Photo Source: USDOT

CONNECTED VEHICLES AND YOUR PRIVACY

Connected vehicles communicate wirelessly with other vehicles and our roads, sharing important safety and mobility information and generating new data about how, when, and where vehicles travel. The unprecedented level of data generated will be the basis for a multitude of innovative applications that can help prevent crashes and save lives, improve mobility, and enhance our overall livability. However, this information sharing among and data collection from your vehicles have led to concerns about personal privacy.

The U.S. Department of Transportation (USDOT) is committed to ensuring that connected vehicle technology preserves personal privacy and the system protects against unauthorized access. The vehicle information communicated does not identify the driver or vehicle, and technical controls have been put in place to help prevent vehicle tracking and tampering with the system.

Connected Vehicle Overview

Connected vehicles use secure wireless technology to communicate with other vehicles of all types; advanced roadside infrastructure such as traffic signals, work zones, toll booths, and school zones; and personal mobile devices—sharing information about their position, speed, brake status, and more. This communication enables the vehicles to sense the environment around them and issue warnings and recommendations to drivers accordingly. For example, apps could warn drivers of impending collisions, icy roads, dangerous curves, and long queues ahead—before the drivers are aware of them.

The vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications will enable safety, mobility, and environmental advancements that current technologies are unable to provide. The technology is expected to reduce unimpaired vehicle crashes by 80 percent, while also reducing the 6.9 billion hours Americans spend in traffic annually.

The USDOT has been researching and testing this system of communicating vehicles for over a decade. The connected vehicle environment that is being researched is based on dedicated short-range communication (DSRC), which is a wireless technology that has more security and privacy protections than traditional Wi-Fi.

Connected vehicle safety applications require that the wireless devices in motor vehicles send and receive a basic safety message (BSM) containing information about vehicle position, heading, speed, and more relating to vehicle state and predicted path. The BSM, however, ***contains no personally identifying information*** (PII) and is broadcast in a very limited geographical range, typically less than 1 kilometer. Nearby motor vehicles will only use that information to warn drivers of crash-imminent situations.

Photo Source: USDOT


Photo Source: USDOT

U.S. Department of Transportation

Privacy Up Front

The V2V system that the Department has been developing, along with several research partners, is designed with privacy in mind. No personal vehicle identification will be collected, broadcasted, or shared. The Department is pursuing the deployment of connected vehicle technologies in a manner that protects consumers from unwarranted privacy risks and safeguards the system from unauthorized access.

Facts about Privacy and the Connected Vehicle System

V2V technologies do not pose a significant threat to privacy and have been designed to help protect against vehicle tracking:

- The V2V system will not collect or store any personally identifiable information about individuals or vehicles.
- The safety messages exchanged by vehicles cannot be used by law enforcement or private entities to identify a speeding or erratic driver.
- The V2V system will not permit tracking through space or time of specific owners, drivers, or passengers.
- Third parties attempting to use the V2V system to track a vehicle would find it extremely difficult to do so, particularly in light of simpler and cheaper means available for that purpose.
- The V2V system will not collect financial information, personal communications, or personally identifiable information about individuals or vehicles. It will enroll V2V-enabled vehicles automatically, without collecting any information identifying specific vehicles or owners.
- The V2V system will not provide a "pipe" into the vehicle for extracting data. It will enable the National Highway Traffic Safety Administration (NHTSA) and motor vehicle manufacturers to find lots or production runs of potentially defective V2V equipment without use of VIN numbers or other information that could identify specific drivers or vehicles.

As designed, the Department is confident that the connected vehicle system will both achieve the agency's safety goals and protect consumer privacy appropriately.

How to Preserve Privacy in a Connected Vehicle Environment?

Physical Controls: Physical protection around equipment such as tamper-proof casings

Technical Controls: Technologies designed to protect data, such as firewalls, access management, and encryption

Administrative Controls:

- Laws and regulations regarding unauthorized collection, storage, and disclosure of data
- Fair Information Practice Principles

Photo Source: USDOT

For more information about this initiative, please contact:
Claire W. Barrett, Chief Privacy Officer
USDOT | (202) 366-8135 | privacy@dot.gov | www.its.dot.gov

FHWA-JPO-16-268