



Protecting Customer Privacy in Mileage-Based User Fee Collection

Mileage-based user fees are emerging as a replacement for gas taxes to ensure user-supported road funding remains viable as the vehicle fleet becomes increasingly fuel efficient and eventually electrifies. Policymakers and the public have expressed concerns about road user privacy in mileage fee systems, especially those that involve a location-based component. Fortunately, protecting the privacy of location-based mileage fee customers is a solvable problem with practical technology and policy solutions.

How the Global Positioning System (GPS) Works

- GPS satellites broadcast radio signals that transmit their locations and the precise time from onboard atomic clocks.
- A GPS receiver detects these signals and uses the time of arrival to calculate its distance from a GPS satellite.
- Using the distance calculations from at least four GPS satellites, a GPS receiver can determine its position (longitude, latitude, altitude) and time.
- Because GPS signals are sent one-way from the satellites and location is calculated by the GPS receiver using multiple satellites, GPS by itself cannot be used to track the location of a GPS receiver.
- Privacy concerns only arise when a GPS receiver is paired with a secondary wired or wireless communications system that can transmit location information computed and stored locally on a GPS receiver.
- Privacy and data security considerations should thus be focused on those secondary communications systems.

Addressing Location-Based Mileage Fee Privacy Concerns

In location-based mileage fee systems, policies should be implemented that ensure customers' personally identifiable location data are protected. These include:

- Storing all location data on board vehicle computers, transmitting only mileage-count information for revenue-collection purposes.
- Strict data retention policies that destroy stored onboard location data after a set interval, upon completion of any customer billing disputes or audits.
- The use of trusted third-party payment processors that operate as intermediaries between customers and government revenue agencies.
- Requiring a court order based on probable cause in an authorized criminal investigation before granting law enforcement access to onboard location data.

Recommendation: Customer privacy protection and data security should be thoroughly investigated during mileage-based user fee pilot programs.

Reason Foundation Transportation Policy Contacts

Adrian Moore, Vice President of Policy

(adrian.moore@reason.org)

Marc Scribner, Senior Transportation Policy Analyst

(marc.scribner@reason.org)

Reason Foundation is a national 501(c)(3) public policy research and education organization with expertise across a range of policy areas, including public sector pensions, transportation, infrastructure, education, and criminal justice. For more information about Reason Foundation, visit reason.org

