Fordham Urban Law Journal

Volume 41
Number 5 *Symposium - Smart Law for Smart Cities: Regulation, Technology, and the Future of Cities*

Article 5

March 2016

Sharing the Road: Smart Transportation Infrastructure

Dorothy J. Glancy
Santa Clara University School of Law

SHARING THE ROAD: SMART TRANSPORTATION INFRASTRUCTURE

Dorothy J. Glancy[*]

ABSTRACT

Smart cities require smart transportation. Advanced Intelligent Transportation Systems provide ever-smarter transportation infrastructure for the United States and countries around the world. Among the most advanced forms of ground transportation infrastructure is a group of technologies that connect vehicles invisibly to other vehicles through information exchanges. These advanced transportation technologies are of two types: On the one hand, Connected Vehicle Safety Systems use vehicle-to-vehicle dedicated short range communications technologies. On the other hand, Connected Vehicle Mobility Applications use a much wider variety of mobile wireless technologies. These two types of technologies that connect vehicles will increasingly make existing physical infrastructure safer and more efficient. At the same time, these vehicle-connecting technologies confront a number of legal and policy issues, including the regulatory environment, products liability, insurance, law enforcement access, privacy, and security as discussed in this Article.

TABLE OF CONTENTS

---

[*] Professor, Santa Clara University School of Law. B.A. Wellesley College, J.D. Harvard Law School. This Article was presented on February 28, 2014 at the symposium on "Smart Law for Smart Cities: Regulation, Technology, and the Future of Cities," held at Fordham University School of Law.

INTRODUCTION

If you believe that a city's transportation infrastructure is built only of concrete, asphalt, and steel, think again. In the future, more and more ground transportation infrastructure will rely on information and communications technologies that are, for the most part, invisible and intangible.

Designed to enable ever-increasing numbers of vehicles to share limited roadways, new wireless connectivity to and from personal vehicles is among the most advanced of the smart transportation infrastructure. The new information and communications technologies discussed here help move personal vehicles along roadways as safely, efficiently, and humanely as possible. These new connected vehicle technologies are also used in commercial vehicles, such as trucks and buses. However, the earliest applications are likely to be in passenger vehicles that provide personal mobility for individuals and their families and friends. The central purpose of these new information and communications technologies is to facilitate physical movement of individual people from place to place in their daily lives while avoiding accidents and traffic congestion. A close look at these improvements to personal mobility will help illuminate how we can cooperatively share the road to make room for others.

Personal mobility—to move from one physical place to another physical place—is an important aspect of individual freedom. For the foreseeable future, the ability of an individual to change her or his physical location[1] to go to work, to seek education, to attend cultural events, and to enjoy recreational opportunities will depend primarily on personal mobility through use of a private vehicle on a physical

1. "Geolocation" is often used in this context to refer to a specific geographical place on earth, as opposed to locations in space and cyberspace. *See* ISO/IEC 19762-5:2008(EN) (Int'l Org. for Standardization and Int'l Electrotechnical Comm'n 2008), *available at* https://www.iso.org/obp/ui/#iso:std:iso-iec:19762:-5:ed-1:v1:en (last visited Dec. 11, 2014).

roadway. The new transportation infrastructures discussed here will enhance the ability of a growing number of individuals to do so safely and efficiently.

This Article begins by describing background data provided by dynamic urban transportation modeling and the intelligent transportation systems that have been developed over the past quarter century or so. Then this Article looks at vehicle communications technologies that will connect vehicles in a smart new transportation infrastructure made up of information. Two types of vehicle communications, one vehicle-oriented and the other consumer-oriented, represent different connected vehicle approaches to vehicle cooperation in ways that augment transportation's limited physical infrastructure. These two types of connected vehicle information systems operate differently. Each takes a distinctive approach to shared legal and policy issues such as regulation, liability, privacy, insurance, and other matters. This Article concludes by looking even further into the future at how these and other technologies will contribute to even more advanced transportation technologies such as driverless personal transportation.

I. URBAN TRANSPORTATION

Cities are not static. Like sharks that require a continuous stream of water through their gills, cities require transportation to carry people and goods through their streets, or they will die. The complex influence of transportation on the dynamic health and resilience of cities is a field shared these days with land and transportation planners, by modelers, mathematicians, and physicists.

Transportation metrics estimate that 4.8 billion hours are wasted annually in traffic congestion.[2] In 2013 there were 5.7 million police-reported vehicle crashes.[3] The total amount of wasted fuel topped 3.9 billion gallons in 2009 alone.[4] By making transportation infrastructures smarter, much of that environmental and human loss can be prevented. One of the connected vehicle technologies

---

2. *See* U.S. DEP'T OF TRANSP., FACT SHEET: IMPROVING SAFETY AND MOBILITY THROUGH VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY 1 (2014), http://www.safercar.gov/staticfiles/safercar/connected/V2V_fact_sheet-02032014.pdf.

3. *See* U.S. DEP'T OF TRANSP., TRAFFIC SAFETY FACTS: 2013 MOTOR VEHICLE CRASHES: OVERVIEW 3 (2014), http://www-nrd.nhtsa.dot.gov/Pubs/812101.pdf.

4. *See* U.S. DEP'T OF TRANSP., *supra* note 2, at 2.

discussed in this Article is expected to avoid eighty percent of vehicle crashes involving non-impaired drivers.[5]

In their optimistically titled *A Unified Theory of Urban Living*, Geoffrey West and Luis Bettencourt created mathematical models to try to understand the deep complexity of modern urban areas.[6] They theorized that, like biological organisms, cities are at once defined and confined by their infrastructure.[7] Part of that infrastructure is, of course, the transportation grid. Using census data, Bettencourt and West determined that when a city increases in size by 100% (i.e., doubles in size), it requires an increase in resources of only about 85%.[8] The 15% bonus reflects what urban economists call "agglomeration economies"—a combination of economies of scale and network effects—that make urban areas so dynamic.[9] On the other hand, there are also "diseconomies of agglomeration," such as traffic congestion, crime, and pollution.[10] As cities grow in size, there appears to be an increase in social problems, such as traffic congestion, crime, noise, and pollution in a roughly proportionate relationship to the growth in productive output and innovation.[11] The smart transportation technologies discussed here seek to ameliorate traffic congestion and prevent vehicle crashes commonly associated with urban transportation.

In *The New Science of Cities*, Michael Batty uses urban simulation models to better understand the complex interplay between location in physical space and network flows. Batty's models explore relationships between people and places, as well as between different locations and activities within a city.[12] A geographer by training, Batty emphasizes the importance of the highly complex network flows between and among nodes of particular human activities that characterize cities.[13] Batty suggests that there is an intrinsic order of

---

5. *See id.* at 1.

6. *See* Luis Bettencourt & Geoffrey West, *A Unified Theory of Urban Living*, 467 NATURE 912 (2010), *available at* http://www.nature.com/nature/journal/v467/n7318/full/467912a.html; *see also* Jonah Lehrer, *A Physicist Solves the City*, N.Y. TIMES MAG., Dec. 17, 2010, http://www.nytimes.com/2010/12/19/magazine/19Urban_West-t.html.

7. *See* Bettencourt & West, *supra* note 6, at 12–13; *see also* Lehrer, *supra* note 6, at 4.

8. *See* Bettencourt & West, *supra* note 6, at 12.

9. *See* JAN BRUECKNER, LECTURES ON URBAN ECONOMICS 2–10, 20 (2011).

10. *See* Luís M. A. Bettencourt et al., *Growth, Innovation, Scaling, and the Pace of Life in Cities*, 104 PROC. NAT'L ACAD. SCI. 7301 (2007).

11. *See* Bettencourt & West, *supra* note 6, at 913.

12. *See generally* MICHAEL BATTY, THE NEW SCIENCE OF CITIES (2013).

13. *See id.* at 1–3.

scale that determines a city's form and how it functions.[14] Despite certain predictable results of scaling up in size, the growth of cities takes the form of nonlinear dynamics. Because the dynamics of city growth change constantly, a growing city is unlikely to reach a static equilibrium.[15] Batty's mathematical urban simulations indicate that the multifaceted nonlinear dynamics of cities keeps urban areas in a constant state of disequilibrium.[16] As a result, the characteristic nonlinear dynamics of urban areas, including their transportation systems, make predicting and controlling cities daunting.[17] One strategy for coping with urban disequilibrium in transportation is the development of better infrastructure such as the new connected vehicle information systems discussed in this Article.

In a similar vein to Batty's research, Marc Barthelemy and Rémi Louf—two French physicists—recently modeled information regarding roughly 9000 United States cities and towns between 1994 and 2010.[18] Their analysis indicates that traffic congestion causes cities to splinter and to generate suburbs (subcenters): "as a city grows and congested roadways make it increasingly difficult to get to the center, subcenters emerge along the outskirts."[19] They explain that:

> While agglomeration economies seem to be the basic process explaining the existence of cities and their spectacular resilience, this study brings evidence that congestion is the driving force that tears them apart. The nontrivial spatial patterns observed in large cities can thus be understood as a result of the interplay between these competing processes.[20]

They note that "the number of activity subcenters in urban areas scales sublinearly with their populations . . . ."[21] In other words, the growth in the number of suburbs tends to be slower than a city's population growth. Still, many people ultimately move out of the city center, and then they move their businesses or workplaces out to be nearer to where they live. Of course, they make these moves after they have put up with being stuck in traffic for a while. Connected

---

14. *See id.* at 119.
15. *See id.* at 123.
16. *See generally id.*
17. *Cf. id.* at 3, 271 (discussing the complex "science of cities").
18. *See generally* Rémi Louf & Marc Barthelemy, *Modeling the Polycentric Transition of Cities*, PHYSICAL REV. LETTERS, 198702-1 (2013).
19. Sarah Fecht, *The Traffic Effect*, SCI. AM., Feb. 2014, at 17 (2014).
20. Louf & Barthelemy, *supra* note 18, at 198702-4.
21. *Id.* at 198702-3.

vehicle technologies are designed to make more efficient use of existing roads and highways, and to alleviate traffic congestion that otherwise tends to tear cities apart.

In imagining future cities, transportation has always played an important role. A well-known example is Le Corbusier's *Ville Contemporaine* (or Contemporary City), unveiled in 1922.[22] Transportation routes were at the heart of *Ville Contemporaine*, which was organized around a multimodal transportation hub that interconnected buses, trains, and highways.[23] Around the *Ville Contemporaine*'s transportation hub, Le Corbusier placed his famous sixty-story cruciform skyscrapers, clad in walls of glass and set on rectangular green spaces.[24] In just about any imaginable utopia[25] or dystopia[26] people have to get from one geographical location to another. That requires transportation.

Of course, transportation—in the sense of geographical movement from location to location—might not be necessary in the future Mirror Worlds forecasted by David Gelernter.[27] In *Mirror Worlds*, digital reflections representing the reality of nearby or faraway places, or even transportation flows, may be experienced without having to physically move from one's computer.[28] That is part of Gelernter's point about the potential for delocalizing information in future Mirror Worlds. However, at least for now, transportation from one physical location to another is a key part of everyday life for most people. Even someone who "works from home" (telecommutes), and orders everything needed for life and work from online suppliers, depends on transportation for delivery of goods, some services (such as computer repair), clothing, and food necessary to sustain life.

---

22. *See* STANISLAUS VON MOOS, LE CORBUSIER: ELEMENTS OF A SYNTHESIS 196 (MIT Press 1979); *see also* RICHARD PADOVAN, TOWARDS UNIVERSALITY: LE CORBUSIER, MIES AND DE STIJL 193 (Routledge 2002).

23. *See* PADOVAN, *supra* note 22, at 193.

24. *See* Francesco Passanti, *The Skyscrapers of the Ville Contemporaine*, ASSEMBLAGE, Oct. 1987, at 52, 61–62.

25. *See, e.g.*, THOMAS MORE, UTOPIA (New York, The Heritage Press 1935); B. F. SKINNER, WALDEN TWO (Macmillan Publ'g Co. 1976).

26. *See, e.g.*, ALDOUS HUXLEY, BRAVE NEW WORLD (Harper & Row 1946); GEORGE ORWELL, 1984 (Penguin Grp. 2003).

27. DAVID GELERNTER, MIRROR WORLDS: OR THE DAY SOFTWARE PUTS THE UNIVERSE IN A SHOEBOX...HOW IT WILL HAPPEN AND WHAT IT WILL MEAN (1st ed. 1991).

28. *See generally id.*

In *Smart Cities*, Anthony Townsend foresees the promise and peril of digitally-planned and computer-managed cities of tomorrow.[29] Townsend refers to "smart" cities in the sense of being connected, both internally and externally, by ubiquitous computing.[30] Publicly available wireless information systems enable smart city connectivity. In addition, smart cities also use wireless networks to coordinate physical transportation that moves people and goods efficiently from one place to another.[31] Everywhere in smart cities, information technologies shape and guide transportation, as Townsend's numerous examples from Rio de Janeiro to Barcelona demonstrate so well.[32] Townsend expects an increasingly intense "symbiotic relationship between cities of tomorrow and information technology."[33]

This Article explores in depth one specific transportation-related aspect of what Townsend describes as "the intersection between urbanization and the ubiquitous digital technology that will shape our world and how we will live in it."[34] For Townsend, transportation is only part of his picture of present and future smart cities. Being smart about urban transportation will require new technologies that will enable increased use of existing physical infrastructure more efficiently and with greater safety.

