Before the
National Highway Traffic Safety Administration
Washington, D.C. 20590

In the Matter of	)	
	)	
Federal Motor Vehicle Standards;	)	
V2V Communications	)	Docket No. NHTSA-2016-0126

COMMENTS OF PUBLIC KNOWLEDGE, CONSUMER FEDERATION OF AMERICA, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Michael Calabrese
New America's Open Technology Institute
740 15th Street NW, Suite 900
Washington, D.C. 20005
(202) 986-2700

John Gasparini
Public Knowledge
1818 N Street NW, Suite 410
Washington, D.C. 20036
(202) 861-0020

Jack Gillis
Susan Grant
Consumer Federation of America
1620 I Street NW, Suite 200
Washington, D.C. 20006
(202) 387-6121

April 12, 2017

Public Knowledge and New America's Open Technology Institute (collectively, "Commenters") write today in response to the National Highway Traffic Safety Administration ("NHTSA")'s Notice of Proposed Rulemaking[1] ("NPRM") regarding the mandating of Dedicated Short-Range Communications ("DSRC") for Vehicle-to-Vehicle ("V2V") communications. We write to express concerns about the implementation of DSRC as currently detailed in the NPRM. Specifically, we raise concerns regarding the potential for non-safety uses of DSRC spectrum and radios, cybersecurity, and privacy risks associated with DSRC, and the implications this mandate may have for ongoing efforts to find ways to share the 5.9 GHz band with non-DSRC unlicensed users. Commenters urge that, as NHTSA considers moving forward, it ensures that any further steps it takes take steps to address the concerns outlined below

I. THE DEPLOYMENT OF COMMERCIAL APPLICATIONS ON DSRC PLATFORMS AMPLIFIES CONCERNS REGARDING CYBERSECURITY, PRIVACY, AND ROAD SAFETY.

A. Commercialization of the DSRC Service Amplifies Concerns about Cybersecurity, Privacy, and Safety.

NHTSA's stated objective in pursuing a mandate for DSRC is to "revolutionize motor vehicle safety," specifically by "reduc[ing] the number and severity of motor vehicle crashes, thereby reducing the losses and costs to society that would have resulted from these crashes."[2] This is an admirable goal, and one which Commenters share. The support for this objective in the ANPRM record, and throughout the public debate on the DSRC issue, is unanimous. It is worrying, however, that in pursuing this laudable goal, the door remains open to commercialization[3] of the DSRC service. The FCC's service rules do not presently prohibit commercialization of DSRC technology, though a Petition for Rulemaking submitted by Commenters to that body remains pending.[4] NHTSA's NPRM neither mandates nor prohibits

[1] *Federal Motor Vehicle Safety Standards; V2V Communications*, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017) ("NPRM").
[2] *Id*. at 3855.
[3] By "commercialization", Commenters refer collectively to any application or service deployed using DSRC radios or DSRC-allocated spectrum that serves a purpose directly or indirectly linked to revenue-generating private industry activities. Toll payment, for example, would not be included, as it serves a public goal of facilitating more efficient use of road systems. Wireless payments at McDonald's or a gas station, however, would qualify as commercialization because they do not further a life and safety end or meet some other public purpose. Even more clearly, infotainment applications, particularly those already provided by general-purpose commercial networks, would fall in the realm of commercialization. However, functions that serve safety and public policy purposes, such as preventing collisions, increasing road safety, streamlining traffic, reducing congestion, or helping to limit emissions, would of course not fall under any reasonable definition of "commercialization."
[4] Consumer & Governmental Affairs Bureau Reference Information Center Petition For Rulemaking Filed, *Public Notice*, Docket No. RM-11771 (rel. Jul. 25, 2016).

any particular category of applications from being deployed on DSRC services.[5] The only extent to which the NPRM speaks to functionality of DSRC units is in the narrow space focused on Basic Safety Messages. There is no reason an automaker could not deploy an additional DSRC radio to facilitate non-commercial services in the DSRC band, but the NPRM does not appear interested in addressing this concern.

The cybersecurity risks arising from commercialization are fairly straightforward. Even to the extent a DSRC system, or the automotive system as a whole, is secure, connecting it to a commercial network, or more broadly to the whole internet, introduces a whole host of new vulnerabilities. As discussed in Section III, below, substantial cybersecurity risks exist with DSRC as currently proposed. Permitting connection of DSRC devices and cars themselves, which already exhibit substantial cybersecurity weaknesses, only enhances the vulnerability by exposing automotive systems to the broader internet and creating additional attack vectors. In conjunction with a mandate for DSRC connectivity, the absence of limitations on commercialization on the band amplifies privacy and security concerns, as it vastly expands the scope of applications whose impact might need to be considered by regulators.

