Published on *The National Law Review* https://natlawreview.com

The Internet of Things (Part 2): Vehicle-to-Vehicle Communications

Article By:

Barbara Murphy Melby

Christopher C Archer

Our cars will soon be talking to one another. They will send messages about their location, speed, acceleration, size, position, and turn-signal status, and they will use that information to tell us what our fellow drivers are doing on the road around us. These future cars will alert us to what we can't see coming around the corner, helping us avoid potential crashes.

Vehicle-to-vehicle (V2V) communication is an interesting example of how the Internet of Things (IoT) will soon affect our daily lives. Last week, we provided a brief introduction to the IoT in part one of this series. Part two discusses recent regulatory and industry developments related to V2V communications technology and focuses specifically on regulatory and industry responses to privacy issues.

V2V Regulations Are on the Way

The National Highway Traffic Safety Administration (NHTSA) recently initiated the regulatory process to require passenger cars and light truck vehicles to have V2V communications technology by 2019. The proposed regulations will also create minimum performance requirements for V2V devices and messages.

In its advanced notice of proposed rulemaking, and accompanying technical report, the NHTSA presented research findings conducted over 10 years with the U.S. Department of Transportation (DOT). The report contains detailed analysis of various aspects of V2V communications, including explanations on how the technology and systems would work; examinations of specific safety applications, such as left-turn assist and intersection movement assist; and discussions of important legal issues arising from V2V communications.

NHTSA Addresses Privacy Concerns

One of the central issues facing V2V communications is consumer privacy. A recent survey found that consumers are concerned about data privacy in V2V technology, with 45% of new car buyers in the United States strongly agreeing with the statement "I am reluctant to use car-related connected

services because I want to keep my privacy."

The NHTSA took this concern head on, stating in its report that "the [V2V] system will not collect or store any data identifying individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V system that could be used by law enforcement or private entities to personally identify a speeding or erratic driver." Further, the system will not enable location tracking and will not allow collection of financial information or personal communications. The NHTSA expressed confidence that "as designed…the V2V system both achieves the agency's safety goals and protects consumer privacy appropriately."

Although the NHTSA and DOT are waiting for V2V technology to develop further before performing a full privacy risk assessment, the agencies conducted an interim privacy risk assessment and concluded that they "have reason to believe that a properly-designed V2V system would curtail any serious risks to privacy," while acknowledging that "there may be no way to entirely eliminate privacy risks from the V2V system."

See Section VIII of the report for the agencies' full discussion of privacy considerations.

The FTC Announces Its Support of NHTSA's Privacy Risk Assessment

In a letter dated October 20, the Federal Trade Commission (FTC) responded to the NHTSA's request for comment on privacy issues related to V2V communications. The FTC stated that it "supports NHTSA's implementation of a deliberative, process-based approach to address privacy and security risks," finding that the risk assessment discussed in the NHTSA report included a "multi-step process of evaluating the needs served by V2V technology, identifying system functions to serve those needs, identifying the data that must be collected to serve the needs, describing and quantifying privacy risks, and identifying ways to control these risks."

The letter concluded with a statement of support for the NHTSA principle that V2V regulations should be based on the Fair Information Practice Principles (FIPPs) and should promote safety while protecting consumer privacy.

The Auto Industry Commits to Seven Privacy Principles for V2V Technology

Shortly after the FTC's letter, on November 12, certain participating members of the Alliance of Automobile Manufacturers (the Alliance) and the Association of Global Automakers (the Association) submitted a letter to the FTC announcing their commitment to seven privacy principles (the Privacy Principles) related to V2V communications technology.

The Alliance and Association noted in their letter that the Privacy Principles are based on the FIPPs and "establish a framework that automakers and other participants in the automotive industry may choose to adopt when offering innovative vehicle technologies and services."

The seven Privacy Principles stated in the letter are:

1. Transparency

2. Choice

3. Respect for Context

4. Data Minimization
5. Data Security
6. Integrity and Access
7. Accountability

More details on the seven Privacy Principles can be found here.

For part 1, click here.

National Law Review, Volume IV, Number 331

Source URL:https://natlawreview.com/article/internet-things-part-2-vehicle-to-vehicle-communications