II. INTELLIGENT TRANSPORTATION SYSTEMS

The transportation sector of smart cities includes a wide range of technologies known collectively as "Intelligent Transportation Systems," or sometimes just "ITS." The connected vehicle technologies that are the focus of this article are among the most advanced ITS currently under development in the United States.

For more than three decades, various applications of ITS have contributed to the safety, mobility, and convenience of transporting people and goods from one place to another—not only into and out of cities, but also within cities.[35] The United States transportation

---

29. ANTHONY M. TOWNSEND, SMART CITIES: BIG DATA, CIVIC HACKERS, AND THE QUEST FOR A NEW UTOPIA (2013).

30. *Id. passim.*

31. *Id.* at 98–107.

32. Townsend explores smart transportation systems in Rio de Janeiro, Brazil, *id.* at 66–69, 90–92, and Barcelona, Spain, *id.* at 43.

33. *Id.* at 4.

34. *Id.*

35. *See, e.g.*, RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., INTELLIGENT TRANSPORTATION SYSTEMS (ITS) STANDARDS PROGRAM STRATEGIC PLAN FOR 2011–2014, at 4 (2011), *available at* http://www.its.dot.gov/

sector turned its attention to ITS in 1991, when Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA).[36] The ISTEA established a federal program to research, develop, and operationally test what were then called "Intelligent Vehicle Highway Systems" (IVHS) and to promote their implementation.[37] The program's purpose was to facilitate deployment of information and computer technology to enhance the efficiency, safety, and convenience of surface transportation.[38] Among the statute's intended results were improving access, saving lives and time, and increasing productivity.[39] In 1994, what started out as IVHS was renamed "Intelligent Transportation Systems" to match the name used in the rest of the world.[40] For more than three decades, many types of ITS have been developed and deployed, from anti-lock brakes to electronic stability control and on to adaptive cruise control and the connected vehicle technologies discussed here.

ITS technologies are a transportation feature not only of the United States, but also of many other nations. A yearly ITS World Congress gathers over ten thousand ITS suppliers, researchers, and users from all over the world.[41] In addition to United States corporations and agencies, major suppliers of ITS technologies are

---

standards_strategic_plan/stds_strat_plan.pdf ("Intelligent Transportation Systems (ITS) can be defined as the application of advanced information and communications technology to surface transportation in order to achieve enhanced safety and mobility while reducing the environmental impact of transportation. The addition of wireless communications offers a powerful and transformative opportunity to establish transportation connectivity that further enables cooperative systems and dynamic data exchange using a broad range of advanced systems and technologies."). For further background information, see the *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, an eighteen-year-old publication that provides current information about ITS applications.

36. Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, 105 Stat. 1914 (codified as amended in scattered sections of U.S.C.). This statute was the general authorizing legislation for funding surface transportation programs administered by the United States Department of Transportation.

37. *See id.* at § 6052(a) (providing that "the Secretary shall conduct a program to research, develop, and operationally test intelligent vehicle-highway systems and promote implementation of such systems as a component of the Nation's surface transportation systems").

38. *See generally id.*

39. *See generally id.*

40. *Road Transportation Informatics,* JPL'S WIRELESS COMMUNICATION REFERENCE WEBSITE, http://www.wirelesscommunication.nl/reference/chaptr01/roadtrin/ivhs.htm (last visited Dec. 2, 2014).

41. The theme of the 2014 ITS World Congress was "Reinventing Transportation in our Connected World." It featured some of the connected vehicle technologies described in this Article.

located in Europe, Japan, South Korea, and Singapore.[42] Since 1992, the International Standards Organization has developed international guidelines regarding "[s]tandardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field."[43]

Many definitions have tried to capture the essence of ITS since they launched in the early 1990s. Perhaps the most succinct description is that adopted by the Federal Highway Administration within the United States Department of Transportation (USDOT): "Intelligent Transportation System (ITS) means electronics, communications, or information processing used singly or in combination to improve the efficiency or safety of a surface transportation system." [44] Elsewhere within the USDOT, the Research and Innovative Technology Administration (RITA) has defined ITS as:

> [T]he application of advanced information and communications technology to surface transportation in order to achieve enhanced safety and mobility while reducing the environmental impact of transportation. The addition of wireless communications offers a powerful and transformative opportunity to establish transportation connectivity that further enables cooperative systems and dynamic data exchange using a broad range of advanced systems and technologies.[45]

ITS technologies include three types of technologies: those associated with roadway infrastructure, those associated with vehicles, and those that provide integrations between vehicles and infrastructures. Currently, the most familiar ITS technologies include electronic toll collection, in-vehicle navigation systems, automatic parking systems, and dynamic message signs.

---

42. *See* STEPHEN EZELL, INFO. TECH. & INNOVATION FOUND., EXPLAINING INTERNATIONAL IT APPLICATION LEADERSHIP: INTELLIGENT TRANSPORTATION SYSTEMS 1, 20–35 (2010), *available at* http://www.itif.org/files/2010-1-27-ITS_Leadership.pdf. For additional discussions of ITS research and developments, see the *International Journal of Intelligent Transportation Systems Research*.

43. *See ISO/TC 204 Intelligent Transportation Systems*, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/iso/iso_technical_committee?commid=54706 (last visited Dec. 2, 2014).

44. 23 C.F.R. § 940.3 (2014).

45. RESEARCH & INNOVATIVE TECH. ADMIN., *supra* note 35.

USDOT explains that the purposes of ITS are to "improve[] transportation safety and mobility and enhance[] American productivity through the integration of advanced communications technologies into the transportation infrastructure and in vehicles. Intelligent transportation systems (ITS) encompass a broad range of wireless and wire line communications-based information and electronics technologies."[46]

At present, the centerpiece of ITS technologies is USDOT's Connected Vehicle Program.[47] This program encompasses several types of technologies designed to connect vehicles to each other, to roadside infrastructure, and to the world beyond transportation—at least to the World Wide Web.[48] The Connected Vehicle Program is the source of the invisible transportation infrastructure that is about to transform urban transportation in the United States from simply concrete, steel, and asphalt into a much smarter, interactive digital information-based system.

Connected vehicle technologies combine communications, internal vehicle sensors, roadway sensors, and analytic technologies to connect vehicles with other vehicles and with the roadway environment. To enable future vehicles to share the road with greater safety and efficiency, two quite different types of vehicle connections, discussed below, provide a variety of interconnected transportation

---

46. *About ITS: List of FAQs*, RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/faqs.htm (last visited Dec. 2, 2014). Sometimes the purpose of ITS is more succinctly stated as to "improve surface transportation safety and mobility and contribute to America's economic growth." RESEARCH & INNOVATIVE TECH. ADMIN., *supra* note 35.

47. *See Challenges and Future of Federal Surface Transportation Research: Hearing Before the Subcomm. on Research & Tech. of the H. Comm. on Sci., Space and Tech.*, 113th Cong. (2014) (statement of Gregory D. Winfree, Assistant Secretary for Research and Technology, United States Department of Transportation) [hereinafter *Surface Transportation Hearing*] (emphasizing the importance of USDOT's Connected Vehicle program as one of the most active and promising of the ITS technology research efforts). Underscoring the centrality of connectedness to USDOT ITS technology research, the most recent Progress Update of the ITS Strategic Research Plan carries the title "Transforming Transportation through Connectivity." RESEARCH & INNOVATIVE TECH. ADMIN., *supra* note 35.

48. *See generally Connected Vehicle Technology,* RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/landing/cv.htm (last visited Dec. 2, 2014) (providing information about the USDOT Connected Vehicle program); *Regulation & Policy*, FED. HIGHWAY ADMIN., U.S. DEP'T OF TRANSP., http://ops.fhwa.dot.gov/travelinfo/resources/policy.htm (last modified July 30, 2014) (providing extensive information about connected vehicle initiatives within USDOT); *Vehicle-to-Vehicle Communications,* NAT'L HIGHWAY SAFETY ADMIN., http://www.safercar.gov/v2v/index.html (last visited Dec. 2, 2014) (providing information about USDOT connected vehicle initiatives).

infrastructures. These advanced transportation technologies will enable transportation infrastructure to accommodate more people, goods, and services more safely while using roughly the same physical transportation resources.

III. CONNECTED VEHICLE TECHNOLOGIES

Perhaps because vehicle communications involve technologies from various disciplines (from computer science to wireless networks and software applications) the terminology used in discussing communications to and from connected vehicles lacks precision. "Telematics," in the most general sense, refers broadly to the "conjunction of computers and telecommunication devices . . . ."[49] Sometimes "telematics" is also used to refer to wireless communications associated with a vehicle.[50] Regrettably, a stable definition of telematics seems unlikely in the near future.

The USDOT has not helped to provide consistent definitions of connected vehicle communications. What are now the Vehicle-to-Vehicle (V2V) data-exchange aspects of the USDOT's Connected Vehicle Program has morphed from Vehicle Infrastructure Integration (VII) to the short-lived "IntelliDrive℠" brand to the current usage of V2V, V2I (for Vehicle-to-Infrastructure), or V2X (for Vehicle-to-a catch-all category that includes various wireless devices).[51] As the vehicle communications aspects of connected vehicles are now conceived, the USDOT recognizes two main categories or types of vehicular communications: (1) Connected Vehicle Safety Systems that use Dedicated Short Range

---

49. NAT'L ACAD. OF ENG'G, CITIES AND THEIR VITAL SYSTEMS: INFRASTRUCTURE PAST, PRESENT, AND FUTURE 16 (Jesse H. Ausubel & R. Herman, eds., 1988).

50. *See Telematics*, *IT Glossary*, GARTNER, http://www.gartner.com/it-glossary/telematics (last visited Dec. 2, 2014) (defining telematics as "the use of wireless devices and 'black box' technologies to transmit data in real time back to an organization. Typically, it's used in the context of automobiles, whereby installed or after-factory boxes collect and transmit data on vehicle use, maintenance requirements or automotive servicing. Telematics can also provide real-time information on air bag deployments or car crashes and locate stolen vehicles by using GPS technology. In addition, telematics can serve as the platform for usage-based insurance, pay-per-use insurance, pay as you drive (PAYD) insurance, pay how you drive (PHYD) programs for fleet insurance, or teen driving programs for retail business. . . . . New models are emerging, however, called 'mobile telematics,' in which smartphones connect to the car's computer system to pull data and send this to the insurer using the phone's wireless network.").

51. *See generally* RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., ACHIEVING THE VISION: FROM VII TO INTELLIDRIVE: POLICY WHITE PAPER (2010), *available at* http://www.its.dot.gov/research_docs/pdf/2From%20VII%20to%20IntelliDrive.pdf.

Communications (DSRC) transceivers to send and receive vehicle status communications; and (2) Connected Vehicle Mobility Applications that generally use cellular wireless to send and receive a wide range of data, from the status of the vehicle, to navigation assistance and infotainment. Some infotainment applications use satellite communications that transmit digital signals to moving vehicles.[52]

The USDOT has also preliminarily developed an integration of these two types of vehicle communications in what is called the Core System.[53] There is only baseline documentation for the Core System, which is designed to enable all types of connected vehicle communications: V2V, V2I, and V2X communications.[54] The available documentation includes a Core System concept of operations and high-level system design "that can use various means of communications technology, can be deployed incrementally, and promotes national interoperability."[55]

Because Connected Vehicle Safety Systems involve more specific technology and are more narrowly defined, they will be discussed first, followed by the more heterogeneous Connected Vehicle Mobility Applications. With a basic understanding of both types of connected vehicle systems, it will then be possible to discuss the legal and policy issues presented by these two types of connected vehicle technologies.

A. Connected Vehicle Safety Systems (V2V)

Connected vehicles using Dedicated Short Range Communications (DSRC) V2V Safety technology are already on roads and highways as test vehicles. In 2014, the V2V Safety Pilot successfully completed the first stage of demonstrating that V2V technology works in a real-world environment.[56] In February 2014, the National Highway

---

52. *See generally* CHRISTOPHER HILL, MODULE 13: CONNECTED VEHICLES (n.d.), *available at* http://www.pcb.its.dot.gov/eprimer/documents/module13.pdf.

53. *Connected Vehicle Core System Baseline Documentation*, RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/press/2011/connected_vehicle_coresystem_docs.htm (last updated Nov. 5, 2014) (a collection of Core System documentation). This documentation also "identifies potential areas for new and updated standards, and identifies critical risks to system deployment." *Id.*

54. *See id.*

55. *Id.*

56. For information on the Safety Pilot Model Deployment program, see generally SAFETY PILOT, http://safetypilot.umtri.umich.edu/ (last visited Dec. 2, 2014).