In defense of commercialization, the auto industry ignores the issue of commercialization and does not comment on its implications, focusing exclusively on cybersecurity as it pertains to Basic Safety Messages.[6] The auto industry emphasizes only safety applications for DSRC. However, the FCC's current service rules for the band incorporate numerous categories of applications that may utilize DSRC technology and spectrum.[7] Not all of these applications are safety-related, or even related to broader transportation policy goals, such as improving efficiency of road use, reducing congestion, or curtailing emissions.[8]

Functions contemplated in the FCC's rules include gas payment, drive-thru payment, rental car processing, parking lot payment, and access control rental car processing.[9] These functions are described as "safety-related" though the examples above suggest otherwise. While Commenters recognize that NHTSA is not the appropriate venue to seek redress for these concerns, it nevertheless warrants consideration in this proceeding, as the technology contemplated by this NPRM's mandate specifically permits these non-safety functions, yet the

[5] NPRM at 3858.
[6] *See, e.g.,* Opposition of General Motors, Docket No. RM-11771 (Aug. 24, 2016); Opposition of Alliance of Automobile Manufacturers and Association of Global Automakers, Docket No. RM-11771 (Aug. 24, 2016).
[7] Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band), *Report and Order*, WT Docket No. 01.90, FCC 03-224, Appendix C (rel. Feb. 20, 2004).
[8] *Id*.
[9] *Id*.

NPRM remains silent regarding any concerns stemming from these plainly commercial applications.

B. NHTSA Has Authority to Address Commercial Applications, but the NPRM Remains Troublingly Silent on This Important Issue.

Despite NHTSA's broad authority to oversee devices attached to or integrated with motor vehicles, the NPRM is silent on non-safety uses of DSRC technology. In discussing regulation of V2V technology, NHTSA describes its authority under the Safety Act as "broad enough to comfortably accommodate this evolution in vehicle technologies."[10] Specifically, the NPRM goes on to state, in relevant part, that NHTSA's authority over "V2V-related motor vehicle equipment" extends, in part, to any integrated original or aftermarket equipment used for V2V communication, and any software that "provides or aids V2V functions."[11] Notably, in discussing roadside equipment, the NPRM also notes that NHTSA does not agree that "a device that performs non-safety functions in addition to safety functions is necessarily not motor vehicle equipment."[12]

In other words, a DSRC system that performs non-safety functions in addition to safety functions would remain at least in part under the oversight of NHTSA. Commenters agree , but are concerned that despite this position, the NPRM remains silent on issues raised by the deployment of commercial applications on DSRC radios and in DSRC spectrum. NHTSA can and should seek comment on whether such operations should be permitted, and whether it is necessary to permit automakers to deploy such services, particularly in an environment where DSRC is already mandated and non-safety functions may not be needed to further incentivize consumer adoption of the technology. The potential for deployment of commercial services using DSRC systems is deeply concerning to Commenters, and the NPRM's silence on the point amplifies concerns discussed elsewhere in these comments regarding privacy and cybersecurity.

II. IMPLEMENTATION OF DSRC AS CURRENTLY PROPOSED PRESENTS SUBSTANTIAL CYBERSECURITY RISKS WHICH CAN AND SHOULD BE RECTIFIED BEFORE EXPANDING DEPLOYMENT.

Commenters also write to express substantial concerns relating to the cybersecurity implications of the mandated deployment of DSRC as currently proposed. In particular, we echo the concerns raised by Alex Kreilein of SecureSet in his paper, "Security Considerations for Connected Vehicles & Dedicated Short Range Communications."[13] The paper presents specific

[10] NPRM at 3957.
[11] *Id*.
[12] *Id*.
[13] Comments of Alex Kreilein and SecureSet, Docket No. NHTSA-2016-0126 (Mar. 26, 2017) ("SecureSet Paper").

recommendations to adequately address the cybersecurity issues presented by a mandate for DSRC, and to ensure that an adequate framework is in place to ensure the long-term success and safety of any deployment.

While the NPRM makes substantial forward strides on cybersecurity issues, it falls short of proposing adequate solutions. For example, the NPRM presumes, on the topic of security updates, that they need not be mandated on consumers, as "we assume that, at this point in time, nearly all consumers are already well-accustomed to the need for software updates on their electronic devices . . . and regularly accept and initiate such updates."[14] Commenters respectfully suggest that this impression may be ill-founded. For example, a study by Ubuntu in December 2016 found that "only 31% of consumers that own connected devices perform updates as soon as they become available."[15] Furthermore, "40% of consumers have never consciously performed updates on their devices."[16] "Of those polled, nearly two thirds felt that it was not their responsibility to keep firmware updated. 22% believed it was the job of software developers, while 18% consider it to be the responsibility of device manufacturers."[17] In sum, Ubuntu writes, "Consumers cannot (and should not) be expected to stay on top of every hack and critical software update; it's simply not realistic. Nor do consumers particularly see this as their problem to solve."[18] Research from the Pew Research Center supports these views, finding that consumers lack significant understanding of a number of cybersecurity issues.[19]

