Date of Hearing: May 5, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 3116 (Irwin) – As Amended May 4, 2020

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 electronic device information, as defined in the Electronic Communications Privacy Act. 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 personal information, as defined in the California Consumer Privacy Act (CCPA), and is also electronic device information, as defined in the Electronic Communications Privacy Act (CalECPA).

5) 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 of Criticality**: In response to the unique constraints the COVID-19 crisis has placed on the legislative process, the Committee elected to focus attention this session on bills that address only the most urgent issues and issues critical for an efficient recovery from the pandemic. In order to prioritize bills that require immediate attention, the Committee asked the author of each bill to provide a Statement of Criticality explaining the applicability of one or more of the following criteria to that bill:

   - the bill addresses a problem that was created by, or has been significantly exacerbated by, the ongoing public health crisis due to COVID-19, or the response thereto;

- the bill addresses an urgent problem that presents a threat to the safety and security of Californians and must be resolved immediately; or

- the bill makes a technical change to an existing program or function that must be immediately adopted to preserve the utility of that program or function.

In response, the Author writes:

> AB 3116 provides clarity that mobility device information is covered under current provisions of CalECPA as it relates to government use of location information. As Legislative Counsel has already stated, mobility devices and geolocation tracking fall under CalECPA. Given that local governments are disputing that interpretation, this bill is simply meant to clarify this existing law while providing a path towards reasonable aggregate and deidentified data use for transportation planning. As efforts continue to use data and technology to address this public health emergency at the local level, it is of critical importance that misinterpretations of existing law which harm the privacy of Californians are not allowed to persist.
>
> This crisis may end up exacerbating current misuse of location data by local governments depending on what they decide to do regarding data collection in each of their localities and how they intended to operationalize that data in each department that may be provided access to it. The legislature should be addressing this misinterpretation of law and leveraging of local permitting power which currently enables local governments to access this sensitive information without oversight, data protections, and consumer rights.
>
> As the legislature has made clear with CalECPA and CCPA, among other groundbreaking policies, data privacy is considered a safety and security issue for Californians. Given that local government entities are currently, actively pursuing this data tracking of Californians, this bill addresses an urgent problem that is a threat to security and safety.
>
> As California importantly explores how user data can help public health agencies right now, it's critically important that any government use of user data during this crisis is discussed within the appropriate legal framework, to ensure our policies reflect how moments of uncertainty & emergency response impact our decisions and address the potential for ongoing privacy violations post-crisis.

The Committee agrees that the issues addressed by this bill are timely and critical under the current circumstances. Right now, the need for personal information, like health and geolocation information of private individuals, is seemingly greater than it has ever been. Despite the protections, California offers its residents, and in light of the continuing challenge of containing this pandemic, we are seeing the aggressive expansion and development of technology to track individuals and the population in general. This bill seeks to ensure that existing privacy laws are respected and creates reasonable safeguards for the government use and sharing of individuals' geolocation information, which is critically necessary as many state and local governments rush to obtain PI in an effort to contain the spread of COVID-19.

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 technology or a mobile application and frequently 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 in relation to shared mobility devices, two bills were introduced last year, seeking to address some of the issues. AB 1286 (Muratsuchi, 2019) would have created uniform regulations with regard to mobility devices and required that local governments who choose to have shared mobility devices in their community implement safety, 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.

   This Committee has frequently expressed concern regarding the collection and sale of geolocation data. That being said, trip data is clearly useful for a local government to determine how shared mobility devices will be best utilized in a community. Trip data can help ensure that appropriate lanes are created to deal with congestion, and appropriate docking stations are installed in high-use areas to ensure that sidewalks are minimally impacted for pedestrians.

   Local governments need not have access to *personally identifiable* location data, however, for transportation planning. 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.)

   Striking a balance between the needs of local governments to have access to transportation data and individual rights to privacy, AB 1112 was substantially amended in this Committee to ensure that local governments may have access to trip data that is necessary to the development of appropriate transportation planning, in a more consistent manner with other

established California laws and policies, namely CalECPA and the CCPA. Notably, under these laws, law enforcement would not be able to access this information from anyone other than the rider without a warrant, or other limited circumstances authorized by CalECPA. Ultimately those amendments drew opposition from local governments seeking unfettered access to individual trip data, and the author dropped the bill.

At the same time, these bills were moving through the Legislature, the Los Angeles Department of Transportation (LADOT) suspended Uber's permit to operate within its jurisdiction for failing to abide by LADOT's data sharing requirements, as required by its pilot program. Uber subsequently filed an administrative appeal. In the decision upholding the suspension, the administrative hearing officer found weak points in both sides; arguments, writing that Uber "offered no specific case of identification, although the abstract concern is real. LADOT offered no specific scenario, which 'five-second' reporting prevented or solved, even while contending that such reporting, in its administrative view, is necessary to implement" its pilot program.