Traffic Safety Administration (NHTSA) announced that the Agency intends to engage in rulemaking that will require V2V safety technology in all new light vehicles sold in the United States.[57]

Connected vehicle communications using DSRC began development as part of the USDOT VII program late in the 1990s.[58] In 1997, the Intelligent Transportation Society of America, together with the USDOT, petitioned the Federal Communications Commission (FCC) for an allocation of spectrum for DSRC vehicle-based communications.[59] The petition was granted, and the FCC allocated 75 MHz of spectrum between 5.850 and 5.923 GHz (usually described as the 5.9 GHz band) to USDOT for ITS:

> By this action, we allocate 75 megahertz of spectrum at 5.850–5.925 GHz to the mobile service for use by Dedicated Short Range Communications ("DSRC") systems operating in the Intelligent Transportation System ("ITS") radio service. ITS services are expected to improve traveler safety, decrease traffic congestion, facilitate the reduction of air pollution, and help to conserve vital fossil fuels. DSRC systems are being designed that require a short range wireless link to transfer information between vehicles and roadside systems. We are also adopting basic technical rules establishing power limits, unwanted emission and frequency stability limits for DSRC operations. We defer consideration of licensing and service rules and spectrum channelization plans to a later proceeding because standards addressing such matters are still under development by the Department of Transportation. Once such standards are developed, the Commission could take whatever action is necessary to implement the standards related to DSRC use. Our decisions here will further the goals of the United States ("U.S.") Congress and the Department of Transportation to

---

57. Press Release, Nat'l Highway Traffic Safety Admin., U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles (Feb. 3, 2014), http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles; *see also* Todd Spangler, *Feds Move to Require Car-to-Car Safety Communication*, DETROIT FREE PRESS, Feb. 3, 2014, *available at* http://www.usatoday.com/story/money/cars/2014/02/03/nhtsa-vehicle-to-vehicle-communication/5184773/; Matthew L. Wald, *U.S. Plans Car-to-Car Warning System*, N.Y. TIMES, Feb. 3, 2014, *available at* http://www.nytimes.com/2014/02/04/business/us-plans-car-to-car-warning-system.html?_r=1.

58. *See* RESEARCH & INNOVATIVE TECH. ADMIN., *supra* note 35 at 4.

59. *See FCC Licensing Decision Will Help Advance Safe Transportation,* RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP. (Dec. 17, 2003), http://www.its.dot.gov/press/dsrclicensingfinal.htm.

> improve the efficiency of the Nation's transportation infrastructure and will facilitate the growth and development of the ITS industry.[60]

Since the FCC's allocation of spectrum for ITS, there have been a number of efforts to open some of that dedicated spectrum for wireless use. In 2013, the FCC announced that it would consider reallocating some of the 5.9 GHz spectrum for wireless communications.[61] Because of the special properties of the 5.9 GHz spectrum used for V2V communications, and because of concerns about interference with safety messages, the FCC has not finalized any reallocation of the 5.9 GHz spectrum.[62] In 2014, Senator Marco Rubio introduced S. 2505, a bill to "promote unlicensed spectrum use in the 5 GHz band, to maximize the use of the band for shared purposes in order to bolster innovation and economic development, and for other purposes."[63] This proposed legislation would set deadlines for the FCC to develop and publish a test plan for the use of unlicensed devices in the 5.9 GHz band.[64] In testimony before the House Committee on Science, Space, and Technology, USDOT Assistant Secretary for Research and Technology, Gregory D. Winfree, responded:

> We have very serious concerns about any spectrum sharing that prevents or delays access to the desired channel, or otherwise preempts the [V2V] safety applications. At this time, the

---

60. In the Matter of Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850–5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services, 14 FCC Rcd. 18221 (Oct. 21, 1999).

61. *See* In the Matter of Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, 28 FCC Rcd. 1769 (Feb. 20, 2013).

62. *See* Nat'l TELECOMMS. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, EVALUATION OF THE 5350-5470 MHZ AND 5850-5925 MHZ BANDS PURSUANT TO SECTION 6406(B) OF THE MIDDLE CLASS TAX RELIEF AND JOB CREATION ACT OF 2012 (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_5_ghz_report_01-25-2013.pdf.

63. Wi-Fi Innovation Act, S. 2505, 113th Cong. (2014).

64. *See* Press Release, Marco Rubio, U.S. Senator for Fla., Rubio, Booker Introduce Legislation To Expand Unlicensed Spectrum Use (June 20, 2014), http://www.rubio.senate.gov/public/index.cfm/press-releases?ID=52b7f5bb-b20b-4ac2-a35d-0b067b351ad0. In July 2014, Representatives Darrell Issa (R-Calif.), Doris Matsui (D-Calif.), and Anna Eshoo (D-Calif.) introduced a similar legislative proposal, H.R. 5125, in the House of Representatives. Bryce Baschuk, *House Lawmakers Introduce Bipartisan Bill to Increase Wi-Fi Access*, BLOOMBERG BNA (July 23, 2014), http://www.bna.com/house-lawmakers-introduce-n17179892766/. H.R. 5125 directs the FCC to conduct tests within the 5 GHz spectrum band to determine if it can be shared without interfering with current uses, especially vehicle-safety applications. *Id.*

> Department is unaware of any existing or proposed technical solution which guarantees interference free operation of the DSRC safety critical applications while allowing Wi-Fi enabled devices to share the 5.9 GHz spectrum.[65]

As currently allocated by the FCC, USDOT holds the wireless 75 MHz spectrum within the 5.9 GHz band, which is essential to V2V Connected Vehicle Safety Applications.[66] Similar bandwidth is used in Europe and in Asia for similar vehicle safety communications.[67] DSRC over the 5.9 GHz band provides unmatched speed, security, reliability, and protection from interference for V2V communications. This particular part of the wireless spectrum enables transmission and reception of data by DSRC-equipped vehicles nearly instantaneously[68] within the radius of at least a kilometer (over half a mile). The low latency feature of the 5.9 GHz band refers to the very short lag time between acquisition of data and its transmission in a DSRC V2V safety message.[69] For safety messages in a highway environment, where fractions of seconds can make the difference between a car crash and no crash, such low latency is essential.

Several types of technologies, standardized for interoperability among all makes and models of vehicles, are used in V2V safety communications. For safety communications, specialized two-way DSRC transceivers are designed to be embedded in the electrical systems of new vehicles by vehicle manufacturers. In addition, DSRC transceivers can also be added to other vehicles as retrofit or aftermarket devices.[70] Pedestrians or bicyclists can also carry DSRC

---

65. *Surface Transportation Hearing*, *supra* note 47, at 10.

66. *See id.*

67. *See, e.g.*, Press Release, CAR 2 CAR Communication Consortium, European Vehicle Manufacturers Working Hand in Hand on Deployment of Cooperative Intelligent Transport Systems and Services (C-ITS) (Oct. 10, 2012), http://car-to-car.org/index.php?id=20&L=wxuuwcbqab (follow "Memorandum of Understanding on Deployment" hyperlink under "10/2012: Vehicle Manufacturers Signing MoU" header).

68. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., VEHICLE SAFETY COMMUNICATIONS PROJECT TASK 3 FINAL REPORT: IDENTIFY INTELLIGENT VEHICLE SAFETY APPLICATIONS ENABLED BY DSRC 139 (2005), *available at* http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf.

69. Wireless technologies vary in the latency of their transmissions. Satellite transmissions have sufficiently high latency such that existing forms would be relatively useless for V2V crash warning purposes.

70. There are proposals to use after-market DSRC devices. *See, e.g.*, RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., ENABLING AFTERMARKET DEVICES WITH DSRC-BASED COMMUNICATIONS CAPABILITIES: SUMMARY OF INPUT FROM INDUSTRY STAKEHOLDERS (n.d.), *available at* http://www.its.dot.gov/research_docs/pdf/11Exploring%20Enabling%20DSRC%20Devices%20Challenges.pdf.

applications, perhaps as Smart Phone apps (an example of V2X). In addition, DSRC equipment can also be built into roadside units (an example of V2I). Current plans to require V2V connected vehicle safety technologies as mandatory safety equipment do not contemplate either V2I or V2X applications.[71] Nevertheless, such applications are technically feasible and could be added at a future time.

Because precise vehicle location is important, GPS provides location coordinates and elevation, as well as exact time. In addition to vehicle location, the DSRC unit (sometimes called an "On-Board Unit" or "On-Board Equipment") collects data about the vehicle's operational status (speed, direction of travel, etc.) and then transmits that vehicle data in the form of a Basic Safety Message.[72] The vehicle's V2V DSRC transceiver operates as a dynamic ad hoc network node, sending and receiving safety data in a 360-degree radius around a vehicle and from a distance of more than half a mile.[73] The transceiver's media access control (MAC) address[74] changes every three minutes to prevent use of the DSRC transceiver as a tracking device.[75] When a DSRC unit receives Basic Safety Messages from other nearby vehicles, the authenticity of each received message is validated by means of an encrypted public key infrastrucrure (PKI) security[76] certificate that operates as a header to authenticate the message and to assure the message's integrity.[77] Once authenticated, a message with safety data from another vehicle is then processed to provide warnings (e.g., a signal that it is unsafe to move into the lane on the right) or trigger automated systems (e.g.,

---

71. *See generally* Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57 (focusing on V2V technologies).

72. *See* SAE INT'L, SAE J2735: DEDICATED SHORT RANGE COMMUNICATIONS (DSRC) MESSAGE SET DICTIONARY 275–84 (2009), *available at* http://standards.sae.org/j2735_200911/.

73. RAM KANDARPA ET AL., U.S. DEP'T OF TRANSP., FINAL REPORT: VEHICLE INFRASTRUCTURE INTEGRATION PROOF-OF-CONCEPT RESULTS AND FINDINGS—INFRASTRUCTURE (2009), *available at* http://ntl.bts.gov/lib/31000/31300/31334/14488.pdf.

74. A MAC address is a unique identifier for network interfaces, such as a personal laptop connecting to the Internet. In the context of V2V, the MAC address is the identifier of each transceiver.

75. *See* LUCA DELGROSSI & TAO ZHANG, VEHICLE SAFETY COMMUNICATIONS: PROTOCOLS, SECURITY, AND PRIVACY (2012). Such a strategy avoids the potential for tracking specific units, or vehicles, over long periods of time by following their MAC addresses.

76. *See infra* Part IV.F.

77. *See Id.*

apply the brakes), depending on the interface provided by the vehicle's manufacturer.

V2V safety message communications take place in ad hoc networks with radii of about a kilometer.[78] These ad hoc networks are evanescent connections that form among DSRC-equipped vehicles as one DSRC-equipped vehicle moves closer to another DSRC-equipped vehicle. The ad hoc network connection dissipates as vehicles move farther away from each other. To protect privacy, V2V safety communications are anonymous in that they do not identify any particular vehicle as the source of a communication.[79] For similar reasons, virtually no vehicle data is recorded.[80] Standardized V2V communications formats make transmission and reception of meaningful safety data interoperable across all makes and models of vehicles.[81]

The purpose of V2V safety data communications is to provide warnings to drivers, such as a stopped vehicle ahead, as well as to trigger automated systems, such as automated braking or lane alignment, to avoid a crash. A standardized Basic Safety Message is central to V2V safety technology over DSRC.[82] The Basic Safety Message is transmitted over the DSRC wireless spectrum ten times per second and can be received at a distance of about 1000 meters.[83] Governed by the SAE International Standard J2735, the V2V Basic Safety Message includes GPS readings of time, latitude and longitude, elevation, positioning accuracy, transmission, speed, heading, acceleration, transmission state, steering wheel angle, brake status, and vehicle size, as well as a changing vehicle ID.[84] This V2V Basic Safety Message provides precise information about the exact location and behavior of a DSRC-equipped vehicle in real time.[85] There is also a second, optional part of the Basic Safety Message called Vehicle Safety Extension Data, which includes additional data, such as event flags (indicating hazard lights, anti-lock braking system activation, loss of traction control, hard braking, and air bag

---

78. *See* KANDARPA ET AL., *supra* note 73, at 17–19.

79. *See generally* DELGROSSI & ZHANG, *supra* note 75, at 155–57, 233 (discussing vehicle and message anonymity and privacy threats).

80. *See generally id.* at 151–64.

81. *See generally id.* at 48, 133.

82. *See* DELGROSSI & ZHANG, *supra* note 75, at 129, 142.

83. *See* MICHAEL MCGURRIN, U.S. DEP'T OF TRANSP., VEHICLE INFORMATION EXCHANGE NEEDS FOR MOBILITY APPLICATIONS 1 (2012), http://www.its.dot.gov/newsletter/BSM%20report.pdf.

84. SAE INT'L, *supra* note 72.

85. KANDARPA ET AL., *supra* note 73, at 1, 127.

deployment), path history, and path prediction.[86] Both parts of the Basic Safety Message are transmitted in the clear—i.e., the message is not encrypted.