Consumers do not routinely update their software, nor do providers necessarily routinely update their software, to address every security threat. In the case of a smartphone, this is concerning but not life-threatening. That is not the case with automobiles. The threat to safety posed by an unsecure car is far greater than that posed by computers or smartphones referenced as examples in the NPRM. While it is laudable that the NPRM proposes mandating the means for over-the-air updates to be received and installed, the NPRM stops short of ensuring that those updates will be adopted. This is a mistake. The Safety Act, on whose authority NHTSA relies for this proposed mandate, obligates NHTSA to work to keep road users safe. NHTSA's approach to cybersecurity here falls short of that goal.

In sum, while the NPRM devotes substantial column inches to the issue of cybersecurity, the approach proposed falls far short of the kinds of protections necessary to ensure consumer

[14] NPRM at 3957.
[15] Thibault Rouffineau, Ubuntu, *Research: Consumers are terrible at updating their connected devices* (Dec. 15, 2016), https://insights.ubuntu.com/2016/12/15/research-consumers-are-terrible-at-updating-their-connected-devices/.
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] Kenneth Olmstead and Aaron Smith, *What the Public Knows About Cybersecurity* (March 22, 2017), *available at* http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/#cybersecurity-knowledge-varies-widely-by-topic-and-level-of-technical-detail.

safety is enhanced by the deployment of DSRC technology. Practices including defense-in-depth, better update policies, and other enhanced cybersecurity practices developed and adopted by industry stakeholders in a collaborative process must be put in place as DSRC moves forward.

III. NHTSA'S NPRM LEAVES THE DOOR WIDE OPEN FOR INTRUSIVE PRIVACY-VIOLATING COMMERCIAL APPLICATIONS.

The NPRM expressly states, in what NHTSA suggests is an adequate privacy disclosure to be included with new cars, that "NHTSA does not regulate the collection or use of V2V communications or data beyond the specific use by motor vehicles and motor vehicle equipment for safety-related applications."[20] It continues, noting that "individuals and entities may use specialized equipment to collect and aggregate . . . V2V communications and use them for any purpose including applications such as . . . commercial purposes." NHTSA expressly contemplates, in fact, that "commercial entities also may use aggregate V2V messages to provide valuable services to customers, such as traffic flow management and location-based analytics, and for other purposes **(some of which might impact consumer privacy in unanticipated ways.) NHTSA does not regulate the collection or use of V2V data by commercial entities or other third parties.**"[21]

While the NPRM is silent on the cybersecurity implications of commercialization, in the privacy space, NHTSA washes its hands of any concerns and moves forward without a second thought. To wit, the auto industry has not exactly been coy about its views on the sorts of privacy policies consumers might expect from these "other entities or other third parties."[22] In comments to Politico in July 2016, Steve Bayless, Vice President for Technology Markets at Intelligent Transportation Society of America, said that "on the commercial side, it's whatever the privacy policy of the application provider is . . . That's the way it is for most applications, like Facebook."[23] What Mr. Bayless, and NHTSA, both overlook is that consumers can choose not to use Facebook. Consumers can choose not to let Facebook track their locations, and consumers can choose whether Facebook is installed on their phones, accessed on their computers, or connected to their lives. Consumers will not be able to choose not to have DSRC, and if the current approach to marketing infotainment systems and connected car features from the auto industry is any indication, consumers won't be able to opt out of this sort of data collection, or choose whether or not Facebook is installed in their cars.

---

[20] NPRM at 3927.
[21] *Id*.
[22] *Id*.
[23] Margaret Harding McGill, *Latest privacy debate: Crash-avoidance technology*, Politico (June 28, 2016), *available at* https://www.politicopro.com/transportation/story/2016/06/latest-privacy-debate-crash-avoidance-technology-117891.

For NHTSA to be silent on this point, and to go so far as to effectively bless widespread data collection and commercialization, describing the results as "valuable services to customers," belies the incompleteness of NHTSA's approach to consumer privacy as contemplated by this mandate. While it may be the case that the BSMs transmitted by DSRC units are not stored if not needed for safety purposes, NHTSA goes so far as to almost explicitly bless hardware and applications being built into vehicles to serve that precise purpose. Given the breadth of jurisdiction NHTSA describes elsewhere in the NPRM,[24] it is not plausible to believe that the choice to avoid addressing the commercial uses of sensitive customer data stems from any concern about legal authority. This can only be read as an affirmative choice on the part of NHTSA to permit and facilitate unrestricted data collection and monitoring of consumers via mandatory DSRC units and NHTSA inaction regarding third-party data collection and use.

