Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition for Rulemaking and Request for	)	
Emergency Stay of Operation of Dedicated	)	
Short-Range Communication Service in the	)	
5.850-5.925 GHz Band (5.9 GHz Band)	)	RM-11771

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

Harold Feld
John Gasparini
Public Knowledge
1818 N St. NW, Suite 410
Washington, DC 20036

Christopher Mitchell
Director, Community Broadband Networks
Institute for Local Self-Reliance
1710 Connecticut Avenue, NW, 4th Floor
Washington, DC 20009

Michael Calabrese
Director, Wireless Future Project
Open Technology Institute at New America
740 Fifteenth Street NW – 9th Floor
Washington, DC 20005

Dee Davis
President
Center for Rural Strategies
46 East Main Street
Whitesburg, KY 41858

Sean McLaughlin
Executive Director
Access Humboldt
P.O. Box 157
Eureka, CA 95502

Meghan Land
Staff Attorney
Privacy Rights Clearinghouse
3033 5th Ave Suite 223
San Diego, CA 92103

John Simpson
Privacy Project Director
Consumer Watchdog
2701 Ocean Park Blvd., Suite 112
Santa Monica, CA 90405

August 24, 2016

TABLE OF CONTENTS

I. INTRODUCTION

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 (collectively, "Commenters") submit these comments in response to the Commission's Public Notice requesting comment on our Petition for Rulemaking and Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band) ("Petition").[1] Commenters appreciate the Commission's prompt attention to the important issues raised by the petition and discussed further in these comments, particularly in light of the auto industry's persistent effort to deploy unsecure devices into the marketplace before these issues can be addressed. We reiterate our request that the Commission act with all appropriate speed to address these concerns.

Commenters appreciate this opportunity to expand upon several aspects of the Petition. In particular, these Comments will offer expanded discussion of the cybersecurity threat posed by the deployment of commercial services in the DSRC band, the impact on consumer privacy presented by mandatory deployment of the DSRC service without any privacy protections in place, and further analysis of the potential harms arising from commercialization of the DSRC service in the first place.

[1] *See generally* Public Knowledge and Open Technology Institute at New America, *Petition for Rulemaking and Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band)*, RM-11771 (Jun. 28, 2016) ("Petition").

II. DEPLOYMENT OF UNSECURE DSRC UNITS NEATLY ADDRESSES THE LAST BARRIER FACING THOSE WITH ASPIRATIONS FOR LARGE-SCALE AUTO HACKING

Experts agree that, given the high vulnerability of cars,[2] there's only one reason car hacking hasn't become widespread. As the Washington Post reported in July 2015:

> "'They haven't been able to weaponize it. They haven't been able to package it yet so that it's easily exploitable,' said John Ellis, a former global technologist for Ford. 'You can do it on a one-car basis. You can't yet do it on a 100,000-car basis.'"[3]

Viruses on computers and other devices spread primarily because those devices talk to one another on networks. Cars are insecure already, regardless of the cybersecurity protections integrated into NHTSA's small portion of the DSRC band. Even if the communications between DSRC units are encrypted, the devices those DSRC units are connecting are not secure. The forthcoming mandate for DSRC device deployment neatly solves for hackers the last major obstacle to large-scale auto hacking, by providing a mandatory, trusted connection between all cars.

It is a fundamental principle of cybersecurity that the more devices and networks you connect to a platform, the more vulnerabilities and attack vectors you introduce into even the most secure of systems. While DSRC creates an additional attack vector, the problem is exponentially exacerbated by commercialization of the service. Connection to the public internet to facilitate services such as mobile payments, advertising, and infotainment content delivery,

---

[2] Federal Bureau of Investigation Public Service Announcement, *Motor Vehicles Increasingly Vulnerable to Remote Exploits* (Mar. 17, 2016) ("FBI Alert"), *available at* https://www.ic3.gov/media/2016/160317.aspx.

[3] Craig Timberg, *Hacks on the Highway*, The Washington Post (July 22, 2015), http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/. *See also* FBI Alert, *supra* note 1 (warning drivers to "exercise discretion in connecting third party devices to your car.")

create a plethora of attack vectors and additional vulnerabilities, any of which could be exploited to breach the car, and then utilize the DSRC unit to spread to every DSRC-equipped car it comes in contact with.

