Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 859 (Irwin) – As Introduced February 17, 2021

SUBJECT: Mobility devices: personal information

SUMMARY: This bill would, among other things, authorize a public agency that issues a permit to an operator for mobility services to require that operator to periodically submit anonymized trip data, and would clarify that trip data is personal information (PI), as specified and subject to the Electronic Communications Privacy Act (CalECPA). Specifically, **this bill would**:

1) Authorize, notwithstanding any other law, a public agency to require an operator to periodically submit to the public agency anonymized trip data regarding the operator's mobility devices operating in the geographic area under the public agency's jurisdiction.

2) Require that a public agency give an operator reasonable notice of any requirement to submit anonymized trip data and sufficient time to aggregate and deidentify any anonymized trip data to be submitted.

3) Authorize a public agency to share anonymized trip data with a contractor, agent, or other public agency only if all the following are true:

    - the purpose of the sharing is to assist the public agency in the promotion and protection of transportation planning, integration of mobility options, and road safety, including the safety of riders, operators, pedestrians, and motorists;

    - a trip included in the data that is being submitted has not ended within the previous 24 hours; and

    - any recipient of the anonymized trip data is expressly prohibited by contract from using or disclosing the anonymized trip data for any commercial purpose.

4) Provide that trip data is PI, as defined in the California Consumer Privacy Act (CCPA).

5) Prohibit any public agency from obtaining trip data except as provided by the Electronic Communications Privacy Act (CalECPA).

6) Define various terms, including:

    - "Aggregated" to mean that the data reflects average information, including trip length, trip duration, approximate trip, and location of no less than five separate trips by no less than five separate users.

    - "Anonymized trip data" to mean data pertaining to a trip taken by a user that has been aggregated and deidentified.

- "Deidentified" to mean information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular user or trip, except that information shall not be deemed to be deidentified if it is provided to a recipient that does not meet all of the following criteria:

    - the recipient has implemented technical safeguards that prohibit reidentification of the user or trip to which the information pertains;

    - the recipient has implemented processes that specifically prohibit reidentification of the information;

    - the recipient has implemented processes to prevent unauthorized access, inadvertent release, or public disclosure of deidentified information; and

    - the recipient does not attempt to reidentify the information.

- "Mobility device" to mean any transportation device or vehicle, including, but not limited to, a bicycle, electric bicycle, dockless bicycle, electric scooter, vehicle utilized on the online-enabled application or platform of a transportation network company, autonomous vehicle, and any other device or vehicle by which a person can be propelled, moved, or drawn that is displayed, offered, or placed for rent in any public area or public right-of-way, subject to certain exceptions.

- "Operational data" to mean data, that is neither trip data nor anonymized trip data, pertaining to the location of a stationary mobility device owned or controlled by the operator that is not engaged by users or on a trip.

- "Operator" to mean a person or entity that makes mobility devices generally available to the public, including through an online-enabled technology application service, website, or system.

- "Trip data" to mean data that is not anonymized trip data pertaining to a trip taken by a user, including, but not limited to, GPS data, an address, time or date stamp, and route data that have not been aggregated and deidentified.

- "User" to mean a rider of a mobility device or accountholder of an operator.

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, Sec. 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 sec. 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 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 Sec. 1546 et seq.)

4) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the Act. Subject to various general exemptions, a consumer has, among other things:

   - the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI;
   - the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;
   - the right to access the specific pieces of information a business has collected about the consumer;
   - the right to delete information that a business has collected from the consumer; and,
   - the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and,
   - the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to ensure that individual trip data from mobility devices is protected under CalECPA, and to create a framework for state or local governments to require the periodic submission of deidentified and aggregated trip data from mobility device operators, as specified. This bill is author-sponsored.

2) **Author's statement:** According to the author:

   > The California Electronic Communications Act (CalECPA) was enacted in 2015 (SB 178 Leno). This statute codified developments in constitutional case law which prohibits a government entity from compelling the production of, or access to, electronic device information without a search warrant, wiretap order, or subpoena. Additionally, the

California Consumer Privacy Act (CCPA) was enacted in 2018, and Prop 24 the California Privacy Rights Act was approved by voters in 2020. These statutes grant a consumer various rights with the respect to their personal information, including geolocation data, which is held by a private entity.

