Before the
Federal Communications Commission
Washington, D.C. 20554

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

OPPOSITION OF GENERAL MOTORS COMPANY

Harry Lightsey
Executive Director, Emerging Technologies, Public Policy
GENERAL MOTORS COMPANY
25 Massachusetts Avenue N.W.
Suite 400
Washington, D.C. 20001

August 24, 2016
# Table of Contents

I. INTRODUCTION AND SUMMARY ............................................................................................ 1

II. THE COMMISSION LACKS ANY LEGAL AUTHORITY TO IMPOSE PRIVACY OR CYBERSECURITY REQUIREMENTS ON DSRC OPERATORS. ................................. 5

III. THE PETITION IS AN UNPRECEDENTED COLLATERAL ATTACK ON OPERATORS’ AUTHORIZED USE OF THEIR SPECTRUM ..................................................... 8

IV. PETITIONERS’ REQUEST FOR AN “EMERGENCY” STAY IS PROCEDURALLY DEFECTIVE................................................................................................................................. 10

V. THE LEGALLY DEFECTIVE PETITION IS BASED UPON A FALSE PREMISE REGARDING THE NEED FOR PRESCRIPTIVE PRIVACY AND CYBERSECURITY RULES FOR DSRC OPERATORS. ................................................................. 12

VI. CONCLUSION............................................................................................................................. 14
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

OPPOSITION OF GENERAL MOTORS COMPANY

General Motors Company ("GM") respectfully submits this Opposition to the Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service ("DSRC") in the 5.850-5.925 GHz Band ("Petition") filed by Public Knowledge and Open Technology Institute at New America ("Petitioners").

I. INTRODUCTION AND SUMMARY.

DSRC technology provides vehicle-to-vehicle ("V2V"), vehicle-to-infrastructure ("V2I") and other ("V2X") communications, helping to protect the safety of the traveling public. It can save lives by warning drivers of an impending dangerous condition or, eventually, to take corrective or evasive actions. DSRC V2V is the culmination of years of work by industry, academia, Congress, the National Highway Traffic Safety Administration ("NHTSA"), and the Commission. This bold vision for the use of technology to help humankind is coming to fruition, with GM deploying DSRC V2V communications in its Model Year 2017 Cadillac CTS.

1 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, RM-11771 (filed Jun. 28, 2016) ("Petition").
Additionally, many states are deploying now, or will deploy in the near future, transportation infrastructure premised on the availability of DSRC-based communications.  

DSRC V2V technology was designed specifically with data privacy and cybersecurity at the forefront. With input from numerous stakeholders, the V2V system as designed contains multiple technical, physical, and organizational controls to guard “against internal and external threats or attacks.” It uses public key infrastructure (“PKI”) security without requiring user personal information, the safety messages exchanged between vehicles do not identify the car, driver or owner, and the V2V devices transmit safety messages only in a limited geographical range. In addition to the security and privacy designed into the V2V system, GM devotes

---

2 See, e.g., Comments of Washington State Department of Transportation, ET Docket No. 13-49, at 2 (filed July 7, 2016); Comments of Michigan Department of Transportation, ET Docket No. 13-49, at 1 (filed July 6, 2016) (noting the operation of 130 DSRC roadside units in Michigan as part of $30 million investment in DSRC technology in the state “with a plan for an additional $40 million investment over the next five years”); Comments of Maricopa County Department of Transportation, ET Docket No. 13-49, at 1 (filed July 6, 2016) (noting initiative that has “deployed connected vehicle applications that integrate vehicles with Systematically Managed ARTerial (SMART) roadway systems” in Maricopa County); Comments of New Mexico Department of Transportation, ET Docket No. 13-49, at 3 (filed July 5, 2016).


4 Id. at 61933 (noting that the V2V system: (1) “will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so”; (2) “will not permit tracking through space or time of vehicles linked to specific owners or drivers or persons”; and (3) “will not collect financial information, personal communications, or other information linked to individuals”); see also Henn, Thorsten et al., Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System, available on Docket No. NHTSA-2015-0060, July 31, 2014; Security Credential Management System Proof–of–Concept Implementation: EE Requirements and Specifications Supporting SCMS Software Release 1.1, available at http://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf; SAE J2945/1-March 2016 On-Board System Requirements for V2V Safety Communications; and IEEE 1609.2-2016 - Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages.
substantial resources to data privacy and cybersecurity in support of the important goal of protecting its customers.

This security-by-design employed in the development of DSRC V2V technology is precisely the approach endorsed by the Commission in its recent Spectrum Frontiers Order. DSRC V2V technology was developed and will be deployed with data privacy and cybersecurity firmly in mind.

Yet, on the eve of the public safety benefits of DSRC being realized, Petitioners have filed a legally baseless, procedurally flawed, and factually unsubstantiated request for rulemaking and an “emergency stay” – a request that bears the hallmarks of political desperation. Petitioners’ failure to even acknowledge industry-government-academia efforts to develop DSRC V2V with its pioneering security and privacy features is inexcusable. While couched in terms of protecting “user privacy” and preventing “cybersecurity attacks,” the Petition is nothing more than an attempt to advance Petitioners’ desire for unlicensed use of the DSRC band by seeking to prevent automakers from utilizing their DSRC licenses. The Commission should see through this obvious ploy.