The VII program was initially planned to enable both safety and other types of communications to be shared among vehicles and between vehicles and roadside equipment.[87] Plans announced by NHTSA do not include the latter features. In fact, NHTSA intends to adopt regulations requiring V2V safety equipment in light vehicles, takes pains to note that there will be no other, non-vehicle, recipients of the V2V Basic Safety Message exchanges.[88] Nevertheless, the DSRC equipment is, in fact, designed with ports for transmission of V2V safety messages to infrastructure recipients.[89]

Randomized, encrypted certificates used to authenticate safety messages, as well as DSRC transceivers' changing of MAC addresses, provide security in V2V safety communications.[90] The Basic Safety Message, containing detailed real-time vehicle location and operation information, is not itself encrypted. However, a security certificate is embedded in each message in a design that meets the Institute of Electrical and Electronics Engineers (IEEE) and SAE standards and protocols.[91] Without the certificate, Basic Safety Message data is

---

86. DELGROSSI & ZHANG, *supra* note 75, at 129–30.

87. *Vehicle-to-Infrastructure (V2I) Communications for Safety*, RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm (last updated Nov. 10, 2014). Although a vehicle communications system with roadside units might seem somewhat simpler than one that solely relies on inter-vehicle communications, this discussion focuses on direct V2V safety communications that are likely to be required by future NHTSA regulations.

88. Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49270 (proposed Aug. 20, 2014); *see* Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57.

89. *See* SAE INT'L, DSRC IMPLEMENTATION GUIDE: A GUIDE TO USERS OF SAE J2735 MESSAGE SETS OVER DSRC *passim* (2010), *available at* http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf (describing safety message transmission and reception capabilities of DSRC equipment).

90. *See* KANDARPA ET AL., *supra* note 73, at 100–01.

91. *See, e.g.*, IEEE STANDARD 802.11P: IEEE STANDARD FOR INFORMATION TECHNOLOGY—TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS—LOCAL AND METROPOLITAN AREA NETWORKS—SPECIFIC REQUIREMENTS, PART 11: WIRELESS LAN MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL LAYER (PHY) SPECIFICATIONS, AMENDMENT 6: WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (Inst. of Elec. and Elecs. Eng'rs 2010), *available at* http://standards.ieee.org/findstds/standard/802.11p-2010.html; IEEE STANDARD 1609.11: IEEE STANDARD FOR WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (WAVE)—OVER-THE-AIR ELECTRONIC PAYMENT DATA EXCHANGE PROTOCOL FOR INTELLIGENT TRANSPORTATION SYSTEMS (ITS) (Inst. of Elec. and Elecs. Eng'rs 2010), *available at* http://standards.ieee.org/findstds/standard/1609.11-2010.html. *See*

disregarded by another V2V device.[92] In addition to the security provided for the Basic Safety Message data exchanges, there is also a secure management system used in issuing the security certificates. That security certificate issuance and management system, which needs to be highly secure, is outlined in a recent NHTSA report.[93]

It is clear that outsiders, such as hackers, could create mischief by spoofing—creating a phantom vehicle or transmitting incorrect or confusing data. A very clever and lucky hacker might be able to influence the behavior of V2V connected vehicles through posing as a device transmitting safety messages that bear no relation to reality. However, the encrypted security certificates required by the V2V system to validate each Basic Safety Message make such threats much less likely to be successful. Moreover, security threats in the form of attempts to insert malware into the system will require additional preventative measures, such as firewalls and other careful measures to prevent unauthorized access to the yet-to-be-determined certificate-issuance system. The details regarding how this powerful and potentially pervasive V2V technology will be governed and by what entity are matters that remian sketchy.

At this point in the development of V2V safety systems, several distinctive features deserve special notice. First is V2V's use of ad hoc networks. Second is the evanescent quality of the vehicle safety data that is not recorded or stored. Third is the enormous amount of vehicle location and operational data transmitted ten times every second, generated by V2V technologies. Fourth is the use of PKI authentication certificates. Fifth is the absence of an off switch. Many details of these features will become clearer as NHTSA makes decisions about whether or not to require V2V DSRC transceivers as required safety equipment in new automobiles in the United States through adoption of a Motor Vehicle Safety Standard.

---

generally Security and Credentials Management, CONNECTED VEHICLE REFERENCE IMPLEMENTATION ARCHITECTURE, http://www.iteris.com/cvria/html/applications/app63.html#tab-3 (last updated Dec. 3, 2014).

92. *Security and Credentials Management*, *supra* note 91.

93. RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., SECURITY CREDENTIAL MANAGEMENT SYSTEM DESIGN: SECURITY SYSTEM DESIGN FOR COOPERATIVE VEHICLE-TO-VEHICLE CRASH AVOIDANCE APPLICATIONS USING 5.9 GHZ DEDICATED SHORT RANGE COMMUNICATIONS (DSRC) WIRELESS COMMUNICATIONS 11–13 (2012), *available at* http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf. The contemplated V2V security management system is more extensively described in RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION (2014), *available at* http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

B. Connected Vehicle Mobility Applications (Mobile Wireless)

The Connected Vehicle Mobility Applications are much more diverse than the narrowly purposed and standardized Connected Vehicle Safety Systems described in the discussion above.[94] Many of these Connected Vehicle Mobility Applications are already in commercial use. In addition, uncounted additional mobility applications come online every day. As a result, it is difficult to describe in one place all of the varied Connected Vehicle Mobility Applications.

Plugging a mobile device into a vehicle is one way to connect a vehicle to Internet applications that provide information that enhances vehicle mobility, such as navigation advice, weather, and traffic reports. Underlying that connectivity are two main smartphone connection platforms offered by Apple and Google. These systems enable smartphone functions to appear on a vehicle's display screen and to be controlled by using the vehicle's controls. Apple's interface, called CarPlay, was launched in March 2014. Google's similar interface, called Android Auto, launched in June 2014,.[95] Aside from these interfaces, vehicle manufacturers install proprietary mapping and infotainment systems.

In addition to Apple's CarPlay and Google's Android Auto, many vehicle manufacturers embed proprietary communications platforms within their vehicles to connect with the vehicles, vehicle parts and operations with their manufacturer, and to provide infotainment

---

94. *See* discussion *supra* Part III.A; *see also The U.S. Department of Transportation (USDOT) Offers a Free Public Meeting and Webinar on the Connected Vehicle Pilot Deployment Program*, RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/meetings/cv_pilot_deployment.htm (last updated Nov. 10, 2014) [hereinafter *Connected Vehicle Pilot Deployment Program*].

95. *See* Press Release, Apple, Apple Rolls Out CarPlay Giving Drivers a Smarter, Safer & More Fun Way to Use iPhone in the Car (Mar. 3, 2014), http://www.apple.com/pr/library/2014/03/03Apple-Rolls-Out-CarPlay-Giving-Drivers-a-Smarter-Safer-More-Fun-Way-to-Use-iPhone-in-the-Car.html; Gabe Nelson, *Google Is Ready to Challenge Apple's CarPlay*, AUTOMOTIVE NEWS, June 23, 2014, http://www.autonews.com/article/20140623/OEM06/306239983/google-is-ready-to-challenge-apples-carplay. Google's Android Auto is the first product to emerge from the Open Automotive Alliance, a Google-led consortium that includes Audi AG, General Motors, Honda Motor Co., Hyundai Motor Group, chipmaker Nvidia, and AT&T. Nelson, *supra*. It was renamed from Auto Link to Android Auto, June 25, 2014. Michael Gorman, *Google Gives Us a Simulated Ride with Android Auto*, ENGADGET (June 25, 2014), http://www.engadget.com/2014/06/25/android-auto-hands-on/.

services.[96] Typically, these systems also communicate vehicle performance and status data back to the vehicle's manufacturer. Among the automotive operating systems commonly used to run embedded vehicle connectivity equipment are: Microsoft Embedded Automotive, open-source MeeGo, and QNX Car from Research in Motion.[97] Android Auto's connected vehicle version of the Android operating system is a recent addition. These embedded operating systems for vehicle communications provide cross-platform mobile access to infotainment, communications functions, as well as integration between a vehicle's automotive systems and its manufacturer.[98]

USDOT has announced a research program, set to start in 2015, that will focus on "Dynamic Mobility Applications."[99] This program seeks to "combine connected vehicle and mobile device technologies in innovative and cost-effective ways to improve traveler mobility and system productivity, while reducing environmental impacts and enhancing safety."[100] The Dynamic Mobility Applications program envisions commercialization through "free and open competition," with the federal government playing "an appropriate and influential role as a technology steward for the continually evolving integrated transportation [information] system."[101] In March 2014, the Federal Highway Administration published a Federal Register Notice requesting information about Connected Vehicle Mobility Applications "that leverage the full potential of trusted communications among connected vehicles, travelers, and infrastructure to better inform travelers, enhance current operational practices, and transform surface transportation systems

---

96. *See generally* iSUPPLI CORP., EMBEDDED TELEMATICS IN THE AUTOMOTIVE INDUSTRY 3 (2011), *available at* http://gallery.mailchimp.com/e68b454409061ef6bb1540e01/files/Embedded_Telematics_in_the_Automotive_Industry_sw_iS.pdf.

97. *See* YING LU ET AL., *On the Application Development of 3G Technology in Automobiles*, *in* 6 PROCEEDINGS OF THE FISITA 2012 WORLD AUTOMOTIVE CONGRESS: VEHICLE ELECTRONICS 319–20 (Soc'y of Auto. Eng'rs of China & Int'l Fed'n of Auto. Eng'g Soc'ys eds., 2012); Craig Trudell & Jeff Green, *BlackBerry Gains as Ford Said to Pick QNX Over Microsoft*, BLOOMBERG (Feb. 24, 2014), http://www.bloomberg.com/news/2014-02-24/blackberry-shares-rise-as-ford-said-to-pick-qnx-over-microsoft.html.

98. *See generally* iSUPPLI CORP., *supra* note 96. A familiar example is General Motors' OnStar. *See* ONSTAR, https://www.onstar.com (last visited Dec. 3, 2014).

99. *See generally Dynamic Mobility Applications*, RES. & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., http://www.its.dot.gov/dma/ (last updated Nov. 7, 2014).

100. *Connected Vehicle Pilot Deployment Program*, *supra* note 94.

101. *Dynamic Mobility Applications*, *supra* note 99.

management."[102] This research program seeks "applications that synergistically capture and utilize new forms of connected vehicle and mobile device data to improve multimodal surface transportation system performance and enable enhanced performance-based systems management."[103]

Currently available mobility applications generally use wireless communications (cellular and PCS) provided by a wide range of carriers to communicate between the vehicle environment and elsewhere, including the Internet and telephones. Many vehicles are also equipped with receivers for satellite radio transmissions of infotainment programming. For short-distances within a vehicle, Bluetooth is frequently used for communications among devices.

The FCC licenses both telecommunications devices and wireless telecommunications carriers that transmit communications to and from mobility applications. Although there have been suggestions that the FCC adopt specific licensing regulations with regard to telematics providers, particularly in connection with 911 systems,[104] so far, the Commission licenses only communications devices and wireless service providers, rather than any particular mobility application or platform. Most Connected Vehicle Mobility Applications include GPS location technologies in part because location is required for wireless communications under the Commission's E911 regulations.[105] These regulations (Phase II of the Commission's E911 rules) now require wireless service providers to provide precise location information (the latitude and longitude of the caller) to Public Safety Answering Points.[106] This information must be accurate within fifty to three hundred meters, depending upon the type of location technology used.[107]

Driver distraction, caused by Connected Vehicle Mobility Applications, is a major area of concern. NHTSA has published guidelines that restrict visual and tactile access to many types of in-vehicle devices and displays likely to be included in Connected

---

102. Connected Vehicle Pilot Deployment; Request for Information, 79 Fed. Reg. 14105, 14105 (Mar. 12, 2014).

103. *Id.*

104. *See, e.g.*, In the Matter of Universal Service Contribution Methodology: A National Broadband Plan for Our Future, 27 FCC Rcd. 5357 (Apr. 30, 2012).

105. *See, e.g.*, Wireless E911 Location Accuracy Requirements, 75 Fed. Reg. 70,604, 70,605 (Nov. 18, 2010) (to be codified at 47 C.F.R. pt. 20).

106. *Id.*

107. *Id.* at 70,607, 70,609, 70,614.

Vehicle Mobility Applications.[108] These guidelines only affect the driver-facing interface aspects of Connected Vehicle Mobility Applications. The guidelines are specifically designated as voluntary,[109] because NHTSA did not want to "evaluate the safety implications of every new device before it is introduced into vehicles."[110] Nevertheless, the agency warns that "the Safety Act authorizes NHTSA to initiate enforcement action when a motor vehicle or item of motor vehicle equipment, including original equipment in-vehicle electronic devices, contains a safety-related defect."[111] So far, NHTSA has brought no formal enforcement actions.

The contents of Connected Vehicle Mobility Applications are highly varied. They range from satellite navigation assistance and mapping to video and audio entertainment. The information and entertainment provided may be accompanied by advertisements that can be targeted at the vehicle's occupants, based on the type of vehicle and its location, previous content, and occupants. There is a real tension between encouraging further development of Connected Vehicle Mobility Applications and avoiding the potentially deadly consequences of driver distraction.

