Comment from David Maxson

This comment recommends codifying and enforcing anonymization methods for maintaining privacy. Privacy is a significant issue in the universe of Big Data, not just for scofflaws operating vehicles. The rulemaking suggests that privacy is preserved, but as stated, it is naive. <<emphasis added>>

NHTSA says: "Privacy: ...The system will not collect or store any data directly <<identifying specific individuals or their vehicles>>, nor will it enable the government to do so. There is no information in the safety messages exchanged by vehicles or collected by the V2V system that <<directly identifies>> the driver of a speeding or erratic vehicle for law enforcement purposes, or to third parties. The system expected to be <<operated by private entities>>will make it difficult to track through space and time specific vehicles, owners or drivers on a persistent basis. Third parties attempting to use the system to track a vehicle would find that it requires significant resources and effort to do so, particularly <<in light of existing means>> available for that purpose... The system will enroll V2V enabled vehicles automatically, without collecting any information that <<identifies specific vehicles or owners.>> ...The system is designed to enable 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. Our research to date suggests that drivers may be concerned about the possibility that the government or a private entity could use V2V communications to track their daily activities and whereabouts. However, <<NHTSA has worked hard>> to ensure that the V2V system both achieves the agency's safety goals and protects consumer privacy appropriately." (End of Quotation)

First, the presumption is naive that only misbehaving drivers are at risk ("driver of a speeding or erratic vehicle..."). With Big Data methods, every vehicle with V2V and a permanent MAC address can be backtracked. Ubiquitous deployment of vehicles with "private" ID numbers not associated with VIN or owner, invites investment in mass applications to capture V2V MAC addresses, associate them with vehicle locations and habits, and cross-referencing to things like license plate readers, toll collections, home and work addresses, and the like.

Today, MAC addresses of personal electronics (less easily tied to individual users in moving cars) are used to anonymously calculate route transit times on highways. With fixed MAC addresses embedded in and broadcast from motor vehicles, and additional data about the motor vehicle operation being broadcast, anonymity is easily lost. Private enterprise will find a way to monetize that information as V2V and V2I technology is deployed. It must be prevented by design.

This language from a slide deck shows the standards people recognized the concern back in 2005:
<Begin Slide Excerpt>
Anonymity Concerns
A fixed MAC address would allow any given vehicle to be tracked wherever it goes
>Lack of privacy from anyone with a receiver
>Big Brother perceptions could never be alleviated
>Automatic speeding tickets
Some are in favor of them, but drivers who speed are the ones we need to encourage to keep safety equipment connected
[Submitter note, this last point shows the same narrow thinking about privacy only protecting scofflaws]
The primary purpose of 802.11p technology is to warn other drivers/vehicles
>Lack of anonymity would discourage the public from using these devices
>Vehicle manufacturers would no longer support program
>Drivers would disable devices
>Loss of public safety benefits
<End Slide Excerpt>

(from WAVE Random MAC Address - https://mentor.ieee.org/802.11/dcn/05/11-05-1628-01-000p-wave-random-mac-address-ppt.ppt)

This leads to the primary concern. Leaving implementation to numerous private parties, some could elect to save the cost of implementing a randomization feature. Others could employ application layer identification to by pass privacy at lower layers. These parties would also be in the position of building their networks to capture and sell personal information that is backtracked to vehicle owners and operators.

NHTSA should mandate anonymization of MAC address (and any other vehicle-specific identifier transmitted) including routine random revision (e.g. on vehicle startup). At the very most, and only if there is no way to otherwise manage it, the MAC address could contain a generic ID of the technology production run or model