September 8, 2016

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: ***In the Matter of Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850 – 5.925 GHz Band (5.9 GHz Band),*** **RM-11771**

Dear Ms. Dortch:

The Intelligent Transportation Society of America ("ITS America")[1] respectfully submits reply comments to the Federal Communications Commission ("Commission") in response to the petition for rulemaking and request for emergency stay (the "Petition") filed by Public Knowledge and Open Technology Institute at New America (collectively, the "Petitioners") in the above-captioned proceeding.[2]

The Petition is fatally flawed for many reasons, including its failure to: 1) acknowledge that Dedicated Short Range Communications ("DSRC") systems already contain robust privacy and cybersecurity protections; 2) comprehend that DSRC systems do not collect personally identifiable information (PII) and therefore do not fall under the Commission's Customer Proprietary Network Information ("CPNI") or proposed Customer Proprietary Information ("CPI") rules even if the Commission were to have authority to regulate DSRC privacy and cybersecurity; and 3) recognize that other government agencies already regulate DSRC privacy and cybersecurity and that the Commission lacks the requisite authority to regulate DSRC in this area. Additionally, the Petitioner's stay request should be denied. Therefore, ITS America reiterates its opposition to the Petition and notes that an overwhelming majority of commenters share ITS America's position that both of the Petitioners' requests are without merit, and the Petition should be denied.

Privacy and cybersecurity have been an integral part of the development of DSRC systems. "With input from numerous stakeholders, the Vehicle-to-Vehicle ("V2V") system as designed contains multiple technical, physical, and organizational controls to guard 'against

[1] ITS America is an association of public and private organizations that are focused on advanced vehicle technology, smart cities, and new models for mobility. Our members include auto, telecomm, traditional IT and emerging tech, and consumer apps and industrial electronics. We also include public agencies and nonprofits, such as road, transit and other transportation infrastructure operators and the research community focused on bringing new technology from the lab to our roads, cars, buses and trucks.

[2] Public Knowledge and Open Technology Institute at New America, Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band) (filed June 28, 2016) ("Petition"); *see also Consumer & Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed,* Public Notice, RM-11771 (rel. July 25, 2016).

internal and external threats or attacks'"[3] The technology used to implement DSRC communications purposely exchanges safety information only in a limited geographical region and in a manner that does not "identify the car, driver or owner."[4] Therefore, even assuming the Commission has the authority to regulate privacy and cybersecurity issues related to DSRC, the information exchanged would not fall under the Commission's CPNI rules or its proposed CPI rules.

In comments to their own petition, Public Knowledge, in particular, make numerous assertions without any basis in fact.[5] They suggest that "[b] ecause the FCC's existing service rules include a backwards-compatibility requirement, it is conceivable that vulnerabilities introduced in first-generation DSRC units will not be patched due to the absence of update mechanisms." There is nothing in the FCC rules or anywhere else to suggest that FCC rules "prohibit" a DSRC device manufacturer from upgrading their equipment or services. Public Knowledge also provides no facts to suggest such updates would necessarily break "backwards compatibility" to any specific level described in detail in the FCC's rules.

Public Knowledge suggests that there has not been adequate "cybersecurity planning" despite the fact that development of the security architecture services and standards in the Institute of Electrical and Electronic Engineers ("IEEE") 1609 working group, has been ongoing since the FCC established DSRC technical and service rules in 2004. The suggestion by Public Knowledge that a "large scale auto hacking" will be the result from the use of DSRC is not supported by any evidence-based risk assessment, only assertions without any basis in fact. None of the other of the respondents to the FCC proceeding support this assertion on a substantive basis, nor is such an assertion found within many of the numerous National Highway Traffic Safety ("NHTSA") proceedings on auto safety and security addressing DSRC, V2V or other emerging technologies over the last several years.

Furthermore, Public Knowledge also never provided specific nor effective changes to the FCC rules that would avert the purported ominous hazards they claim, without also curbing all of the traffic safety benefits that DSRC was designed to provide. In a bizarre prescription, Public Knowledge, in addition to asking the FCC to issue a sweeping blanket ban all DSRC operations in their petition, in their comments to their own petition also asks the FCC to create a new service designation of DSRC operation that does not exist in the current DSRC technical and service rules, then asks the FCC pre-emptively ban that type, for some poorly defied additional measure unrelated to DSRC safety, security, or privacy. In their comments to their own petition, Public Knowledge recommended changes to the service rules -- "90.371(d) No one may offer commercial services via DSRC, or allow commercial services or applications to be offered using DSRC licensed spectrum." Public Knowledge justifies creation of this novel category of DSRC service, and its immediate and pre-emptive ban, based upon some abstract principle of equity related to spectrum use, with no reference to the current FCC technical and service rules defining services, nor to any substantiated potential harms related to safety, security, or privacy that the designation would purportedly and specifically address.

