of criteria are met. First, the disclosure must be pursuant to an agreement through which the receiving public agency agrees that it will comply with the same data security requirements imposed on the original regulating agency. Second, the regulating agency must wait at least 24 hours after the latest event or status notification included in the deidentified shared mobility data before disclosing it. Finally, the purpose of the disclosure must be to assist the recipient public agency with any of the following:

- regulation of the public right-of-way to protect public health, safety, or welfare;
- transportation planning;
- the design, maintenance, and operation of multimodal transportation infrastructure and services; or
- any other public purpose, including an audit of a regulating agency or a shared mobility service provider.

This final requirement lays out some clear goals that justify receiving this data, but also includes a catch all provision again referring to "any other public purpose." The author may wish to consider further defining what legitimate public purposes are, or at the very least, imposing some sort of transparency requirement so that the public is aware of the stated public purpose. In addition, it is unclear who would have oversight over these policies and programs. Therefore, the author may also wish to consider identifying an accountability mechanism for those receiving this potentially sensitive data.

The bill makes clear that a regulating agency or recipient public agency is prohibited from disclosing shared mobility service data to a local, state, or federal law enforcement agency other than as required by law pursuant to a warrant or through a court order, subpoena, or other legal process. In order to ensure that such data, which has been shared for regulatory purposes, is not used for other ends by law enforcement, the author has agreed to the following amendment:

> Amendment
>
> Amend Section 1798.78.4 as follows:
>
> (b) A regulating agency or recipient public agency shall not disclose shared mobility service data to a local, state, or federal law enforcement agency other than as required by law pursuant to a warrant issued under Chapter 3 (commencing with Section 1523) of Title 12 of Part 2 of the Penal Code ~~or through a court order, subpoena, or other legal process~~.

In addition to disclosure to other public agencies, the bill allows a regulating agency or public agency to publicly disclose shared mobility service data that includes location data if all of the following criteria are met:

- at least 24 hours have passed since the latest event or status notification included in the deidentified shared mobility service data;
- any location field has been redacted or the precision of data in a location field has been reduced by using any of the following methods of aggregation, obfuscation, or anonymization:
    - aggregation of records sharing a common geography, time of day, or date range to generate a sum, average, minimum, maximum, or other summary value;
    - replacing precise latitude and longitude data with census blocks or other common geography; or
    - using any other method reflected in an adopted industry standard or used, endorsed, or recommended by the United States Census Bureau or the National Institute of Standards and Technology; and
- the location data does not depict a shared mobility device or service currently in use by a user.

The author's stated intent here is to limit this to deidentified data that includes location information. To make it completely clear that all disclosures are prohibited, except for deidentified data, and only as provided, the author has agreed to the following amendments:

Amendment

Amend 1798.78.3 as follows:

(a) Subject to Section 1798.78.4, a regulating agency, an employee of the regulating agency, a contractor, or an agent who has access to the shared mobility service data, shall not disclose shared mobility service data. A regulating agency may ~~shall not~~ disclose deidentified shared mobility service data to another public agency if ~~unless~~ all of the following are true:

Amend Section 1798.78.4 as follows:

(a) Notwithstanding any other law, including the California Public Records Act (Division 10 (commencing with Section 7920.000) of Title 1 of the Government Code), in order to protect individual privacy and to minimize risk of reidentification of users, a regulating agency, or public agency, an employee, contractor, or agent of the regulating agency who has access to the shared mobility service data, shall not disclose shared mobility service data. A regulating agency or public agency may disclose deidentified shared mobility service data that includes location data to the public if ~~unless~~ all of the following criteria are met:

Although arguably unnecessary, the bill clarifies that it does not prohibit a public agency from disclosing to the public contemporaneous data that identifies the location of shared mobility devices or services that are currently available for public use to facilitate multimodal user access, trip planning, or trip payment.

While the above provisions seek to set the balance on the granularity of the data and the protections that should be afforded to it in its various states, the bill also directly addresses the CalECPA issue. It provides that "[s]hared mobility service data is not electronic device information or electronic information, as defined [in CalECPA]." The bill also states that this is declaratory of existing law.

The issue of the applicability of CalECPA to this information is currently the subject of ongoing litigation. In fact, LADOT and the City of Los Angeles, the co-sponsor of this bill, filed a letter with the Ninth Circuit in that litigation pursuant to Federal Rule of Appellant Procedure 28(j), which authorizes parties to notify the court of "pertinent and significant authorities" that come to a party's attention after their brief has been filed. The letter notified the court of this bill's existence and its relevance to arguments in that case.[21] This Committee has traditionally discouraged passing legislation that could potentially interfere with such litigation, especially when a party to that litigation is a sponsor of the bill.

Outside of merely exempting local transportation regulators from the requirements of CalECPA with regard to the information, the provision also removes CalECPA's protections against law enforcement, including federal law enforcement, compelling disclosure of the information without needing a warrant or wiretap order.

