# Vehicle-to-Vehicle Communications Tech Will Be Mandatory, say Feds

By Lucas Laursen
Posted 4 Feb 2014 | 19:41 GMT

The National Highway Traffic Safety Administration (NHSTA) will soon propose rules for vehicle to vehicle (V2V) communications on U.S. roads, it announced yesterday (http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles). The agency is now finalizing a report on a 2012 trial with almost 3000 cars in Ann Arbor, Michigan, and will follow that report with draft rules that would "require V2V devices in new vehicles in a future year."

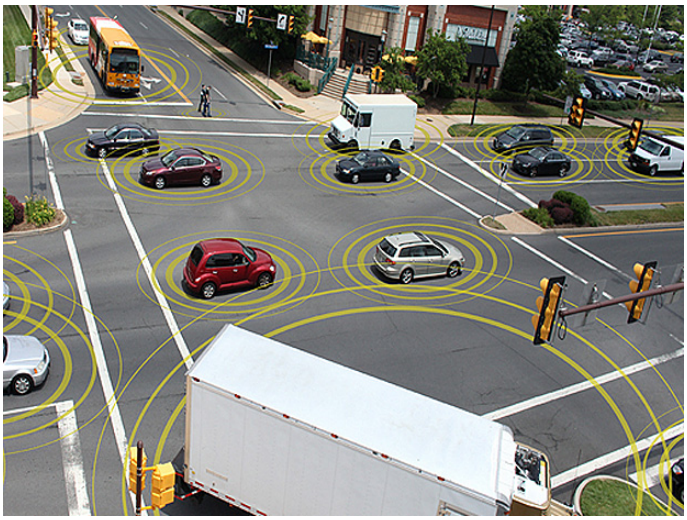

Illustration: U.S. Department of Transportation

A car changing lanes, for example, might get a warning from its V2V system that another car is fast approaching in the driver's blind spot. NHTSA, which has been researching V2V since 2002, claims that such systems could prevent three quarters of road crashes (http://www.its.dot.gov/research/v2v.htm). A public-private partnership in Europe has been testing V2V technologies since 2008, *IEEE Spectrum* reported (http://spectrum.ieee.org/green-tech/advanced-cars/car-talk) at the time.

As envisioned by NHTSA, vehicles equipped with V2V would send position and speed data to one another ten times per second over an ad hoc wireless network. Onboard computers could then calculate whether nearby vehicles are a threat and alert drivers. Future protocols might incorporate information from the sort of onboard sensors that are growing more popular among carmakers, creating a road-spanning network of sensors and alerting cars to problems up or down the road. That kind of data ubiquity would help drivers avoid one another, and is a step toward more autonomy for self-driving cars.

As usual, there are tradeoffs. The agency wrote that V2V data would not identify vehicles, but added that, "vehicles would be identifiable through defined procedures only if there is a need to fix a safety problem" without defining those procedures. That implies that some sort of identifying information is in the system.

Drivers might as well accept that modern vehicles are no more capable of protecting their personal information, including location, than are mobile phones, as a Ford executive's comments made clear (http://www.cnbc.com/id/101324749) last month. The NHTSA also notes on its V2V website (http://icsw.nhtsa.gov/safercar/ConnectedVehicles/) that, "Anonymous data from connected vehicles will be open to the public and can be used for a myriad of new safety, mobility and environmental applications." The paranoid will not take comfort in that: computer scientists have shown again (http://www.bigdata-startups.com/re-identifying-anonymous-people-with-big-data/) and again (http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html) that

identifying individuals from anonymized data is easy.

David Friedman, the NHTSA's acting administrator, put a positive spin on his announcement, writing that future generations will remember this as the moment that, "the historical arc of transportation safety considerably changed for the better." Not the smoothest of people to people communications, but then again, this is about cars.