


CITY OF LOS ANGELES
INTER-DEPARTMENTAL MEMORANDUM

Date: August 15, 2019

To: Honorable City Council
c/o City Clerk, Room 395
Attention: Honorable Mike Bonin, Chair, Transportation Committee

From: Seleta J. Reynolds, General Manager 
Department of Transportation

Subject: **STATE OFFICE OF LEGISLATIVE COUNSEL OPINION ON THE CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT**

On August 2, 2019, the California Office of Legislative Counsel issued an opinion on whether the California Electronic Communications Privacy Act (CalECPA) restricts a local transportation department, a regulatory agency, from requiring real-time data as a permit condition for dockless mobility operators. The Los Angeles Department of Transportation (LADOT) believes this opinion too narrowly interprets the question presented and fails to recognize the Legislature's clear intent of CalECPA to address the actions of law enforcement agencies. LADOT consulted the City Attorney on this matter, does not find that CalECPA applies to existing dockless permit requirements, and will continue to require full compliance from mobility providers.

Statutory text and legislative intent

CalECPA was not written to limit the actions of regulatory agencies or to control the regulation of dockless mobility devices in the public right-of-way by a local department of transportation. In fact, there is no mention in either the statutory text or legislative history of any intent by the Legislature to limit or restrict a government regulator from using electronic data within the course and scope of regulating entities that are not electronic communications services.

Instead, both the text and legislative history of CalECPA make clear that the statute was written to address the actions of law enforcement agencies and to restrict California law enforcement from unwarranted access to electronic communications information when conducting criminal investigations and intelligence gathering.

The June 19, 2015 analysis of the Assembly Committee on Privacy and Consumer Protection, referenced in the Legislative Counsel's opinion, states that CalECPA "[institutes] 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."

The first sentence of the September 9, 2015 Senate floor analysis, also referenced in the Legislative Counsel opinion, states, "This bill creates the California Electronic Communications Privacy Act, which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider."

CalECPA itself is set forth in the “Criminal Procedure” Part of the Penal Code, in Title 12 of that Part, titled “Of Special Proceedings of a Criminal Nature.” The main remedy provided by the Legislature for agency violations of CalECPA (Penal Code Section 1546.4) is a motion “to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter.” Evidentiary procedures of this sort are intended to protect defendants in criminal prosecutions and are not relevant to any local regulatory process. It is clear that in both text and intent, CalECPA is limited to law enforcement access to electronic information in the course of criminal investigations.

LADOT enforcement of individual dockless mobility users

As stated and confirmed throughout the public process to develop the City of Los Angeles’ (City) Dockless Mobility Pilot Program, LADOT is not responsible for the enforcement of moving violations by individual dockless riders. LADOT is responsible for regulating operator compliance with the City Council adopted rules and guidelines, and requires data from operators to fulfill its regulatory obligations.

LADOT has reiterated in its Data Protection Principles (attached), developed and published with public notice and comment, that “law enforcement and other government agencies, whether local, state, or federal will not have access to raw trip data other than as required by law, such as a court order, subpoena, or other legal process.” LADOT expands upon that statement by adding, “the City will make no data available to law enforcement agencies through this process that is not already available to them from operators now.” If a law enforcement agency seeks access to trip data collected by LADOT in its course and scope of regulating privately owned, for-profit dockless operators, that law enforcement agency would need a warrant presented in a form consistent with CalECPA.

LADOT has a responsibility to protect individual privacy and promote a transportation system free from discrimination and the exploitation of personal mobility data. LADOT’s policies reflect this responsibility, and represent a national best practice balancing individual rights to privacy with the public’s interest in a safe, accessible, equitable, and sustainable transportation system. As the regulator of dockless mobility for the City of Los Angeles, LADOT will continue to strike this balance without sacrificing its ability to manage the public right of way to benefit the residents of Los Angeles.

Existing permit requirements

LADOT requires all dockless operators to provide information compliant with the Mobility Data Specification (MDS). LADOT uses this information to enforce regulatory compliance with the City’s Dockless Mobility Pilot. Given CalECPA’s clear intent to restrict law enforcement from unwarranted access to communications data, this regulatory action is not subject to its provisions. Accordingly, all existing permit requirements, including MDS, remain in effect.