Equally inexcusable is Petitioners’ failure to offer any legal authority for their proposed rules. Petitioners point to no authority that would empower the Commission to impose privacy

---


6 See, e.g., NHTSA RFI, 79 Fed. Reg. at 61929 (noting efforts to consider “which security technologies would most effectively provide trusted message exchange and secure communications for safety-critical applications …”).

7 Petition at ii.
and cybersecurity obligations on non-common carriers such as DSRC operators. Because the requested rules are unlawful, the Commission should dismiss the Petition for this reason alone.

Petitioners’ request that the Commission “immediately prohibit” any use of DSRC pending further rulemaking proceedings is unprecedented.\(^8\) In fact, the Petition is squarely at odds with the Commission’s *Spectrum Frontiers Order*, which endorsed addressing privacy and cybersecurity concerns at an “earlier stage” employing a “security-by-design” approach. By contrast, Petitioners have waited until the eleventh hour to raise their privacy and cybersecurity concerns, given that DSRC spectrum was allocated approximately 17 years ago and licensed approximately 12 years ago.\(^9\) Furthermore, Petitioners advocate cybersecurity by regulatory fiat, which is contrary to the minimal impact and flexible approach favored by the Commission.

There is simply no justification or precedent to stop the deployment of potentially life-saving DSRC technology dead in its tracks while the Commission considers whether to adopt new rules and DSRC operators that have spent years working under the existing rules seek to come into compliance with any new requirements.

Finally, Petitioners run roughshod over the Commission’s rules with their emergency stay request. Petitioners make no attempt to address, let alone establish, the standards for the extraordinary relief requested. Furthermore, given that the DSRC rules have been in effect since 2004, Petitioners seek a stay to change, not preserve, the status quo, which is improper.

Petitioners also have failed to comply with the Commission’s procedural rules governing stay

---

\(^8\) Petition at 1.

\(^9\) *See 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 Systems*, Report and Order, 14 FCC Rcd 18221 (1999) (“DSRC Report and Order”).
requests. Accordingly, Petitioners’ request for a “stay of operation” of DSRC spectrum should be summarily denied.

II. THE COMMISSION LACKS ANY LEGAL AUTHORITY TO IMPOSE PRIVACY OR CYBERSECURITY REQUIREMENTS ON DSRC OPERATORS.

No provision of the Communications Act authorizes the Commission to impose privacy and cybersecurity requirements on DSRC operators. DSRC operators have been classified as “private mobile radio service” providers, which the Commission is precluded from regulating as “common carriers.” The Petition cites no statutory authority for the Commission to impose privacy and cybersecurity requirements on non-common carriers. That is because no such authority exists.

The Commission “has no constitutional or common law existence or authority, but only those authorities conferred upon it by Congress.” “If there is no statute conferring authority, a federal agency has none.” Any claimed authority “must come from Congress, not from … the Commission’s own conception of how [a] statute should be rewritten.”

Here, even as Petitioners must acknowledge, Congress has not vested the Commission with authority over the privacy and cybersecurity practices of non-common carriers. As the Petition recognizes, Section 222 of the Communications Act, which obligates telecommunications carriers to protect the confidentiality of proprietary information, extends

---

10 DSRC Report and Order at ¶ 82 (adopting a presumption that DSRC is a private mobile radio service, “except for applications that specify interconnection with the public switched network”).


12 Am. Library Ass’n v. FCC, 406 F.3d 689, 698 (D.C. Cir. 2005) (citation omitted).


only to common carriers.\textsuperscript{15} Section 222 does not apply to private mobile radio service providers generally or DSRC operators specifically.

Because Section 222 has no legal relevancy to DSRC, Petitioners’ reliance upon the Commission’s \textit{2007 Pretexting Order} is as baffling as it is misplaced.\textsuperscript{16} The Commission adopted that order in implementing the requirements of Section 222, and the obligations under the \textit{2007 Pretexting Order} apply only to telecommunications carriers.\textsuperscript{17} Nothing in the \textit{2007 Pretexting Order} would purport to authorize the imposition of privacy and cybersecurity requirements on private mobile radio service providers.

Petitioners suggest off-handedly that the Commission could adopt proposed privacy and cybersecurity rules pursuant to its general authority to act in the public interest under Sections 303(b) and 303(r).\textsuperscript{18} Petitioners are wrong.