Commenters also urge NHTSA to reconsider its views regarding the ability of DSRC to provide information sufficient to individually identify or track vehicles. The SecureSet whitepaper on DSRC discusses the latter issue in detail, noting that "it is unclear to this researcher why the MAC is broadcast unencrypted. But its unencrypted broadcast substantially risks the privacy and personal security of the vehicle. It does, however, enable easy content delivery of a targeted nature, such as DSRC-delivered advertisements to vehicles."[25]

Additionally, the NPRM's assertion that "V2V transmissions would exclude data directly identifying a private motor vehicle or its driver or owner and reasonably linkable to an individual via data sources outside of the V2V system or over time"[26] is at best aspirational. While data aggregation and anonymization have historically been relied upon to protect consumers, more recent research suggests that "adversaries can often reidentify or deanonymize the people hidden in an anonymized database."[27] In conjunction with the ability identified in the SecureSet paper to track individual vehicles, assertions by NHTSA that privacy is not threatened by DSRC, that tracking is not easily possible, and that they will take no action regarding the collection, use, or sale of aggregate data, these facts present a deeply concerning reality: consumers will be saddled with a mandatory tracking system that will not effectively protect their privacy from commercial or other interests.

As the NPRM states, the purposes of the DSRC V2V mandate are to improve road safety, save lives, reduce economic harm from auto collisions, and enhance the efficiency of the use of our roadways.[28] None of these functions require commercialization, nor would any of them be hindered by a prohibition on commercialization. And yet, the NPRM is silent on

---

[24] *See* NPRM at 3957.
[25] SecureSet Paper at 10.
[26] NPRM at 3926.
[27] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1703 (2010).
[28] *See* NPRM at 3855-56.

commercialization in the cybersecurity sections of the NPRM, the auto industry has carefully avoided the subject at the FCC, and most concerning, the NPRM appears to explicitly endorse the collection, packaging, and sale of information for profit. These concerns must be addressed as V2V technologies move forward.

IV. RE-CHANNELIZING THE ITS BAND CAN BEST ACHIEVE THE PUBLIC INTEREST IN BOTH SAFETY-OF-LIFE DSRC AND GIGABIT WI-FI CONNECTIVITY

The NPRM seeks "comment on the costs and benefits of each [band-]sharing proposal, and whether and how [NHTSA] should consider each of these approaches relative to this proposed rule."[29] As the Commenters explained in greater detail in FCC comments last year, as consumer advocates we believe both the DOT and FCC should conclude that the re-channelization approach to sharing the ITS band strikes the best balance between NHTSA's legitimate interest in promoting crash avoidance and the Commission's interest in promoting more fast and affordable broadband connectivity.[30] A re-channelization of DSRC that physically separates life-and-safety DSRC channels from other channels shared with unlicensed operations can best address agency and automaker concerns about potential interference with V2V and other time-critical safety applications, while allowing both commercial DSRC applications and unlicensed uses to share the lower portion of the band in the most efficient and productive manner.

A. Shared Use of the Band Should be Based on the Critical Distinction Between Safety of Life and Other Non-Real-Time DSRC Applications

The critical factor in striking this balance is the distinction between real-time safety and other non-safety (or non-time-critical) DSRC applications. Even among safety-related DSRC applications, it is important to distinguish between applications that can tolerate a degree of latency (e.g., the exchange of traffic flow and other informational data between vehicles and roadside units) and those that cannot (e.g., V2V crash avoidance signaling and first responder incident communication). By dedicating three channels exclusively to DSRC safety applications – including the dedicated 10 megahertz BSM channel essential to real-time V2V crash avoidance alerts – the re-channelization proposal advanced by Qualcomm, Broadcom and the Wi-Fi Alliance virtually eliminates the risk of interference with safety-of-life applications, while at the same time adhering to the FCC's evolving principles of spectrum efficiency and flexibility that

[29] NPRM at 3886.
[30] *See* Comments of Open Technology Institute, Public Knowledge, et al., in response to FCC Public Notice, *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49 (July 7, 2016).

require public safety allocations to be narrowly defined and "limited" to "the amount of spectrum . . . which ensures that those [compelling public interest] objectives are achieved."[31]

