AIRD BERLIS

SPOTLIGHT
MEDIA, SPORTS AND COMMUNICATIONS LAW BLOG

Jan 27, 2020

Connected Vehicles

By Donald B. Johnston

It's been a long time since I wrote anything on connected vehicles – it was way back in 2016. I probably even had hair in those days. So it's high time that I address the subject again.

I mentioned in my previous blog on connected vehicles that there is a tremendous amount of evidence that connected cars are bound to reduce accidents. This is not because machines are so smart; it's really because we all drive like boneheads.

You know it's true. In fact, you, gentle reader, are probably the only good driver reading this article.

There's a great McKinsey report on the subject of accident reduction that is well worth reading. They say that connected vehicle technology will save a huge number of lives and will contribute in a significant way to productivity and welfare in society. You can find the McKinsey report here. McKinsey also has a report on "autonomous" vehicle infrastructure – autonomous meaning the opposite of connected, but there is still a relationship.

Connecting Vehicles - DSRC/WAVE

DSRC stands for *Dedicated Short Range Communications* and WAVE stands for *Wireless Access in Vehicular Environments*. DSRC/WAVE is the motor vehicle communications technology that is at the root of the connected vehicle. If you want to dig a little deeper into the technology, take a look below under the heading ***Digging Deeper***. **[Note: Do not operate a motor vehicle or heavy machinery after reading. I disclaim all responsibility for accidents caused by Johnston-induced narcolepsy.]**

What are the advantages of implementing DSRC/WAVE in motor vehicles? Generally DSRC/WAVE can be used for V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) communications, and those uses open up some significant opportunities.

Traditionally, the public sector has subsidized the automotive industry by building, maintaining and policing roads. However, because the U.S. government is encouraging – and motor vehicle manufacturers are embracing – DSRC/WAVE communications technology for connecting vehicles to one another and to roadside communications technology, MaaS (mobility-as-as-service) could soon be a key part of the management of a typical 'smart' city's road networks. This gives so-called 'smart' cities the opportunity to apply the science of network economics to road network management – for road tolling, parking, traffic management, public safety and many other uses.

Not only that, but (as McKinsey argues) traffic accidents could be dramatically reduced, and lost productivity time wasted in traffic could be recovered moving forward.

DSRC/WAVE enabled vehicles and road infrastructure can support:

- Emergency (police, fire, ambulance) pre-emption
- Collision avoidance
- Interaction with traffic signals
- Managed lane access
- Electronic tolling/congestion pricing

- Park-and-walk (in other words, payment is automatic; it won't really help you walk)
- Pay-as-you-drive insurance
- Driver safety messaging
- Many other use cases

DSRC/WAVE communications technology can allow smart cities to do away with older, single-purpose technologies, like

- Parking meters
- Road tolling and parking transponders
- Optical signalling pre-emption for transit/emergency vehicle priority
- Old-fashioned intersection controllers

Because the DSRC/WAVE standard is supported, and the wireless band has been set aside, throughout North America and Europe, interoperability is guaranteed.

Automakers and their suppliers have spent a lot of money to support the DSRC/WAVE telecommunications technology, including developing standards, communications protocols, chipsets and DSRC communication modules (some new and some retrofit). Every major auto manufacturer is "in".

There is nothing intrinsically different about "self-driving" (autonomous) vehicles that makes them allergic to the DSRC/WAVE connected vehicle technology. In fact, autonomous vehicles operate best with the best possible data. DSRC/WAVE messages from other cars and from roadside infrastructure could deliver critically-important road safety information to autonomous vehicles, which those vehicles could use to more safely navigate from place to place.

Digging Deeper

In 1999, the U.S. Federal Communications Commission allocated wireless spectrum for "Intelligent Transportation Systems." A little later, the European Telecommunications Standards Institute followed suit. That wireless spectrum is dedicated to DSRC/WAVE connected vehicle solutions. The U.S. continues to promote the adoption of DSRC/WAVE through its federal Department of Transportation Intelligent Transportation Systems Joint Program Office.

DSRC/WAVE-enabled devices use IPv6. (Your home or work computer is mostly IPv4.) IPv6 makes it easy to interconnect DSRC devices, like vehicles or roadside infrastructure, to other networks. IPv6 is at the heart of the IEEE 1609 (Wireless Access in Vehicular Environments) suite of specifications pertaining to DSRC/WAVE.

The Collision Avoidance Metrics Partnership (CAMP) and the Vehicle Safety Communications (VSC) consortium (which includes the major automakers and the U.S. National Highway Traffic Safety Administration) have paid very close attention to these issues over the past fifteen years to ensure that DSRC works in a secure and safe manner, and preserves privacy. (Privacy is protected through the Security Credentials and Management System (SCMS), the IEEE 1609.2 security specification and an Elliptic Curve Digital Signature Algorithm (ECDSA), among others.)

Privacy and safety are at the very heart of all these efforts. The published initial requirements specifications in 2011 and the draft specification for SCMS implementation published in 2016 by the USDOT2345 are all about safety and privacy in the connected vehicle.

The result of all these efforts is a connected car system architecture that enables a potentially large-scale deployment of vehicular wireless networking characterized by "Privacy By Design" principles. Interfacing to a vehicle's "CAN bus" so that DSRC/WAVE-enabled SAE J2735 safety messages can be sent to the connected vehicle does not create a vulnerable cyberattack vector for internet communications with the outside world. Even if a "rogue" vehicle were somehow created through industrial sabotage at the factory

level, the SCMS system would quickly “quarantine” that vehicle because it would lack the IEEE 1609.2 security credentials needed to function. Such a non-compliant vehicle – or it could be any device interfacing with a vehicle or the infrastructure that supports vehicle-to-vehicle (V2V) technology) – would be quickly identified by other nodes in the network and denied access to services and communication.

Author

Donald B. Johnston
Partner
T 416.865.3072
djohnston@airdberlis.com