Not long thereafter, 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. This bill, consistent with the Legislative Counsel opinion, would create parameters for the permissible sharing of mobility device information without violating existing privacy laws.

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 electronic device information, subject to 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.

   The Electronic Frontier Foundation (EFF) argues that this bill takes a significant step toward protecting the location privacy of Californians across the state who rely on shared mobility devices. EFF writes, "[l]ocal and regional planning agencies in jurisdictions across the United States are increasingly demanding access to data about new mobility services and devices in order to better plan for the future and ensure that city streets work for everyone. EFF agrees that planning agencies should be able to collect some data in order to ensure that new transportation devices are deployed safely, efficiently, equitably, and sustainably. But planning agencies should not need to collect sensitive, personally identifiable information

about riders in order to do so." EFF writes that it would move to a support position if the bill's reference to CalECPA was improved. EFF writes:

> Section 1798.78.4(b) of A.B. 3116 currently provides that "Trip data is electronic device information, as defined in Section 1546 of the Penal Code." This statement of existing law is true, but not complete, as trip data is also "electronic communication information" under CalECPA's broad definition of that term. As a result, the existing language of A.B. 3116 will potentially cause confusion and complications down the line. EFF and ACLU therefore have proposed that section 1798.78.4(b) be amended as follows: "A public agency shall not obtain trip data except as provided by Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code." We support A.B. 3116 if so amended.

This amendment would ensure that local governments are aware of their obligations under CalECPA, which generally requires a warrant, before compelling trip data (i.e, data that is not anonymized, aggregated and deidentified, and pertains to a trip taken by a user) from anyone other than the user themselves.

> Author's amendment:
>
> On page 4, lines 23-24, strike "Trip data is electronic device information, as defined in Section 1546 of the Penal Code" and insert *"A public agency shall not obtain trip data except as provided by Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code"*

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, there is currently a desire by many government agencies and individuals 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 our 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.

   A coalition of organizations including Technet, the California Chamber of Commerce and Bay Area Council argue 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."

   The coalition 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."

   A number of cities argue in opposition that this bill would impede their ability to collect useful data and meaningfully regulate shared mobility devices on city streets. Cities including Oakland, San Jose, Los Angeles and Santa Monica specifically argue that the bill is

in conflict with locally-developed data tools which rely on real-time data. At the same time, these cities also point out that they are very privacy focused and already in compliance with many provisions of the bill. Santa Monica, for example, writes that it does "not receive from the shared mobility providers any of the personal identifying information that those providers take from their customers. Nor do we receive real-time data. And we have implemented, and remain willing to implement, additional safeguards to ensure that the data they do obtain is protected and used only for its intended purpose, to regulate the use of shared mobility devices to ensure that the public right of way remains safe for all of the myriad forms of transportation that currently seek to share it."

Oakland writes that their local "privacy provisions ensure that any data we receive is anonymized, classified as 'confidential,' and therefore not subject to the public records act, and only available to law enforcement with a subpoena or warrant, although the data received would have very little use to law enforcement due to its already anonymized nature; which is why there have been no such warrants or subpoenas."

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 majority 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.

As a general matter, the local governments in opposition to this bill also ask the state to delay regulation in this area, as cities are doing it effectively on their own. San Jose specifically points 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.

The precise location of an individual is deeply personal. As noted by EFF, this bill's "protections are critical because even with names stripped out, location information is notoriously easy to re-identify, particularly for habitual trips. This is especially true when location information is aggregated over time. As one 2013 study on human mobility data concluded, 'human mobility traces are highly unique.' Researchers found that only "four spatio-temporal points [were] enough to uniquely identify 95% of the [1.5 million] individuals" in the study."

EFF continues, "AB 3116 appropriately requires local authorities to collect aggregated or nonidentifiable trip data for city-planning purposes. The biggest mistake local jurisdictions could make would be to collect data first, and think about what to do with it after consumers' privacy has been put at risk."

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, 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.

   While the author, sponsor, 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 cannot 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, discussed above in Comment 5, 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) **Prior legislation**: 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

Bay Area Council
California Chamber of Commerce
Electronic Frontier Foundation (if amended)
Internet Association

Silicon Valley Leadership Group
TechNet

Opposition

City of Los Angeles
City of Sacramento
City of Santa Monica
City of Oakland
City of San Jose
San Francisco Municipal Transportation Agency (unless amended)

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