Data Collection for Emerging Mobility Services and Technologies

John I. Kennedy
San Francisco City Attorney’s Office
May 9, 2019
The New Mobility Players
Data, Data, Data

As a transportation planner, imagine a world where you have access to all stationless bikeshare and electric scooter geolocation trip data from the moment that a device is unlocked, including which city streets and sidewalks it travels on, how long it is used for, and where it is ultimately locked and parked. For all trips taken in your locality – and in real-time.
What is “MDS”?  

• APIs providing data reporting specifications developed by LA DOT (and used by a substantial number of other cities and public agencies) which allow cities to gather, analyze and compare real-time data, such as geolocation and other data, from individual trips taken by dockless scooters and electric bikes authorized to operate in the jurisdiction.

• Intended to standardize the trip data collected and reported by scooter/electric bike operators to public agencies.

• Intended to eventually expand to include real-time data reporting on TNC, car-sharing, and autonomous vehicle trips in the future.
This all sounds amazing....

What’s the catch?
The Concern: Data Collection and User Privacy
“De-Identified Data”

• Raw data that is reported to cities using MDS is “de-identified” meaning that no personal information regarding the scooter or bike user is reported - including the user’s name, home address, or other personally-identifiable information.

• There are various standards for classifying data as “de-identified” including the California Consumer Privacy Protection Act. However, if the CCPA does not apply, there is no existing legal standard which determines whether data has been sufficiently “de-identified.”

• Scooter and bikeshare companies’ privacy policies inform users that trip data which has been aggregated and/or de-identified can be used for any purpose and also shared other third parties. Users consent to these privacy policies in order to use their services.
User Privacy

• The collection and reporting of de-identified data to public entities via MDS raises concerns about individual privacy including whether the data must be disclosed in response to public records requests.

• The California Constitution recognizes an individual’s right to personal privacy and the California Public Records Act provides that the right to personal privacy sometimes precludes disclosure of personal information in response to public records requests.

• However, since the data has been “de-identified” and there is no existing law on point, it is unclear whether a city could justifiably withhold it from public release notwithstanding the fact that this data could be used to “re-identify” personal information about users.
Suggestions for Protecting User Privacy

• Minimize the amount of raw data that your agency receives and/or aggregate the data as quickly as possible.
• Pursue local or state legislation that exempts this data from public disclosure in response to public records requests.
• Alternatively, consider local or state legislation to limit the data or other information that mobility services can collect and release to third parties, including public agencies, regarding individual trips.
• Consider proactive steps to reduce the risk of a potential data breach.
Thank you!