Among the challenges faced by Connected Vehicle Mobility Applications are heightened cybersecurity needs. In the context of mobility applications, security threats can be difficult to guard against because of the plethora of information sources and types of communications carried by Connected Vehicle Mobility Applications. In such a setting, identifying, isolating, and preventing security threats from hackers and malware is very difficult. As the Internet of Things increasingly includes vehicles using wireless Internet connections, sensor-rich systems within vehicles[112]—including tires, fuel injection, brakes, steering, and transmission—are likely to become attractive hacker targets. According to a recent report from Vision Zero, "[a] new car may have more than 145 actuators and 75 sensors, which produce more than 25GB of data per hour. The data is analyzed by more than 70 onboard computers to ensure safe and comfortable

---

108. Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices, 78 Fed. Reg. 24,818 (Apr. 26, 2013).

109. *Id.* at 24,881.

110. *Id.*

111. *Id.* (citing 49 U.S.C. §§ 30118–30121 (2000)).

112. Many of these sensors are used in compliance with the Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, Pub. L. No. 106-414, 114 Stat. 1800 (2000) (codified as amended in scattered sections of 49 U.S.C.).

travel."[113] These systems also provide feedback data to the manufacturer of the vehicle.[114] The report warns, "[m]any modern cars have infotainment systems, engine management units, onboard diagnostic units, radios operating at different frequencies, GPS receivers, transponders, Bluetooth devices, and cell phone chips. Malware in any subsystem could compromise the safety of not only the people in the car, but also those around them."[115] Research is underway with regard to potential security threats to this type of connected vehicle. However, thorough investigation of security solutions for Connected Vehicle Mobility Applications is just beginning.[116]

Although Connected Vehicle Mobility Applications have been available much longer than DSRC-based Connected Vehicle Safety Systems, both types of vehicle connectivity are in the process of rapid development. The specific ways in which they will develop will depend in part on the legal and policy environment these technologies encounter.

IV. LEGAL AND POLICY ISSUES FACING CONNECTED VEHICLES

Just how smart connected vehicle transportation infrastructure will turn out to be will depend in part on how well connected vehicles resolve a raft of legal and policy issues. As described in the previous sections, the two types of connected vehicle technologies operate quite differently and have different functions, operations, and architectures that interact with law and policy in different ways. They appear to be compatible technologies, rather than competing technical solutions to the same problem. Nevertheless, both types of connected vehicle technologies face a number of legal and policy challenges that require resolution before the benefits of this mostly invisible transportation infrastructure can realize promised safety and mobility benefits.

The following sections discuss six of the more interesting of these issues: regulation, products liability, insurance, law enforcement, privacy, and security. Some of these legal and policy issues present greater difficulties for one type of vehicle connectivity over the other.

---

113. Max Glaskin, *Safe and Secure*, VISION ZERO INT'L, June 2014, at 40.

114. *See generally* ISUPPLI CORP., *supra* note 96 (discussing the nature and benefits of data utilized by automotive manufacturers by way of embedded telematics).

115. Glaskin, *supra* note 113.

116. Organizations such as the Cyber Security Research Alliance and the Automotive Consortium for Embedded Security are making dedicated efforts to deal with this group of problems. *Id.* at 41, 43.

A. Regulation

Both types of connected vehicle technologies are, in different ways, subject to federal regulatory jurisdiction. For transportation infrastructure technologies to be able to operate all over the United States and apply to all types, makes, and models of vehicles, national interoperability will require national standards.

For both types of connected vehicle technologies, USDOT's NHTSA has been the most active regulatory agency. In February 2014, NHTSA announced that it has begun to take steps to require connected vehicle safety technologies (V2V) in all new light vehicles.[117] The Agency's apparent plan is to propose regulations that require V2V connected vehicle technology in all new vehicles in the United States by early 2017.[118] If NHTSA carries out its plan to adopt a Motor Vehicle Safety Standard, a nation-wide, safety-oriented connected vehicle transportation infrastructure will come into being.[119] In its 2014 press release, NHTSA explained:

> The safety applications currently being developed provide warnings to drivers so that they can prevent imminent collisions, but do not automatically operate any vehicle systems, such as braking or steering. NHTSA is also considering future actions on active safety technologies that rely on on-board sensors. Those technologies are eventually expected to blend with the V2V technology. NHTSA issued an Interim Statement of Policy in 2013 explaining its approach to these various streams of innovation. In addition to enhancing safety, these future applications and technologies could help drivers to conserve fuel and save time.[120]

The new infrastructure would be based on DSRC technologies.

In contrast, with regard to Connected Vehicle Mobility Applications, NHTSA has issued "Guidelines for Reducing Visual-Manual Driver Distraction During Interactions With Integrated, In-Vehicle, Electronic Devices" to restrain such applications from becoming highway safety-hazards through distracting drivers:

> NHTSA is concerned about the effects of driver distraction on motor vehicle safety. Crash data show that 17 percent (an estimated 899,000) of all police-reported crashes involved some type of driver

---

117. Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57.

118. Elvina Nawaguna, *U.S. May Mandate 'Talking' Cars by Early 2017*, REUTERS, Feb. 3, 2014, *available at* http://www.reuters.com/article/2014/02/03/us-autos-technology-rules-idUSBREA1218M20140203.

119. *See* Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49270 (proposed Aug. 20, 2014).

120. Nawaguna, *supra* note 118.

> distraction in 2010. Of those 899,000 crashes, distraction by a device or control integral to the vehicle was reported in 26,000 crashes (3% of the distraction-related police-reported crashes).[121]

NHTSA's Federal Register Notice defines "driver distraction," as referring to "a specific type of inattention that occurs when drivers divert their attention away from the driving task to focus on another activity."[122] The stated purpose of the guidelines is "to reduce the number of motor vehicle crashes and the resulting deaths and injuries that occur due to a driver being distracted from the primary driving task while performing secondary tasks involving the use of an in-vehicle electronic device."[123]

The Notice accompanying the guidelines categorizes distractions into three types:

- Visual distraction: Tasks that require the driver to look away from the roadway to visually obtain information;
- Manual distraction: Tasks that require the driver to take a hand off the steering wheel and manipulate a device; and
- Cognitive distraction: Tasks that require the driver to avert their mental attention away from the driving task.[124]

Connected Vehicle Mobility Applications, such as infotainment and navigation systems, potentially pose all three types of driver distractions.

The other main federal regulatory agency that regulates connected vehicles is the FCC, which has allocated spectrum to Connected Vehicle Safety Systems and licenses V2V DSRC transceiver equipment, but has otherwise left V2V DSRC communications largely unregulated.[125] On the other hand, with regard to the mobile wireless communications (e.g., Wi-Fi, 4G, LTE, etc.), which transmit Connected Vehicle Mobility Applications, the Commission has extensive wireless communications regulations.[126]

---

121. Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices, 78 Fed. Reg. 24,818, 24,819 (Apr. 26, 2013).

122. *Id.* at 24,822.

123. *Id.* at 24,881. The guidelines are directed at connectivity devices built into vehicles by manufacturers.

124. *Id.* at 24,819.

125. *See* In the Matter of Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850–5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services, 14 FCC Rcd. 18221 (Oct. 21, 1999).

126. *See, e.g.*, Comprehensive Review of Licensing and Operating Rules for Satellite Services, 77 Fed. Reg. 67,172 (Nov. 8, 2012) (to be codified at 47 C.F.R. pt. 25).

In addition, a third agency, the Federal Trade Commission (FTC) has taken note of "Connected Cars" in the context of considering privacy and security issues posed by the Internet of Things.[127] In the future some Connected Vehicle Mobility Applications may present unfair or deceptive trade practices that will attract FTC enforcement attention. In contrast, V2V safety systems, which do not carry data about identified consumers, appear unlikely to be scrutinized by the FTC.

B. Products Liability

Both types of connected vehicles would face potential products liability litigation if malfunctioning devices result in injury. At present, V2V safety systems, based on DSRC, are not yet available as consumer products. On the other hand, Connected Vehicle Mobility Applications have been commercially available for some time. Various forms of these Mobility Applications are in fact heavily marketed to consumers. With regard to both safety and mobility types of connected vehicle technologies, the specter of products liability has been an ongoing concern for vehicle manufacturers deciding whether or not to embed either type of connected vehicle technology in their vehicles. Even if NHTSA requires V2V DSRC safety systems as a Federal Motor Vehicle Safety Standard,[128] vehicle manufacturers would not be absolved from liability for defective safety equipment. If the safety equipment turns out to be defective or misrepresented, products liability is likely. In addition to tort-based products liability for harm caused by these technologies, legal actions based on contract warranties, both express and implied, will also be available to purchasers of connected vehicles.. Moreover, there are also federal and state "Lemon Law" statutes that may apply in some cases.[129]

Products liability is a complicated field with rules that vary considerably from state to state. However, the *Restatement (Third)*

---

127. *See Internet of Things—Privacy and Security in a Connected World: Conference Description*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (last visited Dec. 3, 2014). The FTC's interest is in the Connected Vehicle Mobility Applications, which interface directly with consumers, rather than the Connected Vehicle Security Systems that rely on DSRC.

128. *See supra* notes 57 and 88 and accompanying text.

129. *See, e.g.*, Magnuson–Moss Warranty Act, 15 U.S.C. §§ 2301–2312 (2012); *Publications*, INT'L ASS'N LEMON L. ADMINS., http://www.ialla.net/pub_1.htm (last updated Jan. 27, 2014) (providing extensive information about the Lemon Law statutes of the various states).

of Torts: Products Liability, adopted by the American Law Institute in 1998, provides some assistance in thinking generally about legal grounds for product liability.[130] Products liability law combines tort and contract law to provide causes of action that seek to impose civil liability on the manufacturer of a commercial product that causes harm. Because commercial versions of V2V DSRC transceivers have not yet been sold to end users, the application of products liability law to Connected Vehicle Safety Systems is at present theoretical. On the other hand, many types of consumer-oriented mobility applications are already embedded in the electrical systems of passenger cars or attached to vehicles after purchase of the vehicles.[131] So far, reported court decisions regarding products liability litigation involving Connected Vehicle Mobility Applications appear to be sparse.

With regard to connected vehicle technologies discussed in this Article, products liability actions could be brought against either device manufacturers or the manufacturers of the vehicles in which the devices are embedded, as well as vehicle and equipment dealers.[132] Products liability litigation typically involves multiple defendants. Moreover, there may also be multiple plaintiffs since products liability causes of action are usually available to anyone suffering injury caused by a consumer product.[133] A wide range of products liability causes of action may be used in litigation involving connected vehicles. These potential actions include breach of express and implied warranties,[134] negligence,[135] manufacturing defects,[136] design defects,[137] warning defects,[138] and strict liability.[139]

---

130. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. (1998).

131. The latter are called "after-market" devices. *See* Andrew Tolve, *The Future of Aftermarket Telematics, Part I*, TELEMATICS UPDATE (Jul. 2, 2013), http://analysis.telematicsupdate.com/print/35886 (discussing the future of after-market devices in light of competition from embedded telematics).

132. *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 5 (1998) (discussing the liability of commercial sellers or distributors of product components).

133. *Id.* § 1.

134. Implied and express warranties provide a contractual basis for product liability. Usually these warranties take the form of assurances that a product is of sufficient quality for its intended use. *See* U.C.C. § 2-314 (2002). For an interesting account of how difficult it can be to obtain copies of written consumer warranties from the manufacturer of a vehicle with a mobility application embedded in it, see Francesca Svarcas, *Turning a New Leaf: A Privacy Analysis of Carwings Electric Vehicle Data Collection and Transmission*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 165 (2013). As noted above, federal and state Lemon Laws usually are based on product warranties. *See supra* note 129 and accompanying text.

135. Negligence liability would be based on a product manufacturer's failure to exercise reasonable care in designing or building a product that causes reasonably foreseeable harm. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL &

A great deal of theoretical and academic writing has considered products liability law as it may apply to autonomous vehicles.[140]

EMOTIONAL HARM §§ 6, 7 (2010); RESTATEMENT (SECOND) OF TORTS § 281 (1965). An example might be based on carelessly coded software that causes a navigation system to provide erroneous directions that result in a car crash.

136. If a defect in a product that is ordinarily safe contains a manufacturing flaw that causes harm to a person or property, the one suffering that harm can hold the manufacturer liable (often strictly liable), even when the manufacturer had exercised "all possible care" to avoid the defect. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(a) (1998) Connected vehicle computer systems marketed to consumers may normally be safe, but may contain flaws or "bugs" that can cause harm to users.

137. If a product has a defective design that causes harm to others, the manufacturer or seller can be held legally responsible for the harm. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (1998) New technologies often face legal challenges based on their new designs, particularly user interfaces. That might be particularly applicable to the nature of warning interfaces that could be designed in ways that either unreasonably alarm drivers, or are ineffective in delivering a warning about a nearby safety hazard.

138. Liability can also be based on failure to explain risks involved in using a product. If harm is caused by lack of information or warnings about potential product risks, the manufacturer or seller can be held liable for failure to warn when an injury related to this lack of information occurs. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(c) (1998) Connected vehicles will likely be sold with extensive warnings about the risks of relying on the information provided by the V2V or other system embedded in the vehicle.