Real-time V2V safety-of-life applications are inherently narrowband and designed to require only a fraction of the 75 megahertz of spectrum currently allocated for ITS and DSRC technology. Basic safety messages (BSMs) are designed to be simple transmissions, broadcast in all directions by an onboard DSRC antenna, that include information on the vehicle's speed, heading, braking status, and other details on its current state. Safety-of-life applications require real-time transmission of small amounts of data on the order of 100 to 500 bytes of information per transmission with a general latency requirement of 100 milliseconds or less.[32] NHTSA and international regulatory bodies acknowledge the narrowband character of V2V safety communications and emphasize that the real-time reliability of the BSMs communicated between vehicles is what's most critical.[33]

Accordingly, NHTSA's proposed V2V mandate requires that all basic safety messaging between vehicles (V2V) use a single, dedicated 10 megahertz channel – the Basic Safety Messaging (BSM) channel.[34] As a result, most of the ITS band will not be used for real-time crash avoidance or public safety purposes. Additional real-time public safety applications – such as communication between first responder vehicles, or interactions with roadside units – must be accommodated, but they will still occupy only a fraction of the band's capacity. DSRC proponents also argue that some safety-related V2I communications may be time-sensitive. However, as a 2014 technical study by CableLabs explained, most of the safety-adjacent V2I services envisioned for the DSRC band—stop signal warnings, reduced speed warnings, railroad crossing warnings, weather warnings, and the like—likely will not require the low latency that

---

[31] *Report of the Spectrum Policy Task Force*, ET Docket No. 02-135 (Nov. 2002), at 41, *available at* http://sites.nationalacademies.org/cs/groups/bpasite/documents/webpage/bpa_048826.pdf. *See also* FCC, "Report of the Spectrum Efficiency Working Group," Spectrum Policy Task Force (2002), at 34-36, *available* https://transition.fcc.gov/sptf/files/SEWGFinalReport_1.pdf.

[32] Harding, J. et al., *Vehicle-to-vehicle communications: Readiness of V2V technology for application,* National Highway Traffic Safety Administration, Report No. DOT HS 812 014, at 98 (Aug. 2014) ("*V2V Readiness Report*"). *See also* National Highway Traffic Safety Commission, *Vehicle Safety Communications Project: Task 3 Final Report – Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, at 141 (March 2005).

[33] *See* NCTA Comments to Department of Transportation National Highway Traffic Safety Administration, NHTSA Docket No. 2014-0022 (filed Oct. 20, 2014), at 13-14; *See also HSTP-CITS-Reqs Global ITS Communication Requirements*, ITU Technical Paper (Jul. 11, 2014), at 11-12 ("Safety applications do not require high bandwidth"), *available at* http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ITS-2014-REQS-PDF-E.pdf.

[34] NPRM at 3885. In the *V2V Readiness Report*'s section discussing three potential V2I applications – real-time traffic information, weather updates and Applications for the Environment (AERIS) – NHTSA cautions that other DSRC applications must not congest the BSM channel. "It is critical that safety messaging not be compromised due to broadcasting more data for V2I." *V2V Readiness Report* at 13.

BSMs rely upon.[35] Time-sensitive V2I warnings could also potentially travel on one of three reserved public safety channels.

In contrast to V2V and other time-sensitive safety applications, commercial and informational DSRC applications will generally be wider-band transmissions, less delay-sensitive and typically require connectivity to the Internet or other external data sources (that is, backhaul to cloud services).[36] From the outset, the auto industry has emphasized other potential DSRC applications in addition to real-time V2V safety. These non-safety-of-life apps range from navigation assistance (e.g., turn-by-turn directions), mobile tolling and parking payments, real-time traffic and weather updates, in-vehicle displays of advertising and roadside signage, among others.[37] These applications are clearly useful, but are also generally "ancillary" to the core safety-of-life applications that narrow-band DSRC signaling enables on a single V2V safety channel.[38]

Moreover, most of the informational services DSRC technology is touted to deliver are *already* publicly available via smartphone applications and other mobile edge providers that include Apple CarPlay, Android Auto, Mirrorlink and OEM-designed integrations of cellular connectivity. And as ubiquitous, high-speed cellular and Wi-Fi connectivity increasingly give drivers and their passengers the ability to access any mobile app or service anywhere, the utility, efficiency and equity of an exclusive and free band of spectrum for competing auto industry *commercial* applications is rightly called into question. And however useful these non-safety (or

---

[35] Rob Alderfer, et al., "Optimizing DSRC Safety Efficacy and Spectrum Utility in the 5.9 GHz Band," CableLabs (Oct. 2014), at 8, 13-14, attached to FCC Comments of NCTA – The Internet & Television Association, *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49 (July 7, 2016), *available at* https://goo.gl/1adkOo. Section IV. C of the CableLabs paper describes the European conclusion that safety-related functions can limited to 30 megahertz of spectrum.