Despite the development of these statues, in 2018 the Los Angeles Department of Transportation (LADOT) developed open source APIs to run a program, Mobility Data Specification (MDS), which facilitates data sharing between mobility operators and local governments [citation omitted]. Although seemingly innocuous, MDS collects information on the time and exact location of the start, end, and route of each device with a 24 hour delay. Since the launch of MDS, local governments across the country have adopted permitting requirements for micro-mobility operators including Los Angeles, Long Beach, San Diego, San Francisco, San Jose, and Santa Monica. The goal is to have centralized data sharing for cities to manage the mobility services within their jurisdiction, beginning by tracking e-scooters, e-bikes, and other micro-mobility devices, with the intention of incorporating other mobility services such as TNCs. However, this sharing is deeply intrusive and raises privacy concerns.

In the summer of 2019, […] Office of Legislative Counsel analyzed and issued an opinion concluding that CalECPA restricts a department of a city or county from requiring a business to provide the department with real-time location data from its mobility devices as a condition of granting a permit to operate. Unfortunately, some local governments continue to ignore CalECPA by fallaciously and dangerously arguing that CalECPA only applies to police departments.

On February 23rd, 2021, a federal judge dismissed the ACLU's lawsuit against the Los Angeles Department of Transpiration on substantive and procedural grounds, which alleged various privacy violations from their Mobility Data Specification permit requirement, identifying that only the Attorney General can enforce CalECPA, and calling the other general privacy issues presented "more appropriately addressed as a matter of public policy."

The ACLU is still reviewing its decision to appeal, but with at least one court unwilling to stand up for Californian's privacy rights, legislation is necessary to provide unequivocal protections to this sensitive data.

3) **Debate over individual trip data**: Shared mobility devices are a relatively new transportation option where devices like bikes, electric bikes, and electric scooters are shared among users. They are typically enabled by a mobile application and run by private companies. Providing more low-emission mobility options can create a more diverse, convenient, and accessible transportation network that may reduce emissions and congestion and improve the quality of life in cities. That is not to say that incorporating shared mobility devices into California communities has been without problems. As with all new technologies, shared mobility devices can also pose significant challenges regarding the management of public-rights-of-way, encouraging public safety, and adapting old regulations to new business models. Shared electric bikes and scooters, with their promise of improving congestion and offering low-cost, green transportation in urban areas, have been widely criticized as riders fail to properly operate them.

Part of the technology involved with shared scooters and other similar devices requires that the operator have access to location data at the beginning and end of each trip so that the devices can be retrieved for charging and maintenance. In addition, many providers of these devices keep continuous trip data, which necessarily raises questions as to what can be done with that trip data and how that might impact the privacy of the rider.

In light of the challenges experienced by communities by the introduction of shared mobility devices, three bills were introduced last legislative session, seeking to address some of the issues presented. AB 1286 (Muratsuchi, Ch. 91, Stats. 2020) created uniform regulations with regard to mobility devices and required that local governments who choose to have shared mobility devices in their community implement parking, maintenance, and operational rules prior to shared mobility devices being dispersed in communities. By contrast, AB 1112 (Friedman, 2019) would have largely prohibited local governments from adopting certain policies or regulations. The central point of debate in AB 1112 was the ability of local governments to compel the disclosure of trip data, defined as any data elements related to trips taken by users of a shared scooter of an operator, including, but not limited to, GPS, timestamp, or route data. That bill failed to move forward in the Senate and AB 3116 (Irwin, 2019) was introduced to address the sharing of information between operators and local governments.