It is important to be clear at this stage, too, that DSRC's most ardent supporters and the primary licensees, the auto industry itself, are woefully ill-equipped to address cybersecurity issues. The auto industry is not well-equipped to address these issues, as discussed at length in the Petition,[4] and cannot be relied upon to address cybersecurity issues of their own volition. It is unclear that the auto industry understands the nature and extent of the cybersecurity challenges they face. When asked about cybersecurity protections for DSRC units by a Politico reporter, Steven Bayless, vice president for technology markets at ITS America, offered the following response: "'What's being exchanged between vehicles is just data . . . There's no possibility of a virus being spread between cars.'"[5] All information exchanged by digital systems is in the form of, as Mr. Bayless puts it, "just data."[6] All information stored and exchanged by any computer connected to any network is encoded as "just data" - viruses included. Cybercriminals and terrorists absolutely can and will use this attack vector for nefarious purposes, exchanging "just data" to potentially devastating effect.

Simply put, DSRC deployment already creates a massive cybersecurity issue by connecting vulnerable cars to one another. Commercialization of the service, particularly without cybersecurity protections, provides attackers with not only a means of spreading malware rapidly

---

[4] *See* Petition at 5-9.
[5] Margaret Harding McGill, *Latest privacy debate: Crash-avoidance Technology*, Politico (Jun. 28, 2016), https://www.politicopro.com/transportation/story/2016/06/latest-privacy-debate-crash-avoidance-technology-117891.
[6] *See generally* Wikipedia, *Data (Computing)* (last accessed Aug. 24, 2016), https://en.wikipedia.org/wiki/Data_(computing).

along the nation's roadways, but a plethora of potentially vulnerable commercial attack vectors to gain access to the already-insecure car, in addition to the numerous vectors already present in the modern car.

III. CYBERSECURITY RISK IS HEIGHTENED DUE TO BACKWARDS COMPATIBILITY MANDATE AND THE LACK OF CLARITY FROM AUTOMAKERS REGARDING ONGOING SECURITY PRACTICES.

The 5.9 GHz band was allocated to the auto industry in 1999, and the FCC set service rules a few years later. Since then, progress has been slow until recently. When the FCC began to examine the viability of sharing the 5.9 GHz band with other users, however, a decade of slow progress evaporated and the auto industry was suddenly ready to put units in production cars within a few years. Those first production units will hit showroom floors as early as next month, in advance of both NHTSA's mandate and the FCC's conclusion of its sharing proceeding.

There are a number of issues with a rushed deployment like this. First and foremost, the current DSRC service rules contain a backwards compatibility mandate. Because the technology will not achieve results until a critical mass of vehicles are DSRC-equipped, and the process of getting that many cars on the road will take upwards of two decades, it is necessary to ensure that DSRC units shipped out today are able to communicate with units developed and deployed decades in the future.

As a result of this requirement, it is possible that security holes present in units shipped today will of necessity be built into future devices, or will not be able to be patched out of later generations of DSRC tech, because they interfere with backwards compatibility. As a result, this vulnerability combined with the requirement for backwards compatibility and a lack of adequate update and maintenance mechanisms, will provide a permanent attack vector for the full fleet of DSRC-equipped vehicles. Vulnerabilities of this sort can and should be addressed if the

Commission requires DSRC licensees to develop and share with the agency, cybersecurity plans which include not only breach response protocols, but also procedures and policies for updating and securing all deployed DSRC units of any generation on an ongoing basis.

IV. THE AUTO INDUSTRY'S URGENCY TO DEPLOY MUST NOT RELIEVE THEM OF RESPONSIBILITY UNDER ANY RULES EVENTUALLY IMPLEMENTED.

As discussed above, the auto industry is rushing to deploy DSRC units in the hopes that, once the tech is on the road, it will be harder for consumers and policymakers to cry foul on their Trojan horse plan to monetize public safety spectrum. Whether or not they are successful, and regardless of whether or not the Commission sees fit to grant our requested Stay of Operation for the DSRC service, it must be made clear to the auto industry, as licensees of the 5.9 GHz band, that their rush to deploy will not absolve them of responsibility for any cybersecurity vulnerabilities which may exist in first-generation DSRC units.

Because 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. Furthermore, those vulnerabilities would be perpetuated in future devices due to the need to ensure backwards compatibility with unpatched units per the existing service rules. Without adequate cybersecurity planning, including provisions for updating all active units deployed at any point in time by a DSRC licensees, threats that could be patched in later versions may perpetuate, and innovations in cybersecurity may not be implemented in protecting this vulnerable service.

