

October 6, 2016

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

RE: ET Docket No. 13-49 – Revision of Part 15 of the Commission’s Rules
RM-11771 – Petition for Rulemaking in the 5.9 GHz DSRC Band

Dear Ms. Dortch:

On October 4, 2016, John Gasparini, Policy Fellow at Public Knowledge, met with Daudeline Meme, Legal Advisor to Commissioner Clyburn, regarding the above-captioned proceedings.

PK noted that no one who opposed PK’s Petition, other than CTIA, defended the commercial use of DSRC spectrum. Nor did any party explain how use of commercial applications is consistent with the encryption and cybersecurity measures that licensees state are incorporated into the non-commercial life and safety network, or why permitting commercial use of the DSRC spectrum is even consistent with the public interest in light of the changes that have occurred since 2004. The closest any stakeholder came to defending commercial use was ITS America in its reply comments, which simply noted that no one objected on privacy or cybersecurity grounds when the Commission authorized commercial use of the spectrum in 2004.¹

PK observed that the bulk of the objections from parties who are neither vendors of DSRC equipment, DSRC licensees, or potential DSRC licensees (such as the California Department of Transportation) objected primarily to the Commission’s continued use of its privacy and cybersecurity authority, recently reaffirmed in the *Spectrum Frontiers R&O and FNPRM*. Setting aside that the Commission rejected precisely these arguments previously, PK noted that the Commission - if it proceeds to a rulemaking - is permitted to seek comment on whether to prohibit commercial operation on the DSRC spectrum as correcting a previous mistaken grant of a spectrum windfall that *also* improves cybersecurity and privacy in light of the additional vulnerabilities and risk to consumers raised by permitting commercial applications in the band. This alone would enhance consumer privacy and cybersecurity, without use of other Commission authority to which commenters like ITIF object.

¹ Reply Comments of ITS America, Docket No. RM-11771 (filed Sept. 9, 2016).

PK noted, in particular, the contradictory assertions of DSRC licensees, who argued that cybersecurity and privacy standards built into NHTSA's DSRC standards were sufficient to protect the entire band, while simultaneously insisting that the NHTSA DSRC radio would only be capable of sending basic safety messages, not of supporting any other service. This suggests the use of a separate radio, outside NHTSA's jurisdiction and solely governed by FCC service rules, for the provision of commercial services. DSRC licensees completely avoided commenting on commercial services or even admitting that those services would be carried by a radio other than the NHTSA DSRC radio.

In addition, PK noted that the Department of Justice has formed a think tank to consider the national security implications of connected devices, and has explicitly singled out connected cars as a potential threat to national security.² As the head of the DOJ National Security Division, Assistant Attorney General John Carlin, explained, "the internet on wheels . . . clearly is going to present national security risks as this transformation takes place."³

In light of this explicit concern about connected cars raised at the highest level of official counter-terrorism planning, opponents' insistence on ignoring or, at most, casually belittling the concerns raised by four major auto safety organizations and nearly 20 other public interest advocacy groups, is extremely disquieting. In addition, the Department of Justice action emphasizes the need to have every federal agency engaged on cybersecurity issues. It is absurd to imagine that the FCC, the agency explicitly charged with maintaining the reliability and safety of all means of communications by wire and radio⁴, does not have the responsibility, let alone the authority, to ensure that all providers of licensed communications services are cognizant of cybersecurity and have plans to address this evolving threat. Even if one accepts the assurances that DSRC is not merely secure itself, but that using DSRC to connect extremely vulnerable cars to one another, and to the Internet at large (through commercial applications) does not simply create a secure channel of communication for the transmission of malware, this says nothing as to how DSRC licensees plan to address inadvertent vulnerabilities, address future threats, or keep their systems updated to meet current and future cybersecurity challenges.

Assistant Attorney General Carlin pointed to the truck attack in Nice, which killed 81 people, as an example of the kind of damage a hacked car could do. Yet DSRC licensees object even to submitting a plan for how they will address cyberthreats on DSRC, and insist that the warnings of Petitioners and consumer advocates are little more than 'nonsense rhetoric.'

² See Dustin Volz, "Justice Department Group Studying National Security Threats of Internet Linked Devices," Reuters (Sept. 9, 2016).

³ *Id.* (Ellipses in original.)

⁴ See 47 USC § 151.

At the same time, PK stresses that the Commission should not delay the ongoing proceeding regarding spectrum sharing in the 5.9 GHz band. As noted repeatedly by PK, the concerns raised by our DSRC Petition are distinct from the issues raised in the 5.9 GHz Sharing Proceeding. Accordingly, PK recommended the following Commission actions:

1. The Commission should move promptly to issue a full Notice of Proposed Rulemaking. This NPRM should seek comment on whether any use of exclusive portions of the band for commercial services serves the public interest. Comment should also be sought regarding whether general concerns with regard to spectrum windfalls - in addition to privacy and cybersecurity concerns raised by Petitioners - justify eliminating the authorization for commercial services.
2. The Commission should issue an interim rule prohibiting use of DSRC spectrum for commercial applications or services, pending resolution of the NPRM proceeding. It should also warn DSRC licensees that any devices deployed will ultimately need to comply with any future rules adopted by the Commission.
3. The Commission should propose rules consistent with those proposed by Petitioners in comments filed August 24, 2016.
4. The Commission should use the information gathered in ET Docket No. 13-49 to inform the rulemaking, but should not delay any action in Docket No. 13-49 pending resolution of the rulemaking initiated as a result of this petition.

In accordance with section 1.1206(b) of the Commission's rules, an electronic copy of this letter is being filed in the above-referenced dockets. Please contact me with any questions regarding this filing.

Sincerely,

/s/ John Gasparini
Policy Fellow
Public Knowledge

Cc: Daudeline Meme