Local governments require data from operators so that they may engage numerous activities, including transportation planning and ensuring that shared mobility devices are disturbed equitably within the community. Local governments need not, however, have access to *personally identifiable* location data (or data that could be rendered personally identifiable) for these purposes. Indeed, this Committee has long argued that blanket access to such information would be in violation of CalECPA, which generally prohibits any government entity from compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device, absent a warrant, as specified. (Pen. Code Sec. 1546 et seq.) This belief was confirmed last year when the Office of the Legislative Counsel issued an opinion concluding, among other things, that CalECPA does in fact prohibit a department of a city or county from imposing a real-time data sharing requirement on a dockless mobility provider as a condition of granting a permit to operate in the department's jurisdiction.

More recently, the Los Angeles Department of Transportation (LADOT) was granted a motion to dismiss all claims in a case brought by the ALCU. *In Sanchez v. LADOT* (2021) U.S. Dist. LEXIS 34711, the district court held that CalECPA 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 processing. It does not, however, allow the person to initiate an entirely new civil action before another, unrelated tribunal." The court then recognized "[p]laintiff's concern with the unprecedented breadth and scope of the [City of Los Angeles'] location data collection. But that alone does not mean it violates their constitutional or statutory privacy rights. This is an issue that may be more appropriately addressed as a matter of public policy, which is not for this Court to opine."

This bill, consistent with the Legislative Counsel opinion and invitation from the court to address statutory privacy protections as a matter of public policy, would create parameters

for the permissible sharing of mobility device information without violating existing privacy laws.

Oakland Privacy writes in support:

> The Legislature has discussed many bills on mobility data over the last few years, always failing to arrive at a clear consensus for policy going forward. The question pits two fundamental interests against each other: the interest of privacy in our movements around cities and the interest of municipalities in traffic management and the effective utilization of roads and sidewalks. In a recent hearing in court, the court ruled that the decision was not a legal one, but a basic question of policy for elected officials to decide. Our support for Assembly Bill 859 is not simply based on our name and profile as a privacy rights organization, and prioritizing the privacy interest over the transportation management interest, but in a sincere belief that in fact these two interests are complimentary, and far less opposed than has been previously presented.

4) **Clarifies existing law regarding the collection and disclosure of certain types of personal information as it pertains to both commercial entities and government agencies**: This bill defines trip data as data that is not anonymized trip data, pertaining to a trip taken by a user, including, but not limited to, GPS data, an address, time or date stamp, and route data that have not been aggregated and deidentified. The bill specifies that trip data is both PI within the meaning of the CCPA and subject to the requirements of CalECPA. The practical effect of these clarifications is an increased ability of California residents to safeguard their geolocation information from both private businesses and government agencies.

   Specifically, the designation of trip data as PI in the CCPA ensures that users of mobility devices have important rights with regard to their trip data namely, the right to direct the mobility device operator to not sell the consumer's data, and the right to instruct the operator to delete the data. The designation of trip data as electronic device information, as defined in CalECPA ensures that government agencies cannot compel that information absent a warrant, as specified.

   Staff notes that even absent this bill, trip data arguably satisfies both of these definitions. Thus, these provisions represent merely a clarification and not a substantive change in the law. That is not to say that the clarifications are not important. We are seeing now how governments across the globe are using technology to spread public health messages, render benefits, and increase access to healthcare. At the same time, consumers are turning to technology as a tool and resource to assist with work, connect with friends and family, and stay informed.

   Unfortunately, this influx of technology also brings with it threats to individual privacy and civil liberties. Despite the current protections California offers to its residents, we are seeing the aggressive expansion and development of technology to track individuals and the population in general. For example, over the past year there has been a desire by many government agencies and businesses to develop contract tracing tools to monitor and contain the spread of COVID-19. Depending on how those applications are built and which rules are applied, contract tracing has the potential to permanently track and record individuals using geolocation and other personal data in ways that impermissibly violate their right to privacy and other civil liberties.

Given the increased interest of many private and public entities during the COVID-19 pandemic to track individuals, it is likely that new privacy protections will have to be created. In order to effectively do that, it is critical that our existing privacy laws are uniformly applied and consistently enforced so that there is a strong foundation upon which to build more specific protections.