V. COMMERCIALIZATION OF PUBLIC SAFETY SPECTRUM CREATES ECONOMIC INCENTIVES WHICH UNDERMINE THE PUBLIC SAFETY MISSION.

As a general rule, we do not allow those granted public safety licenses to exploit these licenses commercially.[7] First responders don't lease their spectrum to commercial users, and emergency communications bands are not usable by commercial operators. The 5.9 GHz band, as utilized by the DSRC service, should be no different. Where public safety is the purpose of a spectrum allocation, sound policy dictates that commercial interests be excluded, to avoid creating incentives for a licensee to favor revenue-generating commercial services over critical public safety communications.

The DSRC service in the 5.9 GHz band should not break this trend. If the insistence of the auto industry on deploying DSRC is motivated exclusively by a desire to improve safety and save lives, as the industry claims, then the industry should have no qualms about accepting a non-commercial condition on the use of this band to ensure that it is used exclusively for important public safety functions. Alternatively, in light of the strong public policy reasons for prohibiting commercial operation, the auto industry must explain why the lifesaving aspects of DSRC are dependent on the auto industry receiving an exclusive commercial spectrum windfall,

[7] The significant precautions around secondary leasing to fund FirstNet demonstrates the lengths Congress and the FCC will go to in order to prevent commercial exploitation of public safety spectrum, and to protect public safety spectrum management from potential conflicts of interest that would undermine the public safety mission. Rather than license the spectrum to a private, non-profit public safety entity, Congress elected to create a new, government entity as the sole licensee of the spectrum. This government entity – FirstNet -- has the primary mission of serving public safety licensees. See Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. 112-96, §§ 6201-08. While the statute requires FirstNet to fund itself through secondary leasing of excess capacity to commercial (or other) entities, the statute expressly prohibits FirstNet from offering any commercial services to consumers. Id. § 6212. Even with regard to this highly limited wholesale leasing, Congress imposed additional restrictions and accountability mechanisms. Id. §§6209-6211. This extremely indirect, tightly controlled secondary leasing by a federal licensee is a far cry from the unrestricted commercial use currently authorized for DSRC.

in contravention of longstanding principles of sound spectrum policy. Given that commercialization of the spectrum affirmatively creates significant cyber vulnerabilities and privacy concerns, supporters of commercial use must meet a particularly high burden to justify commercialization of DSRC.

VI. PRIVACY POLICIES FOR COMMERCIAL SERVICES WHICH ARE "LIKE FACEBOOK" ARE INSUFFICIENT TO PROTECT CONSUMERS.

As detailed in the Petition, deployment of commercial services alongside public safety DSRC functions creates substantial consumer privacy problems, particularly in the context of a mandate. When asked about commercial privacy protections, Mr. Bayless of ITS America demonstrated, yet again, how disinterested the auto industry is in consumer protections: "'On the commercial side, it's whatever the privacy policy of the application provider is,' he explained. 'That's the way it is for most applications, like Facebook.'"[8]

There are, needless to say, a few key differences in terms of consumer choice and privacy protections, between commercial DSRC services, and Facebook. For starters, Facebook isn't mandatory. The auto industry is pushing for DSRC to be mandatory in all cars sold in the US. Facebook's location-tracking features also aren't mandatory. There's no indication of any form of opt-in mechanism for these privacy-threatening technologies; the choice consumers may well be given is simply "agree, or don't buy a car." Robust privacy protections which require consumer consent and ensure adequate protection for consumer data, covering both how it may be used and what must be done in the case of a breach, are necessary to protect any consumer service. If, as the auto industry insists, commercialization of the band is necessary and desirable,

[8] *See* McGill, *supra* note 5.

these services should not be unique among wireless technologies in having no privacy protections attached.

VII. CONCLUSION

For the foregoing reasons, in addition to those outlined in the Petition, Commenters strongly urge the Commission to grant the Petition's requests in full. In this manner, the Commission can exercise sound judgment in spectrum and public safety policy, and protect the safety and security of drivers, passengers, and all consumers.

