# Scooters, Rideshares, and Taxis: Is Your Ride Private? Mobility Data Specification and its Impact on Victim Safety

## Overview

Survivors of domestic violence, sexual violence, and stalking endure trauma that often remains unseen by society, experiencing pain and fear that few can understand and that often has a lifelong impact. Communities have worked tirelessly over several decades to create supportive resources for victims, and while there are many success stories, the threats survivors face are constantly evolving. This is particularly true in the digital age, when technological advancements create new avenues for abusers to misuse to stalk, harass, or harm others. That is why it's important for technology based companies and public officials to consider and understand the threats survivors face related to technology, and work to ensure products and services are built and used in ways that do not compromise their privacy and safety. An emerging area of concern for survivor privacy is the development and use of Mobility Data Specification (MDS).

## What is Mobility Data Specification?

This technology was initially designed for the Los Angeles Department of Transportation as a way to track and monitor autonomous cars. But the city soon decided to also use the technology to help the city and regulators understand and manage traffic from the rapid influx of new vehicles in the micromobility industry – e.g. companies that have launched hundreds of user-operated, shareable, lightweight vehicles like scooters, bikes, and electronic skateboards into many cities for short-distance travel. The use of the technology has been expanding to related gig-economy industries like rideshares, and is starting to be implemented in cities across the country, including Chicago, Portland, Santa Monica, Seattle and Washington, D.C.

MDS is a data language used by cities to communicate with connected vehicles. It was designed to give city governments a way to analyze and regulate the many types of micromobility, gig-economy, taxi, and autonomous vehicle traffic operating within their boundaries. MDS currently works through three programs, or Application Programming Interfaces (APIs):

- The Provider API allows regulators to look up *historical* information (after the trip has concluded) about the start point, end point, duration, distance, route, and cost of a trip of a specific vehicle.
- The Agency API allows regulators to access *precise, real-time* vehicle locations, and enables cities to instantly send instructions to vehicle operators. For example, it could allow cities to reroute cars or prohibit access to certain neighborhoods in an attempt to improve traffic flow.
- The Policy API allows regulators to set and send policy guidance about specific locations, like speed limits, off-limit areas, and create caps on the numbers of vehicles in certain areas to ensure equitable distribution of access.

In 2018, Los Angeles began requiring micromobility companies with city permits to share real-time status information through MDS about their dockless bikes and scooters. Officials have stated they intend to expand MDS to other modes of transportation, like the cars used in rideshares.

**What is at Stake?**

**Victim Privacy:**

While MDS doesn't collect personal details like names and addresses, it would be relatively easy to piece together the data elements it does collect and use them to figure out who someone is. That means MDS could be used to identify and track individual riders (victims), revealing sensitive information like their home address, work, relationships, travel habits, and more.

Currently, city planners are required to disclose very little about their data collection and protection practices. They rely largely on self-regulation, and many have started to implement MDS systems without seeking input from impacted residents and stakeholders like victim advocates and survivors themselves. Perhaps worse, they haven't set clear policies to govern how MDS data is used, shared, stored, or secured. This means there are few protections in place to keep those who have access to MDS data from abusing the system and using it to stalk and harm an intimate partner. Such

acts of malicious access to data has been well documented by big tech companies and governments alike, including Uber, Facebook, and the NSA. Even if regulatory employees act with the soundest moral code, there is no foolproof way to keep MDS data from falling into the hands of bad actors and those who might cause riders harm when it is transferred or leaked, as witnessed by frequent reports of municipal data breaches.

**Victim Safety:**

For those affected by domestic or sexual violence, keeping personal information secure is vital. No survivor should have to face the anxiety of knowing their location data could be accessed by someone who wishes to harm them. The use of MDS APIs without ample privacy protections and security protocols puts survivors of domestic violence, sexual violence and stalking at increased risk for further violence. The Electronic Frontier Foundation and the ACLU have both expressed serious concerns about this, and have filed lawsuits challenging the constitutionality of the use of the technology. And because MDS APIs can collect real-time location information, not just historic travel data, the Center for Democracy and Technology (CDT) has further warned, "It also means that criminals and others who wrongly access information will have a much greater range of options for harm. Stalkers can intercept a rider."

*To learn more about our work related to MDS and the CARS Coalition, reach out to us at safetynet@nnedv.org. To learn more about the CARS Coalition, including the status of MDS in your area, please contact CARS at keeley@stopridersurveillance.com.*

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials, or contact us with any follow up questions.

 Supported by US DOJ-OVW Grant #2016-TA-AX-K064. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.