[36] According to one study, "other drivers of near-future growth include the increased availability of high-speed wireless networks and cloud-based data services around the world, and the development of application programming interfaces (APIs) needed to create connected car software." Richard Vierecki et al., *Connected Car Study 2015: Racing ahead with autonomous cars and digital innovation*, Strategy& (Sep. 16, 2015), at p. 11, *available at* http://www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/connected-car-2015-study. Another found that "telecom operators are often said to be nervous about being restricted to the role of data pipe providers," but that "within the automotive industry, there is an opportunity to become much more if embedded telematics becomes the long-term de-factor connectivity method." GSMA and SBD, *2025 Every Car Connected: Forecasting the Growth and Opportunity*, at 2 (Feb. 2012), *available at* http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsma2025everycarconnected.pdf.

[37] *See generally* Michael Calabrese, *Spectrum Silos to Gigabit Wi-Fi – Sharing the 5.9 GHz 'Car Band'*, Open Technology Institute at New America *(Jan. 2016)* ("*OTI 5.9 GHz Report*")*, available at* https://goo.gl/RY8M09.

[38] *See* Alderfer, et al., *Optimizing DSRC Safety Efficacy and Spectrum Utility in the 5.9 GHz Band*, Attachment to Comments of NCTA to NHTSA, at 10 (Oct. 20, 2014). "A variety of other services have been envisioned by DSRC stakeholders, though these services are generally ancillary to NHTSA's core interest in V2V safety and are at an even more nascent stage of development."

non-time-critical) DSRC applications may prove to be, as consumer advocates Commenters believe that NHTSA should limit its own regulatory intervention to a determination of how many DSRC channels are necessary to facilitate and safeguard time-critical V2V and related safety applications.

B. The European Union has Concluded 20 MHz is Sufficient for V2V and Related Time-Critical Road Safety Applications

Global developments reinforce the fact that real-time safety applications using DSRC require at most 30 megahertz of the larger 5.9 GHz band. Both the EU and Japan have allocated considerably less spectrum specifically for safety-related DSRC systems. In Europe, regulators concluded that two DSRC channels (20 megahertz) are sufficient for "time critical road safety applications" and another 10 megahertz for non-critical but safety-related applications. Japan has taken an entirely different approach, focusing on non-time critical roadside applications (e.g., tolling) and in any case uses entirely different bands of spectrum than the U.S. and Europe.

In 2008 the Electronic Communication Committee (ECC) of the European Conference of Postal and Telecommunications Administrations (CEPT) issued decisions allocating the spectrum band from 5855 to 5925 MHz for potential ITS use.[39] While this is nearly identical to the current U.S. allocation, there are notable differences. The CEPT makes a clear distinction between the allocation for critical safety and non-safety ITS services. "Traffic Safety Applications" (including non-critical but safety-related applications) are specifically allocated a 30 MHz block in the middle of the band, from 5875 to 5905 MHz.[40]

In Europe, the bottom 20 MHz (5855 MHz to 5875 MHz) is specifically allocated for "non-safety applications" for ITS on a shared basis with license-exempt devices. The 150 MHz immediately below 5875 MHz – which includes the spectrum corresponding to the lowest 25 MHz of the U.S. allocation for ITS (5850 to 5875 MHz) – is allocated for ISM (unlicensed) devices and a diverse array of Short Range Devices that use shared frequency bands on a license-exempt basis.[41] Finally, the top 20 MHz of the band (5905 MHz to 5925 MHz) is not actively allocated to ITS services, but instead is reserved and "to be considered for future ITS extension."[42]

---

[39] *See* Electronic Communications Committee, "The harmonized use of the 5875-5925 MHz frequency band for Intelligent Transport Systems (ITS)," ECC Decision (08)01 (amended Jul. 3, 2015), *available at* http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCDEC0801.PDF.

[40] *See* Electronic Communications Committee, *The European Table of Frequency Allocations and Applications In The Frequency Range 8.3 kHz to 3000 GHz* (May 2015), at 121, *available at* http://www.erodocdb.dk/docs/doc98/official/pdf/ERCRep025.pdf.

[41] *Id*. *See also* European Commission Digital Agenda for Europe, "Short Range, Mass Market" (May 9, 2014), *available at* http://ec.europa.eu/digital-agenda/en/short-range-mass-market.

[42] *See* ECC Decision (08)01, *supra* note 130.