Respectfully Submitted,

/s/ Christopher Mitchell
Director, Community Broadband Networks
Institute for Local Self-Reliance
1710 Connecticut Avenue, NW, 4th Floor
Washington, DC 20009

/s/ John Gasparini
Policy Fellow
Public Knowledge
1818 N St. NW, Suite 410
Washington, D.C. 20036

/s/ Michael Calabrese
Director, Wireless Future Project
Open Technology Institute at New America
740 Fifteenth Street NW – 9th Floor
Washington, DC 20005

/s/ Dee Davis
President
Center for Rural Strategies
46 East Main Street
Whitesburg, KY 41858

/s/ Sean McLaughlin
Executive Director
Access Humboldt
P.O. Box 157
Eureka, CA 95502

/s/ Meghan Land
Staff Attorney
Privacy Rights Clearinghouse
3033 5th Ave Suite 223
San Diego, CA 92103

/s/ John Simpson
Privacy Project Director
Consumer Watchdog
2701 Ocean Park Blvd., Suite 112
Santa Monica, CA 90405

August 24, 2016

APPENDIX A - PROPOSED RULES

Proposed Non-Commercial Rule

Rule 90.371 (47 C.F.R. § 90.371) is amended as follows.

By inserting after existing Rule 90.371

"90.371(d) No one may offer commercial services via DSRC, or allow commercial services or applications to be offered using DSRC licensed spectrum."

Proposed DSRC Cybersecurity Rules

Rule 90.371 (47 C.F.R. § 90.371) is Amended as follows:

By inserting after existing Rule 90.371

"90.371(e)(1) Each DSRC licensee is required to submit to the Commission a Statement describing its network security plans and related information, which shall be signed by a senior executive within the licensee's organization with personal knowledge of the security plans and practices within the licensee's organization. The Statement must conform, at a minimum, to the following requirements:

A. Contents.

   a. Security Approach. A high-level, general description of the licensee's approach designed to safeguard the planned networks' confidentiality, integrity, and availability with respect to communications from:

      i. A device on the licensee's network;

      ii. One element of the licensee's network to another element on the licensee's network;

      iii. The licensee's network to another network; and

iv. Vehicle to vehicle or infrastructure.

b. Cybersecurity Coordination. A high-level, general description of the licensee's anticipated approach to assessing and mitigating cyber risk induced by the presence of multiple participants in the band. This should include the high level approach taken toward ensuring consumer network confidentiality, integrity, and availability security principles, are to be protected in each of the following use cases: communications between a wireless device and the licensee's network; communications within and between each licensee's network; communications between vehicles that are under end-to-end control of the licensee; and communications between vehicles, and between vehicles and infrastructure, which are not under the end-to-end control of the licensee;

c. Cybersecurity Standards and Best Practices. A high-level description of relevant cybersecurity standards and practices to be employed, whether industry-recognized or related to some other identifiable approach;

d. Participation with Standards Bodies, Industry-Led Organizations. A description of the extent to which the licensee participates with standards bodies or industry-led organizations pursuing the development or maintenance of emerging security standards and/or best practices.

e. Update Procedures. A high-level description of the process by which a licensee will ensure that devices deployed by the licensee and remaining in operation are updated on an ongoing basis to address newly-discovered vulnerabilities while ensuring compatibility with other devices utilizing the band.

f. Other Security Approaches. The high-level identification of any other approaches to security, unique to the services and devices the licensee intends to offer and deploy; and

g. Plans with Information Sharing and Analysis Organizations. Plans to incorporate relevant outputs from Information Sharing and Analysis Organizations (ISAOs) as elements of the licensee's security architecture. Plans should include comment on machine-to-machine threat information sharing, and any use of anticipated standards for ISAO-based information sharing.

B. Timing. Each DSRC licensee shall submit this Statement ot the Commission within three years after grant of the license, but no later than six months prior to deployment.

C. Definitions. The following definitions apply to this section:

a. Confidentiality: the protection of data from unauthorized access and disclosure, both while at rest and in transit.

b. Integrity: the protection against the unauthorized modification or destruction of information or equipment.

c. Availability: the accessibility and usability of a network upon demand."

Proposed DSRC Privacy Rules

In order to address the substantial privacy and data breach issues presented by the commercialization of DSRC spectrum, the Commission should implement privacy rules mirroring its existing CPNI rules, which protect consumers against abuse by providers of other commercial services.[9]

[9] *See generally* 47 C.F.R. § 64.2001 *et seq.*