139. Strict liability can be imposed without fault on the part of the manufacturer of an unreasonably dangerous product. Even though a manufacturer or seller of a connected vehicle has exercised all possible care, if its product causes harm because the product turns out to be unreasonably dangerous, the manufacturer or seller will be held responsible for harm that results even when the manufacturer or seller is determined to have engaged in no faulty behavior. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(a) (1998); RESTATEMENT (SECOND) OF TORTS § 402A (1965). A connected vehicle navigation system may be appropriately made with due care, but may be an inherent hazard because it blocks a driver's view of oncoming traffic.

140. *See generally* JOHN VILLASENOR, CTR. FOR TECH. INNOVATION AT BROOKINGS, PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION (2014), *available at* http://www.brookings.edu/~/media/research/files/papers/2014/04/products%20liability%20driverless%20cars%20villasenor/products_liability_and_driverless_cars.pdf; M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571 (2011); Kyle Colonna, *Autonomous Cars and Tort Liability*, 4 CASE W. RES. J.L. TECH. & INTERNET 81 (2012); Sophia H. Duffy & Jamie P. Hopkins, *Sit, Stay, Drive: The Future of Autonomous Car Liability*, 16 SMU SCI. & TECH. L. REV. 453 (2013); Andrew P. Garza, *"Look Ma, No Hands!": Wrinkles and Wrecks in the Age of Autonomous Vehicles*, 46 NEW ENG. L. REV. 581 (2012); Kyle Graham, *Of Frightened Horses and Autonomous Vehicles: Tort Law and its Assimilation of Innovations*, 52 SANTA CLARA L. REV. 1241 (2012); Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321 (2012); Bryant Walker Smith, *Proximity-Driven Liability*, 102 GEO. L.J. 1777 (2014); *see also* JAMES M. ANDERSON ET AL., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf; Bryant Walker Smith, *Uncertain Liability*, CTR. FOR INTERNET

However, there has been relatively little published academic legal analysis published regarding application of products liability to connected vehicle technologies.

Products liability is unusual in placing potential legal liability on any entity in the chain of product-design, product-development, and product-distribution before the product reaches the end user. Under products liability law, any person injured by a product can seek damages from anyone involved in making or distributing the product.[141] Makers and distributers of new technologies such as the DSRC transceiver used in V2V connected vehicles are rightfully concerned about the scope of product liability risks if harm results from the new technologies, no matter how carefully they have been made. Existing applications of Connected Vehicle Mobility Applications provide some litigation experience as a basis for estimating risks from potential products liability.[142] Even with regard to these applications, there appear to be few products liability legal precedents regarding the specific type of active-safety warning technology involved in vehicles connected using V2V.[143]

Litigation regarding connected vehicles is likely to be highly complex, as well as expensive. Assume that drivers involved in a vehicle crash are all driving connected vehicles, and that in one or more of the vehicles the connected vehicle technologies somehow caused or contributed to the crash. Numerous parties and their lawyers would be involved. In addition to each driver involved in the crash, that driver's insurer, the manufacturer of each driver's vehicle, and the manufacturers of the connected vehicle technologies in those vehicles would likely be parties. This scenario does not include the potential for injured parties who were not drivers or passengers in the vehicle, but who may have been harmed in an actual vehicle crash.[144]

The potential costliness of products liability litigation operates as a factor discouraging the deployment of new technologies such as those

---

& SOC'Y (May 27, 2013, 5:25 PM), http://cyberlaw.stanford.edu/blog/2013/05/uncertain-liability.

141. *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 1 (1998).

142. It may be surprising to note that in searching for reported decisions regarding connected vehicle technologies, there appear to be fewer than ten reported cases involving products liability actions regarding navigation systems. In fact, there appeared to be more reported decisions regarding theft of navigation systems than product liability actions related to navigation systems.

143. Both seat belts and airbags are passive-safety technologies designed to ameliorate injury in the event of a crash. Active safety technologies, which are designed to prevent accidents through warnings to drivers, may be treated differently by products liability law.

144. *See generally* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 1 (1998).

involved in connected vehicles, even when the safety and mobility benefits of the technologies are compelling. According to a 2013 study by the Government Accountability Office (GAO), "[a]utomobile manufacturers may be reluctant to move forward with plans to install V2V technologies in their newly manufactured vehicles because of the uncertainty that accompanies these liability issues."[145] On the other hand, USDOT officials told GAO investigators that they "do not believe that V2V technologies pose any greater liability issues for automobile manufacturers than existing sensor-based crash avoidance technologies . . . ."[146] In the meantime, because it appears to be so difficult to estimate products liability risks from connected vehicles, developers have sought legislative or regulatory limitations on potential products liability.[147]

C. Insurance

Because connected vehicles provide rich sources of information about both vehicles and drivers, automobile insurance companies have taken a keen interest in connected vehicles and the data they generate. The anonymous nature of data used in V2V safety systems makes that V2V data less directly useful for calculating automobile insurance rates and pricing automobile insurance coverage based on an individual driver's "driving data" about how an automobile is used or how the driver behaves.[148]

In contrast, consumer-facing Connected Vehicle Mobility Applications are already widely used in what is called "usage based insurance" (UBI).[149] This type of insurance establishes pricing for automobile insurance through use of a wide range of driver-behavior and vehicle-usage measures.[150] For example, automobile insurance is available on the basis of "Pay-As-You-Drive" (PAYD, based on mileage driven), "Pay-How-You-Drive" (PHYD, based on driving behavior), or "Pay-As-You-Go" (Pay-Go, in which a driver pays for

---

145. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-13, INTELLIGENT TRANSPORTATION SYSTEMS: VEHICLE-TO-VEHICLE TECHNOLOGIES EXPECTED TO OFFER SAFETY BENEFITS, BUT A VARIETY OF DEPLOYMENT CHALLENGES EXIST 28 (2013).

146. *Id.*

147. *See id.*

148. *See* TELEMATICS UPDATE, INSURANCE TELEMATICS REPORT 2014 (EXTRACT), at 9 (2014).

149. *Id.*; *see also*, *Usage-Based Insurance and Telematics*, NAT'L ASS'N OF INS. COMMISSIONERS, http://www.naic.org/cipr_topics/topic_usage_based_insurance.htm (last updated Nov. 29, 2014).

150. *See Usage-Based Insurance and Telematics*, *supra* note 149.

insurance as he or she is driving, rather than paying for insurance in advance).[151] There is also Manage-How-You-Drive (MHYD), which is designed to provide feedback to drivers about their driving behavior, safety, fuel usage, and the like.[152]

Progressive Insurance offers Snapshot, a device that plugs into the diagnostics port (OBD2) on or under a vehicle's dashboard and bases insurance rates on mileage, time of day, hard braking, and the like.[153] After 10 billion miles driven, "Progressive has found that the measurement of how someone drives is indeed a better predictor of risk than driving record, age, gender or any of the traditional rating factors."[154] Nevertheless, "the models can still get a lot better," according to David Pratt, Progressive's general manager of usage-based insurance.[155] Insurance rating systems and practices are governed by state law and vary from state to state in the United States. It would be possible for automobile insurance companies to use Mobility Applications to gather information about driver behavior for the sole purpose of monetizing the value of the information, instead of for the purpose of pricing insurance. Whether this will lead to more exacting insurance regulation by states to curb such non insurance uses of driver behavior data is uncertain.

There has also been some dispute about the quality and focus of internal vehicle operational data available through the OBD2 diagnostics port, which was designed to provide data related to vehicle emissions standards.[156] Much more extensive vehicle operational information can be extracted through the use of hard-wired embedded insurance-information collection devices that are

---

151. *Id.*

152. *See* Jessica Royer Oken, *Insurance Telematics Business Models: Beyond the Discount*, TELEMATICS UPDATE (Aug. 13, 2013), http://analysis.telematicsupdate.com/insurance-telematics/insurance-telematics-business-models-beyond-discount; *see also* Susan Kuchinskas, *UBI Pricing: Reality or Fantasy? Part I*, TELEMATICS UPDATE (May 27, 2014), http://analysis.telematicsupdate.com/print/36283; Susan Kuchinskas, *UBI Pricing: Reality or Fantasy? Part II*, TELEMATICS UPDATE (May 29, 2014), http://analysis.telematicsupdate.com/print/36286 [hereinafter *UBI Pricing Part II*].

153. An OBD2 port has been required in all United States Vehicles since the late 1990s for vehicle emissions purposes. Susan Kuchinskas, *Magic Bus: The Fight for the OBD2 Port*, TELEMATICS UPDATE (Dec. 31, 2013), http://analysis.telematicsupdate.com/navigation-and-lbs/magic-bus-fight-obd2-port.

154. *See UBI Pricing Part II*, *supra* note 152.

155. *Id.*

156. *See* Kuchinskas, *supra* note 153.

used in Europe.[157] So far, this is not a widespread practice in the United States.

Insurance companies' demand for Connected Vehicle Mobility Applications' vehicle operation data raises a number of ongoing policy issues. Disclosure of how insurance companies use data about drivers collected through telematics, as well as what insurance companies do with a driver's behavior data once collected, raise privacy concerns as well as concerns about insurance business strategies using Connected Vehicle Mobility Applications.

D. Law Enforcement

Law enforcement access to connected vehicles and their data seems inevitable. Nevertheless, on what terms and whether a judicial warrant will be required before law enforcement agents can legitimately have access to connected vehicles and their data remains an important and complicated issue.

It appears likely that a judicial warrant will be required for law enforcement access to information contained in connected vehicles. Opinions in two recent United States Supreme Court decisions—*Riley v. California*[158] and *United States v. Jones*[159]—reflect the Court's increasing interest in understanding and applying appropriate legal principles to new areas of technology, such as connected vehicle transportation infrastructure.

In *Riley*, the most recent of these decisions, the Court ruled that a law enforcement search for digital information in a cell phone, after the phone's owner had been arrested and was in custody, requires a judicial warrant before law enforcement agents can legally access the files within the cell phone.[160] The Court described smart phones as really just "minicomputers," and distinguished searches for digital information within them from searches of physical containers in the context of searches incident to arrest.[161] Chief Justice Roberts's opinion for the Court, explains:

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could

157. TELEMATICS UPDATE, *supra*, note 148, at 12–14.
158. Riley v. California, 134 S. Ct. 2473 (2014).
159. United States v. Jones, 132 S. Ct. 945 (2012).
160. *See Riley*, 134 S. Ct at 2495.
161. *See id.* at 2489.

> reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. See United States v. Jones, 565 U. S. ___, ___ (2012) (SOTOMAYOR, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").[162]

The comprehensive information contained in a connected vehicle is similar, in terms of importance to the individual, to that collected by a smart phone. Depending on the nature of the application or service, a connected vehicle can reveal extensive and intimate details about a person's past and present whereabouts, activities, and interests. In the context of searches of a stopped connected vehicle incident to arrest of the vehicle's driver or occupants, it is likely that courts will rely on *Riley* to determine that searching through digital information contained in connected vehicles similarly requires a judicial warrant. Although the Court's opinion in *Riley* recognizes some exceptions to the warrant requirement, such as exigent circumstances, the fact that Riley was arrested after a car stop did not cause the Court to apply the automobile exception to warrant requirements.[163] As a result, it appears likely that judicial warrants will be required before law enforcement agents access the rich trove of information contained in connected vehicles that have been stopped by law enforcement. The fact that Chief Justice Roberts relied on and quoted from Justice Sotomayor's concurring opinion in *Jones* indicates growing recognition of the sensitivity of location information. Indeed, comprehensive location information seems to be a matter of high privacy expectations for which a judicial warrant is especially needed.[164]

A connected vehicle seems likely to be considered comparable to a cell phone for several reasons. First, the digital data contained within a connected vehicle are typically similar to the digital files described

---

162. *Id.* at 2490.

163. In such circumstances of an arrest following a vehicle stop, the Court's earlier decision in *Arizona v. Gant*, 556 U.S. 332, 344 (2009), would also substantiate the requirement of a warrant in the context of a search of a stopped vehicle and later search of connected vehicle data.

164. *See Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

by Chief Justice Roberts as typically within a cell phone. Both reflect the lives, beliefs, communications, and past locations of their users. In *Riley*, the Court observed that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." [165] The opinion also focuses on the comprehensiveness of the information these devices often contain. Connected Vehicle Mobility Applications similarly contain a comprehensive itinerary of all of the locations visited by the vehicle and its driver, as well as other information about communications and interests of vehicle occupants. Location tracking over time was involved in *Jones*, and appears to be a matter of special constitutional concern to a majority of the Justices.[166]

It is also noteworthy that the aptness of an analogy between connected vehicles and smart phones has seemed appropriate outside the legal context. In 2011, Toyota Motor Corporation President Akio Toyoda unveiled a concept car called the Fun-Vii, by saying, "[s]ome of you might have thought to yourselves: 'Is this really a car?' . . . It's like a smartphone on wheels."[167] More recently, Mark Fields, now Ford Motor Company's CEO, asked a provocative question at Ford's Trends Conference 2014: "[s]ome may view [a car] as a cell phone on wheels, a web portal on wheels, or their largest wearable. If their car is more than just a car, then what's a car company?"[168]

Riley did not deal with the legality of intercepting communications during transmission. In the context of connected vehicles, interception of communications from the two types of connected vehicle techonologies would be subject to different legal analyses. Communications to and from Connected Vehicle Mobility Applications are usually encrypted (at least by the telecommunications carriers). As a result, an electronic surveillance court order would appear to be required under the Electronic

---

165. *Id.* at 2489.