5) **Appropriately limits government agencies' ability to use and share personal information obtained from private companies**: As noted above, trip data from mobility devices can be incredibly useful to local governments in transportation planning. In order to be useful, however, the trip data does not need to be tied to an individual or individual trips. Aggregated and anonymous data can also provide insight into travel patterns, congestion, usage, and infrastructure needs. Accordingly, this bill seeks to balance users' right to privacy with the utility of trip data for local governments by authorizing public agencies to require operators to periodically submit anonymized trip data. The bill would define "anonymized trip data" as data pertaining to a trip taken by a user that has been aggregated and deidentified, and would create an obligation on the part of local governments to safeguard the data from reidentification and further access or disclosure, as specified.

   Recognizing how local governments may need to use the data, the bill would also authorize a public agency to share anonymized trip data with a contractor, agent, or other public agency, so long as the following requirements are met:

   - The sharing of the data must assist in the promotion and protection of transportation planning, integration of mobility options, and road safety, including the safety of riders, operators, pedestrians, and motorists.

   - Any trip included in the data cannot have ended within the previous 24 hours.

   - Any recipient of the anonymized trip data is expressly prohibited by contract from using or disclosing the anonymized trip data for any commercial purpose.

   Many local governments take issue with the bill because it would require them to use a different system than MDS, the mobility data program developed by LADOT. In opposition, the League of California Cities (Cal Cities) argues:

   > California's cities have pioneered groundbreaking data sharing requirements that help monitor regulatory compliance, ensure ADA compliance, address constituent complaints, enforce equitable distribution of services, and bring innovative mobility options to scale with limited public resources.
   >
   > AB 859 would undermine these existing agreements between cities and mobility service operators, and undo years of deliberation and regulatory design at the California Public Utilities Commission (CPUC). This bill would require cities to expend tremendous resources to renegotiate these agreements and modify their current administrative practices which would incur costs at a time when local governments are facing an unprecedented fiscal crisis from the pandemic.
   >
   > Access to disaggregated data allows cities to uncover and avoid data manipulation to ensure decision making related to transportation planning and projects is rooted in

> accurate and complete data. Additionally, reliable data is essential in local governments' ability to adequately enforce the safe and responsible use of this technology.

The Internet Association (IA) writes in support that this bill is necessary because an "alarming trend has recently emerged of government agencies demanding access to precise and individual on-trip location data collected by mobility companies without seeking a court order or search warrant, as is required by the California Electronic Communications Privacy Act (CalECPA). The state further extended privacy protections in 2018 when the legislature passed the most robust privacy law in the country, the California Consumer Privacy Act. This Act specifically intended to protect users from the misuse and rampant distribution of their data, including location information, across the private sector."

IA further argues, "[t]oday, consumer expectations of transparency and privacy are growing, for both companies and government agencies. And this represents a shared responsibility between the public and private sectors as data continues to flow between us. Smart city planning does not have to come at the expense of consumer privacy, and we are dedicated to working with cities and mobility operators to develop smart, effective, and data-rich solutions in this space. In parallel, we are confident the state of California can continue to lead on this issue by reaffirming its laws that govern both the private and public sector's use of location data. With these laws, we are confident that data can be shared safely and responsibly, and most importantly, utilized for the benefit of mobility device users and your constituents."

The California City Transportation Initiative (CaCTI), a coalition of eight of California's largest cities working on progressive urban transportation policy and traffic safety matters, writes in opposition:

> Local agencies need this data to fulfill our public responsibility to ensure equitable and accessible introduction and deployment of these new mobility devices, and to ensure the continued proliferation of these devices does not jeopardize community safety within the public right of way. That is our job; this bill prevents us from doing our job.
>
> The ***data we require does*** **not** ***include any personal information*** about the people who rent and operate shared mobility devices. While the companies themselves do collect that data, our regulatory systems are not built to receive such data. Even though we do not collect information about individual riders, we do protect the device-specific data as though we were. It is confidential and not subject to public disclosure, it is stored in aggregate, and it cannot be shared with law enforcement absent a subpoena or warrant.