The Electronic Frontier Foundation raises serious concerns with this CalECPA provision:

> This bill, as written, would eliminate the protections of the California Electronic Communications Privacy Act (CalECPA), which requires government entities to get a warrant before they can access electronic information about who we are, where we go, who we know, and what we do.1 Location information is highly sensitive, and should be treated accordingly. That's why EFF worked to pass this law in 2018 with a broad coalition of groups dedicated to privacy and free expression. The legislature should not undo the protections of this landmark privacy law.

Given the pending appeal in the above-referenced litigation, the author has agreed to amend one provision of the bill that deems the provision stating that this data is not governed by CalECPA is declaratory of existing law, as follows:

---

[21]Letter, *Supplemental Authority in Sanchez v. LADOT (No. 21-55285)* (March 21, 2022) Los Angeles City Attorney.

Amendment

Amend Section 3 of the bill as follows:

The additions by this act of subdivision (a) of Section 1798.78.2 and subdivision (a) of Section 1798.78.5 to the Civil Code does not constitute a change in, but is are declaratory of, existing law.

4. Stakeholder positions

The United Food and Commercial Workers Western States Council and the California Labor Federation, both co-sponsors of the bill, explain the need for the bill:

> Device specific data is needed to ensure driver safety, welfare, and accurate reporting by mobility devices. The Vehicle Code currently limits drivers to ten consecutive working hours a day, but the San Francisco County Transportation Authority (SFCTA) states that it is "unclear what mechanism exists to enforce maximum drive time restrictions across multiple platforms." Trip-level device specific data provides local governments with the tools they need to enforce existing regulations designed to protect driver safety. We cannot rely on mobility companies to self-report data. Mobility companies have a long track record of providing regulatory agencies incomplete and inaccurate data, or not providing required data at all. Mandating the sharing of trip-level device specific data by mobility companies will make enforcement of worker protection and environmental standards more effective and efficient by providing cities information to verify claims related to hours worked, overtime, and benefits eligibility, to name a few.
>
> Granular, disaggregated data is also needed to meet the state's ambitious climate goals. The California Air Resources Board (CARB) and the California Public Utilities Commission are currently developing regulations to implement the Clean Miles Standard (CMS) which are new requirements for mobility companies to lower greenhouse gas emissions. Implementation and enforcement of the CMS depends on frequent reporting and tracking of mobility data including Vehicle Miles Traveled, Passenger Miles Traveled, engaged and non-engaged miles traveled, as well as comparing miles driven by zero-emissions vehicles (ZEV, hybrid, and non-ZEV vehicles). The agencies must also track the impact on low-and-moderate income drivers and subsidies administered through other clean air programs. This ambitious program depends on granular, individualized data. The ability of state and local agencies to develop and implement policies regarding labor standards, transportation planning, climate and emissions goals and a host of other areas all depend on access to mobility service data.

> SB 1276 (Durazo) balances the public interest policy goals and individuals rights to privacy by regulating how agencies collect, maintain, and use mobility device specific data by requiring state and regulatory agencies to adopt stringent privacy protection measures . . . .

AARP writes in support:

> Cities are seeing an increasing number of privately-run, data-driven transportation products on their streets, from scooters and bikes to rideshare and food delivery services. These products have the potential to expand mobility options for residents, including those underserved by the current transportation system. But they also have real-world impacts on these streets and the residents who use them, from health and safety, accessibility and equity, and affordability. Taxpayer dollars build and maintain those streets, and residents look to their elected local leaders to ensure the responsible management of these essential public right-of-ways.
>
> AARP supports SB 1276 because we believe that cities are best equipped to work together with shared mobility and technology companies and other stakeholders to make streets, sidewalks, and transportation corridors safe and age-friendly. Providing cities with shared mobility data— in a responsible manner that ensures consumer privacy and data security—results in shared knowledge between the public and private sector, that can shape thoughtful strategies for improving the transportation experience for Californians of all ages and abilities.

The City of Los Angeles, another co-sponsor of the bill, writes:

> For the last three years, more than 100 state and local agencies across California and the globe regulated commercial private, for-profit mobility companies in line with SB 1276. These reasonable data requirements have had great public benefit with zero incidents of privacy intrusion. These jurisdictions only collect mobility device information – they do not want or receive information about consumers, and such information collection would not be allowed under this legislation. In that same timeframe, however, mobility companies have provided incomplete, faulty, and even intentionally manipulated data to regulators.

However, groups in opposition contest this assertion that information about consumers is not being included. A coalition of industry groups in opposition, including TechNet and the California Chamber of Commerce argue:

> Location data is featured prominently in this bill as a notable feature of mobility data for which proponents seek to enhance government access. However, the precise location of an individual—whether they are in their personal vehicle, on a bike, on a trolley, or simply walking on the street—can reveal personal details about where that individual lives, who they visit, and which places they frequent. As a result of this, multiple state laws, including the California Privacy Rights Act, designate location as sensitive personal information, subject to heightened protections when it comes to collection, use, and retention. This bill not only fails to acknowledge the personal nature of geolocation data, it also seeks to degrade legal protections this type of data is afforded by existing privacy laws, such as the California Electronic Communications Privacy Act (CalECPA), which restricts government access to electronic information without a warrant or wiretap order.

