
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 vehicles and the data environment has led to concerns about personal privacy.

The U.S. Department of Transportation (USDOT) is committed to supporting the deployment of connected vehicle applications in a manner that both protects consumer privacy and promotes this important technology. To help protect driver privacy, connected vehicle messages do not directly identify you or your vehicle (as through vehicle identification number or State motor vehicle registration), or contain data that is reasonably, or as a practical matter, linkable to you. Technical controls also have been put in place to help prevent vehicle tracking and tampering with the system.

Connected Vehicle Overview

Connected vehicles use 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 as much as 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 research environment uses dedicated short-range communication (DSRC) and a message authentication strategy that provides more comprehensive 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, does not directly identify you or your vehicle and is not, as a practical matter, linkable to you. It also is broadcast in a very limited geographical range, typically less than 1 kilometer.

Photo Source: USDOT


Photo Source: USDOT

U.S. Department of Transportation

Privacy Up Front

The Department is pursuing the deployment of connected vehicle technologies in a manner that protects consumers from unwarranted privacy risks. The V2V system has been designed with privacy in mind. V2V messages do not directly identify you or your vehicle, nor do they contain data that, as a practical matter, is linkable to you.

Facts about Privacy and the Connected Vehicle System

V2V technologies have been designed to help protect consumer privacy and limit the risk of vehicle tracking:

- The V2V system will not collect or store any information directly identifying, or reasonably linkable to, individuals or their vehicles.
- The safety messages exchanged by vehicles, alone, cannot be used by law enforcement or private entities to identify a speeding or erratic driver.
- Third parties attempting to use the V2V system to track a vehicle would find it 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 information directly identifying, or reasonably linkable to, individuals or their 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.

The Department has worked to design a connected vehicle system capable of producing significant safety, environmental, and mobility benefits without unduly compromising consumer privacy.

How to Help 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 broadcast of data linked to specific individuals or vehicles
- Implementation of the Fair Information Practice Principles in connection with the deployment of V2V technologies

Photo Source: USDOT

For more information about this initiative, please contact:
Pina, Mike, Program Manager, Communications and Outreach
ITS Joint Program Office | (202) 366-3700 | Michael.Pina@dot.gov | www.its.dot.gov

FHWA-JPO-16-268 Updated April 2019