In opposition, the City of Los Angeles writes:

> Dozens of cities in the state - as well as the country and globe - have enacted similar data tools and requirements that use disaggregated data to allow them to bring dockless mobility to their communities in a safe and equitable manner. Having direct access to this data, versus simply receiving aggregated data that can be manipulated, gives cities the ability to hold companies accountable for meeting local rules. Restricting our access to reasonable data will force cities to shut down these mobility programs, impacting key sustainability, and equity-focused transportation goals.

> The City of Los Angeles takes privacy and data security extremely seriously, and we strongly object to the contention that direct access to vehicle data inherently compromises the privacy of riders. The City of Los Angeles does not require permitted mobility operators to provide any information about riders and the method of data collection we use is not designed to receive any data related to individuals who rent mobility devices.

Many of these cities point out the need for real-time data to be able to move devices that have been improperly parked, to provide users with real-time availability of nearby devices, and to hold operators accountable for meeting local rules. Staff notes that this bill, which does not regulate operational data, would arguably allow for local governments to collect the a fair amount of the real-time information they claim to need so long as it is not during a trip taken by a user. The location of parked devices and arguably information like maintenance records and total miles traveled, do not raise issues related to individual privacy in the same way that sharing route data (which is, by its very nature, connected to an individual rider) raises concerns. Given the issues raised by local governments in opposition to this measure, however, the author may wish to clarify the permissible use of operational data, which includes location and other data about a device while it is *not* in use, as the bill moves through the legislative process.

When this Committee heard AB 3116 last year, the local governments in opposition to the bill also asked the state to delay regulation in this area, as cities are doing it effectively on their own. San Jose specifically pointed to the impact and budget deficits resulting from the COVID-19 pandemic and asks that conversations around government access to mobility data be continued until the crisis has been resolved.

Looking to the impacts of COVID-19, however, can easily lead one to draw a different conclusion. Namely, that as the use of potentially invasive and ever expanding technologies, well-intentioned or otherwise, grows in response to the ongoing pandemic, provisions like the ones found in this bill will help ensure strong safeguards for privacy that persist beyond the current crisis.

6) **Definition of mobility device is arguably broad**: This bill would define mobility device to mean any transportation device or vehicle, including, but not limited to, a bicycle, electric bicycle, dockless bicycle, electric scooter, vehicle utilized on the online-enabled application or platform of a transportation network company (TNC), as defined, autonomous vehicle, and any other device or vehicle by which a person can be propelled, moved, or drawn that is displayed, offered, or placed for rent in any public area or public right-of-way.

In opposition, a large coalition of labor organizations argues that local governments need data to enforce the provisions of AB 5 (Gonzalez, Ch. 296, Stats. 2019) with regard to TNCs. The coalition writes:

> AB 859 would hamper local governments' ability to enforce the provisions of AB 5 (Gonzalez) – *Dynamex*. Cities are a key partner in ensuring compliance with AB 5 and enforcement of violations. This is particularly true now following the passage of Proposition 22 in November 2020, which exempted transportation network companies from most state labor and wage laws. As a result, cities such as San Francisco, Los Angeles, and San Diego have taken the lead in protecting these workers using the legal tools at their disposal.

A large part of enforcing transportation network companies (TNCs) will occur through auditing. To effectively audit TNCs, cities need data on every trip. AB 859 seeks to hamper cities' ability to audit AB 5 provisions because they prohibit cities from receiving individual trip data. Without it, cities cannot verify hours worked by TNC drivers. This bill would only allow cities to request aggregated data, which provides no value in the context of labor standards enforcement. There is no way to use aggregated data to verify hours worked, which is critical for adjudicating wage and labor issues to protect workers. In fact, this bill goes in the opposite direction of states like New York that are requiring trip-level micro data to not only better protect workers, but to assist in achieving additional public policy goals of safety, transportation planning, air quality improvements, etc.

Furthermore, individual data is needed to ensure driver safety and welfare and accurate reporting by TNCs. 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." Individual trip-level data provides local governments with the tools they need to enforce existing regulations designed to protect driver safety. We cannot rely on TNCs to self-report data. TNCs have a long track record of providing regulatory agencies incomplete and inaccurate data, or not providing required data at all. Mandating the sharing of individual trip data by TNCs will make AB 5 enforcement more effective and efficient by providing cities information to verify claims related to hours worked, overtime, and benefits eligibility, to name a few.