Writing in opposition, the Orange County Business Council states:

> The Business Council recognizes that privacy regulations must equally protect and benefit consumers, businesses and employees, and that these regulations should not interfere with a company's ability to serve its customers. SB 1276 dramatically erodes privacy protections for all three while directly limiting industry's ability to safely protect their consumers' data. The bill would authorize state, county, regional and local government agencies to collect an individual's personal data—including their exact location and method of transportation—that can be extrapolated to reveal sensitive information about them. Any attempt to expand government collection of this data should be coupled with substantial safeguards and oversight; however, this bill's broad definitions and its lack of legally enforceable mandates on regulating agencies to protect this sensitive data provide no such oversight. Consumers would not even be aware their data is being collected by the regulating agencies, or how their data is protected and used.

Oakland Privacy acknowledges the premise of the bill but urges that less invasive measures be deployed to achieve that goal:

> Enforcement of transportation rules and regulations is particularly important against transportation-network companies, who have a notorious track record of flouting regulation, exploiting workers, and endangering consumers' privacy. But the proper mechanism for enforcing compliance with the norms and rules that protect against this type of misconduct is not a law that enables even more harm against workers, consumers, and marginalized people.

None of these worthwhile regulatory and planning goals require the government to intrude on the privacy of riders and expose them to surveillance, tracking, and potential harm from the government. Innovation by cities in the delivery of public services or the regulation of public spaces does not justify a program that collects sensitive information without rigorous safeguards that protect people. It is incumbent upon the government to articulate clear use cases that necessitate the collection and maintenance of troves of intimate personal information to achieve specific regulatory objectives. Mere desire on the part of the government or other stakeholders is inadequate.

SUPPORT

California Labor Federation, AFL-CIO (co-sponsor)
City of Los Angeles (co-sponsor)
United Food and Commercial Workers, Western States Council (co-sponsor)
AARP
American Federation of State, County and Municipal Employees, AFL-CIO
Bluegreen Alliance
California Alliance for Retired Americans
California State Council of Service Employees International Union
Los Angeles County Federation of Labor, AFL-CIO
Transport Workers Union of America, AFL-CIO
United Food and Commercial Workers, Western States Council

OPPOSITION

Anaheim Chamber of Commerce
Asian Industry B2B
California Chamber of Commerce
California Lulac
Central City Association of Los Angeles
Crime Survivors Resource Center
Electronic Frontier Foundation
Livermore Valley Chamber of Commerce
Los Angeles Area Chamber of Commerce
National Action Network Los Angeles
Oakland Privacy
Orange County Business Council
Orange County Hispanic Chamber of Commerce
San Jose Chamber of Commerce
Silicon Valley Leadership Group
TechNet
Valley Industry & Commerce Association

RELATED LEGISLATION

Pending Legislation:

AB 371 (Jones-Sawyer, 2021) amends the insurance requirements applicable to shared mobility service providers and requires providers to affix signs identifying shared mobility devices for purposes of reporting illegal or negligent behavior. This bill is currently in the Senate Insurance Committee.

AB 2488 (Irwin, 2022) requires a public agency that collects precise geolocation data to maintain reasonable security procedures and practices to protect it from unauthorized access, destruction, use, modification, or disclosure and implement a usage and privacy policy, as specified. The bill defines precise geolocation data as any data that is derived from a device and that is used or intended to be used to locate a person, as specified. The bill requires a public agency that collects or intends to collect precise geolocation data to provide an opportunity for public comment, as specified, before collection begins. The bill prohibits a public agency from selling, sharing, or transferring that data except to comply with a lawful court order. It also requires a public agency that collects precise geolocation data to obtain lawful permission to collect it prior to collection and maintain that permission. The bill provides that lawful permission includes any collection in conformity with CalECPA, a subpoena, court order, or search warrant for the particular device from which precise geolocation data is derived, or consent, as defined, of the person who possesses the device from which precise geolocation data is derived. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

AB 859 (Irwin, 2021) *See* Comment 2.

AB 1286 (Muratsuchi, Ch. 91, Stats. 2020) required shared mobility service providers, as defined, to enter into an agreement with or obtain a permit from the local jurisdiction in which the providers' devices are used. Such agreement or permit must require certain minimum levels of liability insurance. The bill also required cities and counties authorizing providers to operate within their jurisdictions to establish rules governing the operation, parking, and maintenance of these devices by ordinance, agreement, or permit terms.

AB 3116 (Irwin, 2020) *See* Comment 2.

AB 1112 (Friedman, 2019) *See* Comment 2.

AB 1142 (Friedman, 2019) *See* Comment 2.

AB 2989 (Flora, Ch. 552, Stats. 2018) required an operator of a motorized scooter to wear a helmet, only if they are under the age of 18, and permits local authorities to authorize the operation of motorized scooters on roads with speed limits up to 35 miles per hour.

SB 182 (Bradford, Ch. 769, Stats. 2017) prohibited a local government from requiring business licenses from drivers for transportation network companies who do not reside in its jurisdiction.

SB 178 (Leno, Ch. 651, Stats. 2015) *See* Comment 2.

****