SJR:mr

Attachment

CITY OF LOS ANGELES

CALIFORNIA

Seleta J. Reynolds
GENERAL MANAGER



ERIC GARCETTI
MAYOR

DEPARTMENT OF TRANSPORTATION
100 South Main Street, 10th Floor
Los Angeles, California 90012
(213) 972-8470
FAX (213) 972-8410

April 12, 2019

SUBJECT: LADOT DATA PROTECTION PRINCIPLES

The City of Los Angeles Department of Transportation (LADOT) works to deliver a safe, livable, and well-run transportation system throughout the region. Our vision is for all people in Los Angeles to have access to safe and affordable transportation choices that treat everyone with dignity and support vibrant, inclusive communities. As we work to achieve our responsibilities of safety, congestion relief, equity, and sustainability, we also have a responsibility to protect individual privacy and promote a transportation system free from discrimination and the exploitation of personal mobility data.

The Mobility Data Specification (MDS)¹ is designed to process vehicle data minimally necessary for our stated goals and to apply strong privacy protections and security protocols. For example, we categorize this data as Confidential under the City of Los Angeles Information Handling Guidelines -- which exempts the data from the California Public Records Act² -- and we apply strong access controls and de-identification measures to the data.

As part of its Dockless Mobility permitting process, the City of Los Angeles requires Mobility Service Providers (Operators) operating on the streets of Los Angeles to comply with the MDS. Such permitting rules set a consistent standard for the transfer, use, and protection of vehicle data from Operators to LADOT.

LADOT will apply the following data protection standards to all data obtained from Operators to carry out the City's and the Department's data protection responsibilities:

- 1) *Data categorization*: LADOT designates raw trip data as Confidential Information under the City of Los Angeles Information Technology Policy Committee (ITPC) Information Handling Guidelines. This long-standing policy for the City of Los Angeles governs the obligations of the City to protect all manners of data under its control. LADOT will withhold this Confidential Information as exempt from release under the California Public Records Act.

¹ <https://github.com/CityOfLosAngeles/mobility-data-specification>

²

https://static1.squarespace.com/static/57c864609f74567457be9b71/t/5bd2165471c10bf711f24edc/1540494932514/Information_Handling_Guidelines.pdf

- 2) *Data minimization*: LADOT will mandate data sets solely to meet the specific operational and safety needs of LADOT objectives in furtherance of its responsibilities and protection of the public right of way.
 - a. *Aggregation, obfuscation, de-identification, and destruction*: Where possible, LADOT will aggregate, de-identify, obfuscate, or destroy raw data where we do not need single vehicle data or where we no longer need it for the management of the public right-of-way.
 - b. Methodologies for aggregation, de-identification, and obfuscation of trip data will rely on industry best practices and will evolve over time as new methodologies emerge.
- 3) *Access limitation*: LADOT will limit access to raw trip data related to vehicles and vehicle trips to what is required for our operational and regulatory needs as established by the City Council.
 - a. Law enforcement and other government agencies, whether local, state, or federal will not have access to raw trip data other than as required by law, such as a court order, subpoena, or other legal process. To be clear, the City will make no data available to law enforcement agencies through this process that is not already available to them from Operators now.
 - b. Similarly, the City will only allow access to raw trip data by contractors under the LADOT Third Party Master Data License Agreement which explicitly limits the use of raw trip data to purposes directed by LADOT and as needed for LADOT's operational and regulatory needs. LADOT will prohibit use of raw trip data for any non-LADOT purposes, including for data monetization or any third party purpose.
 - c. After completion of the Dockless Mobility Pilot, LADOT will create a publicly accessible transparency report discussing the types of third party requests for Dockless Mobility data that LADOT has received and how we have responded to those requests.
- 4) *Security*: The City will enact appropriate administrative, physical, and technical safeguards to properly secure and assure the integrity of data.
 - a. Los Angeles' formal information security program and the comprehensive set of security protections and standards established by the City will govern this data as it does all other city data, including but not limited to security incident and emergency response reporting.³
 - b. The City will conduct ongoing security testing to audit and improve security protections, consistent with the City of Los Angeles' information technology policies and practices.
- 5) *Transparency for the public*: The public deserve a clear description of the data used by LADOT and the ways such data is pertinent to the responsibility of protecting the public right-of-way. To that end, LADOT will publish a list of the data types collected via the MDS and the length of time that data is retained.

³ The current version is *City of Los Angeles Information Security Policy Manual* dated March 8, 2017.

- a. The City of Los Angeles shares certain information with the public to increase transparency, accountability, and customer service and to empower companies, individuals, and non-profit organizations with the ability to harness a vast array of useful information to improve life in our city.
- b. We share data via the City of Los Angeles [Open Data Portal](#). Before we publish any Dockless Mobility data to the Open Data Portal, LADOT will ensure the data is de-identified in accordance with established data protection methodologies.
- c. LADOT will not release any Dockless Mobility data on the Open Data Portal until data de-identification and destruction treatments are implemented.

