Assuring Privacy and Security in Vehicle-to-Vehicle Safety Communications

Professor Dorothy J. Glancy, Santa Clara University School of Law

Technologies that enable vehicles automatically to avoid running into each other, off the road, or over pedestrians promise welcome advances in roadway safety. Vehicle-to-vehicle technologies ("V2V") have been developed to do just that. The Federal Communications Commission has allocated the 5.9 GHz band for transportation-related Dedicated Short-Range Communications (DSRC) and assigned Channel 172 for vehicle-to-vehicle communications. The National Highway Traffic Safety Administration has announced that it will make an agency decision with regard to V2V safety applications in 2013. In the meantime, how V2V safety communications will be governed has not been determined. Not only technical savvy, but also organizational, legal, political and ethical wisdom will be essential to creating appropriate governance for V2V safety communications.

Because privacy and security concerns could jeopardize public acceptance of V2V safety technologies, governance structures will be particularly crucial for V2V safety communications. V2V safety technologies transmit a vehicle's location and operational details ten times each second. Such information about a vehicle's location and how it is operated reflects the whereabouts and behavior that vehicle's driver. Moreover, cumulative V2V safety data could enable both tracking a vehicle in real time, as well as collecting comprehensive behavioral information about all vehicles and their drivers.

Privacy and security issues regarding V2V safety communications include:

- whether participation in V2V safety communications will be voluntary, as opposed to required for all vehicles;
- how to maintain anonymity of V2V safety communications;
- how to assure that V2V safety communications are authentic and secure;
- whether V2V vehicle safety data communications will be retained for research or other uses;
- how to keep hackers from spoofing or tampering with safety communications to create roadway mayhem;
- how to keep interlopers from intercepting V2V safety communications and using them to track vehicles, drivers or passengers; and
- how to prevent V2V safety communications from becoming surveillance tools that threaten civil liberties.

Response to these privacy and security issues through appropriate governance will be crucial in determining whether the vehicle-buying public in the United States will accept V2V safety technologies.

V2V safety communications are unusual. These communications do not contain voice, text or entertainment - only data about where a vehicle is located and its operational status. Specific V2V safety data includes time, location, speed, acceleration, direction of travel, steering, braking status and other information reflecting vehicle operation. DSRC transceivers are specialized two-way radios operating at a range of about 100 meters. They transmit V2V safety data ten times a second from one vehicle to another while the vehicles are moving at highway speeds. The low latency of DSRC transmissions is critical to getting vehicle-status information from one vehicle to another in time to avoid accidents.

Legal requirements, political realities and ethical concerns about responsible corporate and government behavior will play important roles in the governance of V2V safety communications. This presentation discusses a proposed governance model for V2V safety communications that responds to privacy and security concerns in ways that will encourage public acceptance of V2V safety communications.