While the author and stakeholders clearly intend for mobile devices like electric scooters and bikes to be covered by this bill, this definition would also include rental cars, which are separately regulated in the Civil Code. The definition also captures TNCs, defined 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," which are regulated exclusively by the California Public Utility Commission (CPUC). (Pub. Util. Code Sec. 5430 et seq., and Cal. Const. art. XII, Sec. 8.) Because the Legislature gave the CPUC regulatory authority over TNCs, local government agencies should not be able to compel data from them.

The CPUC, however, has imposed substantial reporting requirements on TNCs, and recently began sharing the data it collects more broadly. While local governments may collect and use this data released by the CPUC, or any data the TNC voluntarily provides, the state constitution prohibits local governments from *compelling* data from the TNCs directly.

That being said, the provisions of the bill limiting what a local government can do with anonymized trip data and prohibiting the sharing of trip data with a contractor would apply to any TNC data that a local government acquired. Accordingly, this bill would increase safeguards for trip data generated by individuals using TNCs.

7) **Court asks Legislature to further clarify enforcement of CalECPA**: As briefly described above in Comment 3, the Los Angeles District Court recently held that petitioner riders,

whose trip data was in the possession of the LADOT, lacked standing to bring a claim under CalECPA, and that the only entity that can compel a government agency to comply with CalECPA is the Attorney General. The court wrote:

> 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). The language differs from subpart (c) because the Legislature intended a different meaning. If the Legislature wanted to allow an individual whose information has been targeted to "commence a civil action" to challenge the production, it could have grouped these individuals along with the Attorney General in bestowing that right in subpart (b). But it did not, and instead granted them a different right, employing different language, in a separate subsection the Los Angeles Department of Transportation was granted a motion to dismiss all claims in a case brought by the ALCU. (Emphasis in original.)

The court continued, "This is an issue that may be more appropriately addressed as a matter of public policy, which is not for this Court to opine."

Importantly, the court did not hold that "trip data" is excluded from the definition of electronic device information under CalECPA. Instead, the court held that claims for violations of CalECPA where the there was never a request for information filed in a court (*e.g.*, a request for a warrant) is not actionable under CalECPA. This bill would clarify that trip data is subject to CalECPA, which would allow an operator to refuse to turn over trip data to a local government unless the local government provided a warrant. This bill does not, however, seem to address the standing issue raised by *Sanchez* since the trip data in that case had been turned over to the LADOT voluntarily by the operator.

Accordingly, if the author wishes to address the standing situation raised in *Sanchez*, or otherwise limit the type of information operators can *voluntarily* turn over to local governments, this bill would need to take a different direction and would require significant amendments.

8) **Prior legislation**: AB 3116 (Irwin, 2020) *See* Comment 3.

AB 1112 (Friedman, 2019) *See* Comment 3.

AB 1286 (Muratsuchi, 2019) *See* Comment 3.

SB 178 (Leno, Ch. 651, Stats. 2015) enacted CalECPA, which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.

REGISTERED SUPPORT / OPPOSITION:

Support

Internet Association
Oakland Privacy

Opposition

California City Transportation Initiative (unless amended)
California Conference Board of The Amalgamated Transit Union
California Conference of Machinists
California Labor Federation, AFL-CIO
California School Employees Association
California State Council of Service Employees International Union (SEIU California)
California Teamsters Public Affairs Council
City of Los Angeles (unless amended)
City of Sacramento (unless amended)
Disability Rights Education & Defense Fund (DREDF)
Engineers and Scientists of California, Ifpte Local 20, AFL-CIO
League of California Cities
Northern California District Council of The International Longshore and Warehouse Union (ILWU)
Professional and Technical Engineers, Ifpte Local 21, AFL-CIO
Streets for All
Transport Workers Union of America, AFL-CIO
Unite-here, AFL-CIO
United Food and Commercial Workers, Western States Council
Utility Workers Union of America, AFL-CIO

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200