166. In *Jones*, five Justices expressed this concern. *See Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring); *see also id.* at 958 (Alito, J., concurring) (joined by Ginsburg, J., Breyer, J., and Kagan, J.).

167. Hans Greimel, *Toyota Unveils 'Smartphone on Wheels' Concept Car for Tokyo Show*, AUTOMOTIVE NEWS (Nov. 27, 2011), http://autoweek.com/article/nhra/toyota-unveils-smartphone-wheels-concept-car-tokyo-show.

168. Lyndsey Gilpin, *New Ford CEO Mark Fields Sees Car as Phone, Web, and Wearable on Wheels*, ZDNET (June 25, 2014), http://www.zdnet.com/new-ford-ceo-mark-fields-sees-car-as-phone-web-and-wearable-on-wheels-7000030921/.

Communications Privacy Act (ECPA) for contemporaneous interception of encrypted Mobility Applications transmissions.[169]

However, Connected Vehicle Safety Systems transmit the content of Basic Safety Messages without encryption. These transmissions can be intercepted by law enforcement without a warrant. A Basic Safety Message does not identify which vehicle is sending it. The security certificate that accompanies each Basic Safety Message to authenticate it might provide some identification. This security certificate is encrypted and protected against warrantless law enforcement interception by the ECPA.[170] The odd result is that the data in the Basic Safety Message is available to anyone who can capture it, including law enforcement agents who do not have court authorization.[171] However, as a practical matter, the content of a Basic Safety Message would be difficult to attach to other Basic Safety Messages, much less to the vehicle that transmitted it, without the encrypted security certificate that is protected from interception.

The United States Supreme Court in *Jones*[172] decided that a law enforcement agency's physical attachment of a GPS device to a suspected drug dealer's car in order to follow the suspect's movements for a month constituted a "search" under the Fourth Amendment.[173] The Court in *Jones* did not address the issue of whether law enforcement was entitled, without a warrant, to follow a GPS signal from a device already installed in the vehicle, presumably with the consent of the vehicle's owner.[174] A number of the Justices concurring in *Jones* expressed concern about the constitutionality of law enforcement tracking GPS signals associated with a particular

---

169. *See* 18 U.S.C. § 2518 (2012). Alternatively, a Foreign Intelligence Surveillance Act (FISA) order under 50 U.S.C. § 1801 (2012) could authorize interception of connected vehicle communications involving foreign powers or agents of foreign powers.

170. *See* 18 U.S.C. § 2511 (2012) (combining with 18 U.S.C. § 2510(16), which states that encrypted communications are not considered to be "readily accessible to the general public").

171. *See id.* (stating that broadcast data transmissions that are "readily accessible to the general public" (as the phrase is defined in 18 U.S.C. § 2510(16)) are not subject to warrant requirements).

172. United States v. Jones, 132 S. Ct. 945, 949 (2012).

173. *See id.* at 949.

174. *See id.* at 955 (Sotomayor, J., concurring). Connected Vehicle Mobility Applications would typically present this issue, since most of them include an identifiable person's location information.

vehicle over a long period of time, whether or not the GPS device was installed by law enforcement.[175]

Connected Vehicle Safety Systems transmit each vehicle's GPS coordinates every ten seconds. Were such a system required in all vehicles under, for example, a Motor Vehicle Safety Standard,[176] difficult constitutional issues would arise. Both Fourth Amendment (unreasonable searches and seizures) and Fifth Amendment (self-incrimination) issues could be raised. The resolution of these issues is among the unsettled constitutional matters that the Court has not yet reached.

There is some possibility that transmissions from DSRC-based Connected Vehicle Safety Systems may not be protected at all under the ECPA on the grounds that DSRC transceivers are "mobile tracking device" transmissions, which are not protected as electronic communications.[177] Subsection 3117(b) defines the term "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[178] How far this definition of tracking device reaches, beyond old-fashioned "beepers," has not yet been determined.[179] If DSRC transceivers were determined to be tracking devices exempt from the warrant requirements of the ECPA, then Fourth Amendment requirements would apply, as was the case with regard to the GPS device in *Jones*.[180]

As noted earlier, unencrypted transmissions from connected vehicles, such as anonymous V2V Basic Safety Messages, that are "readily accessible to the general public" are exempt from the ECPA under 18 U.S.C. § 2510(16).[181] As a practical matter, it seems unlikely that federal law enforcement agencies, such as the Department of Justice or the Department of Homeland Security, would engage in comprehensive collection of the enormous quantities of anonymous V2V data. Recording a DSRC device's V2V safety messages transmitted ten times per second amounts to 51,840,000 messages

---

175. *See id.* at 955–57 (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring).

176. *See supra* note 57 and accompanying text.

177. Transmissions from such tracking devices (defined under 18 U.S.C. § 3117 (2012)) are not "electronic communications" governed by the ECPA. 18 U.S.C. § 2510(12)(C) (2012).

178. 18 U.S.C. § 3117(b) (2012).

179. *See, e.g.*, United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).

180. *Cf. Jones*, 132 S. Ct. at 949.

181. *See supra* note 171 and accompanying text.

(each with as many as forty data elements) transmitted per vehicle each day. Such recording is of course possible, but would then require massive data analysis to sort and identify particular messages of interest. Since the unencrypted content of V2V Basic Safety Messages is not identified with regard to any particular vehicle or person, the task of re-identification would be particularly difficult, time-consuming, and costly. Securing a judicial warrant to install a GPS device on a suspect's vehicle, as required under *Jones*,[182] would almost certainly be less expensive and less burdensome.

The Communications Assistance for Law Enforcement Act (CALEA),[183] which requires installation of law enforcement access points (sometimes referred to as "backdoors") in telecommunications networks,[184] would apply differently to the two types of connected vehicle technologies. CALEA does not appear to apply to the vehicle-facing V2V DSRC communications under the FCC's 2005 order that extended CALEA requirements to VoIP and facilities-based broadband as "telecommunications carriers" required to comply with CALEA.[185] Connected Vehicle Safety Systems' ad hoc networks are not open to public communications and therefore are probably not required to provide CALEA solutions. As long as Connected Vehicle Safety System DSRC communications do not interface with a public network, such as the Internet, CALEA requirements would not apply.[186] If Internet connections or other

---

182. *See Jones*, 132 S. Ct. at 949.

183. 47 U.S.C. § 1001–10 (2012).

184. The CALEA requires every "telecommunications carrier" to "ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area . . . ." 47 U.S.C. § 1002(a)(1) (2012).

185. In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd. 14989, 14993, (Sep. 23, 2005). [hereinafter 2005 FCC Order]. 47 U.S.C. § 229 authorizes the Federal Communications Commission to "prescribe such rules as are necessary to implement" CALEA requirements. 47 U.S.C. § 229(a) (2012).

186. The 2005 FCC Order isolates three factors that cause a network to be subject to CALEA compliance:

1. Electronic communication switching or transmission,
2. Replacement for local telephone service, and
3. The public interest in CALEA's application.

As a practical matter, the second factor, which is also known by the acronym SRP (Substantial Replacement Provision), is most important. A network that offers a replacement for any part of a local telephone exchange service in providing public subscribers with communication functionality (such as by interconnecting with

interconnections with publicly available communications networks were added—perhaps in the form of V2I connections—at those interconnections, CALEA solutions would be required to provide law enforcement access to DSRC communications as these communications are transmitted into and across public networks.[187]

In contrast, under the FCC's 2005 order, since Connected Vehicle Mobility Applications typically interconnect with public telecommunications networks they would need to comply with CALEA.[188] Since the nature and purpose of most Mobility Applications include connecting the vehicle to the Internet and wireless telephone carriers, these Connected Vehicle Mobility Applications will generally be subject to required "CALEA Solutions,"—i.e., law enforcement "backdoor" access points.[189]

Connected vehicle data stored outside the vehicle, for example by telecommunications carriers or application providers, is subject to the rules of access established by the Stored Communications Act (SCA).[190] Access to such stored data by law enforcement usually only requires a subpoena or possibly a "2703(d) order" based on the reasonable fact-based belief that the records are relevant and material to a criminal investigation.[191] Litigation regarding law enforcement access to mobile device information held by telecommunications carriers under the SCA has resulted in a large number of widely varied court rulings.[192] Connected Vehicle Mobility Applications are likely to result in a considerable volume of stored communications to which law enforcement may seek access. In contrast, Connected Vehicle Safety Systems do not currently plan to store V2V communications. Moreover, most V2V information is designed to be anonymous, so, even if it were stored, it would be unlikely to be of much interest to law enforcement agencies.

---

ordinary telephone networks), will be subject to CALEA compliance. Whether a communication is in the form of data or words is not relevant. 2005 FCC Order, *supra* note 185 at 15002.

187. *Id.* at 15002–03.

188. *Id.*

189. *See* 47 U.S.C. § 1002(a); *see also supra* note 184.

190. *See* 18 U.S.C. §§ 2701–12 (2012). The SCA is part of the ECPA.

191. Section 2703(d) of the SCA authorizes such orders, giving rise to the "2703(d) order" shorthand name. *See* 18 U.S.C. § 2703(d) (2012).

192. There were more than one hundred reported decisions regarding this issue at the time this Article was written. Some of the disagreement among courts with regard to 2703(d) orders is recounted in Zachary Ross, Note, *Bridging the Cellular Divide: A Search for Consensus Regarding Law Enforcement Access to Historical Cell Data*, 35 CARDOZO L. REV. 1185, 1205–11 (2014).

Routine law enforcement access to connected vehicle information would seriously undermine trust in either of these technologies. Law enforcement's use of Connected Vehicle Safety Systems communications would be particularly damaging to public confidence in these technologies that have long promised protection of users' anonymity. The invisibility of DSRC devices to vehicle drivers compounds the importance of the trustworthiness of Connected Vehicle Safety Systems not to allow extraneous uses of information from the system without the knowledge or consent of the vehicle operator.

E. Privacy

There is no doubt that privacy concerns are among the most challenging legal and policy issues connected vehicles face. In a recent GAO study of connected vehicles, the GAO identified a variety of privacy concerns, from third-party access to misuse of location information.[193] The report recounted that "one automobile manufacturer that is part of the VIIC [Vehicle Infrastructure Integration Consortium] said that it could be difficult to explain how V2V technologies work to the public without raising concerns related to privacy."[194] Nevertheless, informed consent is essential to the protection of privacy.

Connected vehicles will affect three categories of privacy interests: autonomy, personal information, and surveillance. Appropriate response to these privacy interests and concerns will affect whether the public will ultimately accept and use connected vehicles, and make these technologies useful as intangible aspects of the transportation infrastructure.

Autonomy privacy interests are sometimes the most difficult privacy interests to visualize, perhaps because autonomy refers to a person's internal sense of self-determination and capacity to make choices that affect the individual. As noted by automobile manufacturers, Connected Vehicle Safety Systems pose a particularly acute autonomy problem because the V2V system is complicated and difficult to understand.[195] The operation of V2V technology will be invisible to a vehicle driver as the DSRC transceiver sends out real-time information about the location and status of the driver's vehicle. When a V2V-equipped vehicle driver receives warnings about the

193. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 145, at 29.
194. *Id.*
195. *See id.*

behavior of nearby vehicles, those warnings will appear to come from the driver's own vehicle, rather than from the DSRC safety system embedded in the vehicle's electrical system.

The impact on autonomy privacy will be particularly acute if federal regulations are promulgated which require DSRC V2V transceivers as safety equipment, as NHTSA announced in early 2014.[196] Under such circumstances, a driver would have no choice about participating in Connected Vehicle Safety Systems communications from his or her vehicle. To the extent that Connected Vehicle Safety Systems require V2V DSRC transceivers that have no "OFF" switches, a vehicle user will be deprived of basic choices about sending out data, which reflects the driver's behavior as much as it reflects that of the vehicle. That lack of choice and control deprives users of autonomy privacy.

In contrast, Connected Vehicle Mobility Applications are more likely to have been chosen by the vehicle's driver. There are no known plans to require any of these mobility applications as a matter of law. Nevertheless, many drivers may not understand how the applications operate in capturing information about users. Drivers will likely not know what data is being pulled from the operating vehicle and transmitted to unknown and unchosen recipients by the Mobility Application. This lack of informed choice and consent will affect autonomy privacy. Dislike of such intrusions into individual autonomy could well generate privacy legislation that would return some level of choice and control to users of Connected Vehicle Mobility Applications, as was the case with regard to automobile black boxes (Event Data Recorders) in some states.[197]

Autonomy-related consumer frustration about lack of choice and control can lead to tampering with connected vehicle equipment in ways that may endanger the security of connected vehicle communications. One example of such autonomy-related tampering with newly required technology is the initial public rejection of mandatory vehicle seatbelts.[198]

Connected vehicles will also affect personal information privacy interests, primarily through misuse of personal data about individual

---

196. *See supra* note 57 and accompanying text.