The CEPT decision acknowledges that ITS safety applications do not require a full 75 MHz of bandwidth, stating:

> CEPT/ECC studies regarding the necessary spectrum requirements for road safety and traffic efficiency within the 5.9 GHz band based on accepted traffic scenarios with both IVC and I2V communication have confirmed that **a realistic estimate of the needed bandwidth is between 30-to-50 MHz <u>including 20 MHz of bandwidth for time critical road safety applications</u>**.[43]

In addition, as NHTSA has acknowledged, the EU is not contemplating a V2V mandate and is pursuing a "market-driven" approach that does not emphasizes V2V for critical safety signaling. Rather, it supports communication with infrastructure and other networks to enhance mobility and sustainability applications.[44] "While the EU has defined crash-critical safety applications as well, the priority in the EU is driver safety advisories (not safety-critical warnings), driver support messages (such as eco-driving), and commercial applications such as insurance," NHTSA reports.[45]

Japan's ITS spectrum allocation is not harmonized at all with the U.S. or Europe. Japan has assigned 80 MHz for connected car services in the band below 5850 MHz (from 5775 to 5805 MHz and 5815 to 5845 MHz), in what are the license-exempt ISM bands in the U.S. and Europe.[46] Japan also has a limited allocation for Advanced Safety Vehicle (ASV) functions of V2V and V2I in the 760 MHz band.[47] As NHTSA acknowledges, Japan is "appears likely to proceed with a two-band solution" that focuses, as in Europe, on vehicle to infrastructure communication.[48] And neither band corresponds to the U.S. allocation.

---

[43] *See* Explanatory Memorandum for ECC/DEC/(08)01, *available at* http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCDEC0801.PDF.
[44] *V2V Readiness Report*, *supra* note 31, at 116.
[45] *Ibid.*
[46] *See* Hideki Hada, "Intelligent Transportation Systems: Opportunities for Communication-Based Driving Support," Toyota Technical Center (2011), at 11, *available at http://www.toyota.com/csrc/printable/9Hada.pdf. See also* "Frequency Allocation Table of Japan," *available at* http://www.rf114.com/lib/download.php?code=tbl_board&seq_name=bseq&seq=765; Paul Spaanderman, "Spectrum Allocation for ITS: From Out of the EU Perspective," *available at* http://www.imobilitysupport.eu/library/imobility-forum/plenary-meetings/2015-1/5th-plenary-meeting-28-jan-2015-1/presentations/2737-18-paul-spaanderman-tno/file.
[47] *See* John B. Kenney, "DSRC: Deployment and Beyond," Presentation at Toyota InfoTechnology Center (May 14, 2015), at 10, *available at* http://www.winlab.rutgers.edu/iab/2015-01/Slides/06.pdf.
[48] *V2V Readiness Report*, *supra* note 31, at 118.

C. The Automakers' Petition for Reconsideration is Further Evidence that Re-Channelization Best Serves the Public Interest in Both Safety and Broadband

The auto industry's 2016 Petition for Reconsideration seeking to rescind the out of band emission limits adopted by the FCC for unlicensed use of the U-NII-3 band immediately below the ITS band – and immediately adjacent to BSM Channel 172 – reinforces just how easily the interference concerns of the auto industry could be addressed through re-channelization. As Public Knowledge indicated in its opposition to the industry's petition, "the Commission can -- and should – address the purported grievances of the Auto Manufacturers by relocating the life and safety channels to the top 20 MHz of the band."[49]

By re-channelizing to physically separate the life-and-safety channels from any OOBE, the automakers' concern about interference to BSMs can be completely satisfied, removing virtually all risk of interference between future Wi-Fi and V2V safety signaling. This can be done without undue delay since there are no deployments of either DSRC for safety (or any other purpose) or of 802.11ac Wi-Fi anywhere on the band and DOT is expected to give automakers a multi-year transition period before requiring the installation of at least a single-radio DSRC system in every new car sold.

When Channels 172 and 184 were designated for life and safety traffic in 2006, part of the FCC's justification was a request, from the auto industry, to separate the channels in order to relieve anticipated congestion from non-safety traffic.[50] However, as the auto industry has, for a decade since that Order, failed to deploy any DSRC systems, the anticipated congestion has never emerged. Rechannelization would allow the FCC to move forward with a sharing proposal that would benefit the broader public interest while ensuring total protection for important safety of life systems as they are deployed.

D. The Detect-and-Avoid Sharing Proposal Would Effectively Foreclose Wi-Fi and Subject Safety-of-Life DSRC to Unnecessary Interference Risk

Commenters believe that a re-channelization approach strikes a better balance between DOT's interest in promoting auto safety and the Commission's interest in promoting ubiquitous broadband connectivity and innovation. The critical factor in striking this balance is the distinction between real-time safety and non-safety DSRC applications. By dedicating three

[49] Opposition of Public Knowledge to Petition for Reconsideration of Association of Global Automakers and Alliance of Automobile Manufacturers, ET Docket No. 13-49 (June 6, 2016).