---

[3] Comments of General Motors at 2 (filed Aug. 24, 2016).

[4] *Id.*

[5] Comments of Public Knowledge, Open Technology Institute At New America, Institute For Local Self-Reliance, Center For Rural Strategies, Access Humboldt, Privacy Rights Clearinghouse, And Consumer Watchdog

Their proposal to create a DSRC "commercial services" category betrays Public Knowledge's ignorance of the purpose of FCC DSRC technical service rules related to Intelligent Transportation Services. The FCC technical and service rules creates a service framework that mediates between different services on the practical basis of assuring road user safety, not some standard of equity between different categories of spectrum use. To illustrate the purpose of the framework, multiple DSRC users communicating with one another may at times overload one or more of the DSRC service channels. DSRC licensees may compete for channel use and can cause channel overload, that may cause potential service failures at critical moments. FCC technical and service rules for DSRC address this problem by giving safety or public safety communications priority of channel use among all DSRC users, so that such failures do not result traffic fatalities, injuries, create unexpected disruptions to traffic flow or otherwise subvert measures by road operators or public safety entities to actively manage traffic. Standards developed by auto industry and traffic management systems manufacturers in IEEE specified network and service management standards to implement this FCC priority framework. Public Knowledge provides no clear definition a "commercial service" nor cites any concrete examples applications that would fit into this new category, and therefore cannot even illustrate their how this suggested remedy could specifically address the security or privacy harms they fail to demonstrate earlier in their comments.

No other commenters suggested that services framework created by the FCC posed a particular threat to security or privacy. Public Knowledge provides no applicable risk assessment that the current FCC DSRC technical and service rules service priority framework, as implemented in standards or in current deployments, somehow sets the stage for critical vulnerabilities for DSRC. Their unsubstantiated blanket claims that DSRC is somehow insecure, without reference to current security and privacy standards, architecture and even to the FCC rules, are not constructive comments on this matter and cannot be the basis of a change those same rules governing the use of DSRC spectrum.

The FCC's allocation of DSRC, along with the establishment of its technical and service rules, provided the foundation that enabled industry and academia, in coordination with the NHTSA, other parts of the US Department of Transportation ("USDOT") and the Federal Trade Commission ("FTC") to build a sound architecture around security and privacy and to provide assurance that DSRC would be used for the purpose intended – improving transportation safety. The Petition's failure to acknowledge the work of these agencies is also equally astonishing and unconstructive. According to DOT Secretary Anthony Foxx, DOT "wants to speed the Nation toward an era when vehicle safety is not just about surviving crashes; it is about avoiding them."[6] In working to achieve this goal, NHTSA realizes that "cybersecurity must be an integral part of vehicle engineering, manufacturing, and enforcement."[7] By utilizing its enforcement authority under Section 5 of the FTC Act to crack down on "unfair or deceptive acts or practices," the FTC has zealously leaped to protect consumers when companies fail to meet privacy and security expectations. With automobile manufacturers and equipment suppliers subject to oversight by

---

[6] "Transportation Sec. Foxx announces steps to accelerate road safety innovation," May 13, 2015, *available at:* http://www.nhtsa.gov/About+NHTSA/Press+Releases/2015/nhtsa-will-accelerate-v2v-efforts.

[7] NHTSA and Vehicle Cybersecurity (last visited Sept. 8, 2016), *available at:* http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity.

the FTC, consumers have a effective "cop on the block" should any privacy issues arise in the future.

The Commission should ignore the Petition's nonsense rhetoric of a "car zombie apocalypse"[8] and focus on the true public safety benefits of DSRC and V2V technologies. NHTSA estimates that DSRC will help mitigate 80 percent of non-impaired crashes, potentially providing a saving to our economy of $871 billion each year.[9] With over 20,000 highway workers "killed and injured in the line of serving the public," DSRC will serve as an essential tool to help to reduce these tragic accidents.[10]

For the Intelligent Transportation Society of America

Steven H. Bayless
Vice President, Technology and Markets

Jason Goldman
Vice President, External Affairs and Stakeholder Engagement

[8] Petition at 5.

[9] http://www.safetyandhealthmagazine.com/articles/print/10545-nhtsa-motor-vehicle-crashes-have-871-billion-impact Washington – Motor vehicle crashes cost Americans $871 billion in economic loss and societal harm in 2010, according to a new study from the National Highway Traffic Safety Administration. That price tag includes $594 billion tied to loss of life and pain and decreased quality of life due to injuries. It also accounts for $277 billion in economic costs such as productivity loss, property damage, and medical and legal costs – nearly $900 per U.S. resident.

[10] Comments of the State of California Department of Transportation at 8.