197. Fifteen states have considered legislation relating to EDRs from 2009 to 2013. *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. ST. LEGISLATURES (Nov. 12, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

198. Frank Douma & Sarah Aue, *ITS and Locational Privacy: Suggestions for Peaceful Coexistence*, J. TRANSP. L. LOGISTICS & POL'Y, Mar. 2011, at 89, 96–97.

people. Connected Vehicle Safety Systems have been painstakingly designed to maximize anonymity and neither to create nor to collect personal information.[199] The considered effort to build V2V technologies to avoid collecting or using personal information, and instead to rely on anonymous information, illustrates a particularly effective strategy for dealing with personal information privacy concerns with regard to connected vehicles.

Nevertheless, even with reliance on anonymous information, it can be very difficult to prevent anonymous data from being transformed into personal information.[200] For example, outside interests, from data brokers to law enforcement agencies, may seek to intercept, record, and correlate anonymous V2V safety messages with other data that could be used to identify individual users of Connected Vehicle Safety Systems.

In contrast to the built-in anonymity of Connected Vehicle Safety Systems, Connected Vehicle Mobility Applications will generate and collect a great deal of personal information. Many of these mobility applications will be pay-for-use infotainment products and services for which the identity of the user (or at least the user's credit card information) is required through a password or other form of authentication. Information privacy concerns about potential misuse of this personal information are likely to range from opposition to the collection of personal information so that it can be sold or traded, to restrictions against use of information in behavioral advertising. A thorough discussion of these personal information concerns is provided by recent reports from the FTC,[201] the Department of Commerce,[202] and the White House.[203]

---

199. Most of the V2V technologies were developed under the guidance of the VII Privacy Policies Framework. *See* LESLIE JACOBSON, INSTITUTIONAL ISSUES SUBCOMM. OF THE NAT'L VII COAL., VEHICLE INFRASTRUCTURE INTEGRATION PRIVACY POLICIES FRAMEWORK, VERSION 1.0.2 (2007), *available at* http://financecommission.dot.gov/Documents/April2008Meetings_Hearings/VII_Privacy_Policies_Framework-Approved_by_ELT.pdf.

200. The process is called "de-anonymization" or "re-identification." *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1707–25 (2010) (providing instances and explanations of re-identification processes).

201. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

202. *See* U.S. DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010),

Surveillance privacy interests combine both concerns about personal information privacy, and concerns about autonomy privacy. Surveillance privacy interests are reflected in concerns about individuals being tracked or located without their consent, and often without their knowledge. With regard to Connected Vehicle Safety Systems, the USDOT has assured that "V2V technology does not involve . . . tracking vehicle movements. The information sent between vehicles [by DSRC] does not identify those vehicles, but merely contains basic safety data."[204]

To the extent that government agents, private investigators, or others use connected vehicles to keep track of individuals, surveillance privacy interests will be compromised. A New York Court of Appeals decision, in a case involving law enforcement GPS tracking of a criminal suspect, decried some of the privacy impacts of surveillance:

> Disclosed in the [tracking] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.[205]

Concurring in *Jones*,[206] Justice Sotomayor described her concerns about government surveillance: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[207] She also warned against "making available at a relatively low cost such a substantial quantum of intimate [location] information about any person whom the Government, in its unfettered discretion, chooses to track . . . ."[208]

---

available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

203. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

204. *See* Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57.

205. People v. Weaver, 12 N.Y.3d 433, 441–42 (N.Y. 2009).

206. United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring).

207. *Id.* at 956.

208. *Id.*

Such tracking may "'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[209]

V2V Connected Vehicle Safety Systems Basic Safety Messages, which are transmitted ten times every second, include time, location, speed, heading, and other data. Such data appear to be ideal for use in remote surveillance of vehicles and motorists. However, in response to surveillance privacy concerns, Connected Vehicle Safety Systems have been designed to maintain the anonymity of Basic Safety Messages specifically to prevent such surveillance misuse. In contrast, Connected Vehicle Mobility Applications have no such designed-in anonymity with regard to personal information. As a result, there is a substantial possibility that some Connected Vehicle Mobility Applications could be used for public sector or private sector surveillance of individuals. The potential use of Mobility Applications for surveillance and tracking of individuals has already stimulated both FTC enforcement[210] and proposed legislation.[211]

USDOT assurance that Connected Vehicles Safety Systems will not collect or store personally identifiable information[212] is a good start toward appropriately responding to privacy concerns. More broadly, connected vehicle technologies would better serve the interests of the public if they adopted express privacy protections. The Connected Vehicle Mobility Applications promoted by USDOT, as part of the transportation infrastructure, should include clear standards and performance measures with regard to privacy protection, as well as with regard to other "quantifiable benefits."[213]

---

209. *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

210. Probably the most prominent of these enforcement actions against online companies that collect and use location information without informing the person whose location is collected is *United States v. Path*. Consent Decree and Order for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Path, No. 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

211. *See, e.g.*, Location Privacy Protection Act of 2014, S. 2171, 113th Cong. (2014).

212. *See* Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57 ("V2V technology does not involve exchanging or recording personal information or tracking vehicle movements. The information sent between vehicles does not identify those vehicles, but merely contains basic safety data.").

213. *See* RESEARCH & INNOVATIVE TECH. ADMIN., U.S. DEP'T OF TRANSP., DYNAMIC MOBILITY APPLICATIONS (n.d.), *available at* http://www.its.dot.gov/factsheets/pdf/JPO-027_DMA.pdf.

F. Security

According to GAO, security of connected vehicle communications and networks poses one of the most serious unresolved challenges for both safety and mobility types of connected vehicles.[214] However, the two types of connected vehicles are markedly different with regard to the network and communications security they provide. Security appears to be a higher priority for Connected Vehicle Safety Systems than Connected Vehicle Mobility Applications.

As noted above, Connected Vehicle Safety Systems have been designed to use a sophisticated security management system to provide security certificates used in validating and authenticating the content of safety data transmitted among vehicles and maintaining the security of the networks.[215] Connected Vehicle Safety Systems plan to use PKI[216] cryptography for security certificates that will accompany each V2V Basic Safety Message to assure trustworthiness and security.[217] These security certificates also enable DSRC transceivers to detect and report messages from what appear to be misbehaving DSRC transceivers. For example, a DSRC device may be babbling nonsense, providing inaccurate information, or showing signs of having been hacked. The security certificate management system facilitates reporting such malfunctioning devices so that the certificates used by the malfunctioning devices are revoked automatically. DSRC devices automatically ignore incoming messages that lack valid certificates. The security certificates used by DSRC devices to validate their transmissions need to be issued by a trusted third party. At present, the security certificate management authority is rather generally described. Yet to be determined are such matters as how many certificates should be issued, at what intervals, or the process for issuing the certificates.

Indeed, many of the technical specifications regarding how certificates will be provided, how often they will change, and who will manage their distribution and revocation, are all matters that remain to be decided. In the February 3, 2014 announcement that NHTSA

---

214. *See* U.S. GOV'T ACCOUNTABILITY OFFICE *supra* note 145, at 20–23.

215. *See supra* notes 76–91 and accompanying text.

216. *See generally*, JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY, 241–95 (Chapman & Hall 2008) (describing PKI encryption). The IEEE P1363 project develops Standard Specifications for Public-Key Cryptography. *See Standard Specifications for Public-Key Cryptography*, INST. OF ELEC. AND ELECS. ENG'RS, http://grouper.ieee.org/groups/1363/ (last modified Oct. 10, 2008).

217. DELGROSSI & ZHANG, *supra* note 75, at 159–65, 209–37.

would move forward toward regulations requiring V2V Connected Vehicle Safety System technologies as mandatory safety equipment, NHTSA assured the public:

> The information sent between vehicles does not identify those vehicles, but merely contains basic safety data. In fact, the system as contemplated contains several layers of security and privacy protection to ensure that vehicles can rely on messages sent from other vehicles and that a vehicle or group of vehicles would be identifiable through defined procedures only if there is a need to fix a safety problem.[218]

Nevertheless, Ed Adams, a researcher at a company that helped write safety and privacy features into the computer language for the V2V DSRC pilot programs, is concerned: "A lot of us in the security world are just waiting for the next major attack in infrastructure and auto."[219] Adams added, "[w]e're doing our best to make it as secure as possible, but it's just not a realistic goal to make a car's 100 million lines of code hackerproof."[220]

Connected Vehicle Mobility Applications do not have a comprehensive security policy or program. Articles with such titles as *Will Car-Hacking Become the New Carjacking?*[221] have become almost commonplace with regard to the security of these applications. According to the *Wall Street Journal Market Watch*, the need for better security is clear:

> There were more than 26 million connected cars on the road last year, a figure that will rise to 152 million by 2020, the industry group IHS Automotive estimates. Many cars collect location-based data to give drivers turn-by-turn directions, for example, and some have lane assistance features that use radars to keep the vehicle from drifting, or to track diagnostics. In the future, drivers can expect to stream music, download apps, navigate with heads-up touch-screen displays and even alert people when they're drowsy behind the wheel or when their blood sugar is low . . . .[222]

Connected Vehicle Mobility Applications information and communications need to be secure. However, often they are not.

---

218. Press Release, Nat'l Highway Traffic Safety Admin., *supra* note 57.

219. Jose Pagliery, *Talking Cars: The Next Hacking Target*, CNN MONEY (June 10, 2014), http://money.cnn.com/2014/06/10/technology/security/talking-cars-hacking/.

220. *Id.*

221. *See* Priya Anand, *Will Car-Hacking Become the New Carjacking?*, MARKETWATCH (Sept. 13, 2014), http://www.marketwatch.com/story/will-car-hacking-become-the-new-carjacking-2014-06-03/print.

222. *Id.*

Researchers have repeatedly hacked into connected cars with mobility applications—sometimes through breaking into an application's out-of-vehicle servers.[223] Within the vehicle, all that seems to be required is to plug a device into a car's electronic control units through the OBD2 data ports that are required in cars built since the 1990s. Chris Valasek, director of security intelligence at the computer security company IOActive, noted that an "Internet connection could make hacking remotely easier . . . ."[224]

At present, most of the effort to enhance cybersecurity in connected vehicles appears to take the form of research by the automobile industry and security consultants. Eventually, the transportation infrastructure discussed in this Article will require a comprehensive security framework that interconnects the various parts and types of Connected Vehicles. Taking seriously the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology (NIST) in 2014, would provide a good start.[225] NIST's Critical Infrastructure Framework provides cybersecurity vulnerability management strategies and program performance metrics for both public and private infrastructure cybersecurity.[226] The Framework's purpose is to facilitate proactive management of cybersecurity vulnerabilities in the nation's critical infrastructure, including transportation.[227] Such an approach has proved effective in reducing the potential for successful cyber-attacks on both private and public infrastructure. As Connected Vehicle technologies become an integral part of the transportation infrastructure, the importance of such high-level cybersecurity to Connected Vehicles will become ever more vital.

CONCLUSION

The Connected Vehicle technologies discussed in this Article create a new type of information infrastructure that can transform physical ground transportation infrastructure in highly beneficial ways. These technologies remain under development and face many challenges, some of which have been discussed in this Article.

---

223. *Cf.* Glaskin, *supra* note 113, at 40–41.

224. Anand, *supra* note 221.

225. *See* NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0 (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

226. *Id.* at 1–2.

227. *Id.*

Connected Vehicles can avoid or prevent many vehicle-related fatalities and car crashes, waste of resources, and environmental health problems, and can expand the capacity of existing infrastructure to handle more vehicles more safely, securely, and efficiently.

Future applications of these Connected Vehicle technologies will foster more efficient ways for people to use existing physical ground transportation infrastructure. Consider the ability of this invisible transportation infrastructure to avoid "blind" intersection accidents through V2V safety warnings about oncoming vehicles around a corner or out of sight. Also consider the ability of Connected Vehicle technologies to help drivers avoid traffic bottlenecks through Connected Vehicle Mobility Applications that have provided warnings and guidance about using alternative routes. Consider also the potential for platoons of cars or trucks joined closely together by V2V wireless connectivity to save time, fuel, and wear and tear on drivers and to make more efficient use of roadways. If an impending storm or natural disaster necessitates evacuation of an area, these same Connected Vehicle Mobility Applications, together with V2V Safety Systems, can enable orderly, efficient, and even life-saving ways out of areas threatened by high water or high winds.

When the transportation infrastructure begins to accommodate driverless cars, V2V Connected Vehicle Safety Systems data exchanges will provide critical positional signals and roadway status data essential for safe vehicular travel without human drivers. Although it seems likely that driverless vehicle technology will also rely on other vehicle sensors, there will be circumstances in which the precise positioning and traffic information available from V2V safety messages will be indispensable. In such a future, the invisible information-based transportation infrastructure will be just as important as the physical roadways that carry ground transportation.