[50] Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band), WT Docket No. 01-90; 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 Communication Services, ET Docket No. 98-95, RM-9096, *Memorandum and Order*, 21 FCC Rcd 8961 (2006).

channels exclusively to DSRC safety – including the single BSM channel that NHTSA describes as essential to real-time V2V crash avoidance alerts – the re-channelization proposal greatly reduces the risk of unlicensed device interference with safety-of-life applications, while at the same time adhering to the evolving principles of spectrum efficiency and flexibility that the FCC increasingly applies to non-safety wireless services, particularly to those that are largely redundant and even subject to robust competition (such as DSRC navigation assistance, weather alerts, toll collections, etc.)

The fundamental problem with the detect-and-avoid sharing approach, as currently described, is that it would not permit the economically feasible deployment of unlicensed technologies, particularly Wi-Fi, while simultaneously failing to give V2V and other time-critical safety applications complete protection from interference. Detect-and-avoid would substantially preclude channel sharing with Wi-Fi, even on purely commercial DSRC channels, since it would require that if a DSRC signal is detected on any channel, the 100 megahertz from 5825 to 5925 MHz (which includes the adjacent top 25 megahertz of the U-NII-3 band) "will be declared busy for at least 10 seconds." If a DSRC transmission is detected on any one of the seven DSRC channels – regardless of spectral proximity or whether the transmission relates to a V2V safety or a non-safety commercial application – this forecloses access for unlicensed devices to the entire 75-megahertz band.

Vacating the entire band if any DSRC transmission is detected on any channel across a 100 megahertz range is an extreme restriction that may effectively exclude Wi-Fi from the band. Motorized vehicles and roads are ubiquitous. If V2V is widely deployed, 802.11ac Wi-Fi and other unlicensed technologies – no matter how low their transmit power – could only operate indoors and away from windows, in places where the constant patter of mandated V2V safety signaling is not detectable. Although the proposed V2V mandate would apply only to a single 10 megahertz channel designated for real-time V2V signaling, the detection of the V2V Basic Safety Message on this 10 megahertz BSM channel precludes, for all practical purposes, the use of 100 megahertz of spectrum capacity for the vast majority of Americans. This would cripple the utility of Wi-Fi over this spectrum for individual consumers as well as for wireless ISPs, small retailers, schools, local governments and virtually all other Wi-Fi users.

An effective indoor-only restriction would be particularly crippling, since consumers increasingly rely on mobile devices and seamless connectivity as they move between locations. Such an extreme detect-and-avoid requirement seems likely to deter widespread use of the additional 80 and 160 MHz 802.11ac channels that would otherwise be available. The cable industry, which has deployed over 400,000 Wi-Fi hotspots in heavily-trafficked outdoor areas, has stated it is not aware of any outdoor Wi-Fi hotspot deployments in the U.S. that use the portions of the 5 GHz band subject to the DFS requirement that requires unlicensed WLAN deployments to detect and avoid military radar. The detect-and-avoid proposal for sharing 5.9

GHz would seem to create even stricter and more costly limitations and uncertainties about availability.

In short, the detect-and-avoid proposal for sharing across the entire ITS band would effectively fragment the U-NII bands, require a complete retooling of existing 802.11ac devices, and increase device costs – all of which undermine the FCC's goal in proposing the 5.9 GHz band as an extension of the U-NII bands for wide-channel use by 802.11ac Wi-Fi. In contrast, the FCC's proposal to allow unlicensed operations above 5850 MHz under rules that already apply to the neighboring U-NII-3 band would unleash 200 MHz of contiguous and uniquely useful spectrum that accommodates the only unfettered 160 megahertz channel sufficient to support truly gigabit Wi-Fi networks.

Unlike the Cisco approach, under Qualcomm's re-channelization proposal Wi-Fi 802.11ac devices could prioritize DSRC transmissions on the channels they are authorized to share (presumably the bottom 40 megahertz of the ITS band), but without the need to retool the existing 802.11ac standard or limit unlicensed use to a new class of indoor-only devices capable of a detect-and-vacate-the-band restriction. More importantly for consumer broadband access and spectrum efficiency, re-channelization could accommodate the FCC's proposal to permit indoor and outdoor deployments under technical rules compatible with the adjacent U-NII-3 unlicensed band – thereby realizing the broader public interest benefits of 80 and 160 MHz channel widths ("gigabit Wi-Fi") that would be effectively foreclosed under the detect-and-avoid approach.

V. CONCLUSION

Commenters appreciate the opportunity to share our views with NHTSA on this important proceeding. We urge NHTSA to address the serious concerns discussed above if it seeks to move forward with this proposal.

Respectfully Submitted,

/s/ Michael Calabrese
New America's Open Technology Institute

/s/ John Gasparini
Public Knowledge

/s/ Jack Gillis
Consumer Federation of America

April 12, 2017