Section 303(b) authorizes the Commission to “prescribe the nature of the service to be rendered by each class of licensed stations and each station within any class”\textsuperscript{19} – authority the

\begin{itemize}
\item \textsuperscript{15} 47 U.S.C. § 222; Petition at viii.
\item \textsuperscript{17} Although the Commission extended the application of its CPNI rules to providers of interconnected VoIP, it did so pursuant to the Commission’s Title I ancillary jurisdiction because it had not yet determined the regulatory classification of interconnected VoIP. \textit{See 2007 Pretexting Order} at ¶¶ 55-59 (finding imposing CPNI obligations on interconnected VoIP providers to be “reasonably ancillary to the effective performance of the Commission's various responsibilities” in order to protect the reasonable expectations of customers and “the privacy of wireline and wireless customers that place calls to or receive calls from interconnected VoIP customers”).
\item \textsuperscript{18} Petition at viii.
\item \textsuperscript{19} 47 U.S.C. § 303(b).
\end{itemize}
D.C. Circuit has determined is not “unlimited.” By its plain terms, Section 303(b) is limited to prescribing “the nature of the service” a licensee provides. Thus, while Section 303(b) may authorize the Commission to regulate the actual service being provided over the airwaves, it cannot serve as authority to impose requirements ancillary to the service, such as measures that a DSRC operator employs to protect customer privacy and guard against cybersecurity threats.

Although Section 303(r) authorizes the Commission to “make such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this Act,” the statute does not constitute an independent grant of substantive Commission authority. As the D.C. Circuit has made clear, “[t]he FCC cannot act in the ‘public interest’ if the agency does not otherwise have the authority to promulgate the regulations at issue.” No such authority exists here.

Because the Commission lacks the statutory authority to regulate the privacy and cybersecurity practices of non-common carriers, it cannot adopt the proposed rules, even if such rules were otherwise necessary or appropriate, which is not the case. Accordingly, the Commission must dismiss the Petition.

---


21  *See Cellco P’ship*, 700 F.3d at 543 (upholding the Commission’s data roaming rule because it “merely defines the form mobile-internet service must take for those who seek a license to offer it”).


24  The Petition also cites the Commission’s decision to: (1) seek comments on privacy and cybersecurity requirements in connection with geolocation for 911; (2) review Telcordia’s ability to protect privacy and provide adequate cybersecurity protections in its bid to administer the
III. THE PETITION IS AN UNPRECEDENTED COLLATERAL ATTACK ON OPERATORS’ AUTHORIZED USE OF THEIR SPECTRUM.

GM and other DSRC operators are using the spectrum in the manner expressly authorized by the Commission and as a result are about to make the safety benefits of V2V technology available to the public. Even if the Commission had the authority to impose privacy and cybersecurity requirements on DSRC operators, which is not the case, there is simply no lawful basis for the Commission to prohibit operations consistent with existing service rules as requested in the Petition. On the contrary, Commission precedent supports a sound rejection of Petitioners’ attempt to prevent GM’s continued use of DSRC.

Historically, modifications to the Commission’s service rules are implemented in a constructive manner by providing flexibility to and minimizing the impact on operators. Indeed, when changing service rules, the Commission has not only permitted continued operations consistent with then-existing rules, but in some cases granted licensees an additional grace period for coming into compliance with the new requirements. Even in connection with unlicensed operations, the Commission historically offers operators flexibility in meeting new requirements

(footnote cont’d.)

Local Number Portability Database; and (3) reaffirm the importance of cybersecurity in the Technology Transition framework. Petition at 10-11. Of course, in none of these examples has the Commission actually adopted privacy and cybersecurity requirements, and none of these proceedings involve private mobile radio service providers.

rather than directing that operations cease until such requirements have been met.\footnote{Revision of Part 15 of the Commission’s Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report and Order, 30 FCC Rcd 4739 (2014) (adopting new U-NII rules and testing procedures to ensure U-NII devices do not cause harmful interference to FAA weather radar operations or other authorized users); Revision of Part 15 of the Commission’s Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, Order, 30 FCC Rcd 13986 (2015) (extending the December 2, 2015, deadline for U-NII devices to comply with revised Section 15.407 by three months).} In short, there simply is no precedent—and Petitioners cite none—that would support Petitioners’ request to prohibit DSRC operations while the Commission considers whether to impose privacy and cybersecurity requirements on DSRC operators.

Petitioners requested relief also is completely antithetical to the Commission’s desire that cybersecurity requirements have a minimal impact on the deployment of services. The Commission recently expressed that desire in addressing cybersecurity requirements in its \textit{Spectrum Frontiers Order}. There, the Commission took “narrow steps” to “promote an environment that encourages early and ongoing consideration of security issues,”\footnote{\textit{Spectrum Frontiers Order} at ¶ 256.} recognizing that “communications providers are generally in the best position to evaluate and address risks to their network operations.”\footnote{\textit{Id.} at ¶ 255.} Rather than “imposing prescriptive security mandates,” the Commission adopted a “security-by-design approach” for spectrum bands above 24 GHz that would have a “minimal[] impact” on “design and development with respect to this nascent technology.”\footnote{\textit{Id.} at ¶¶ 262-263.} Even though these spectrum bands will not be auctioned or licensed for many
years, the Commission adopted a framework that encourages the development of security standards “in parallel” with emerging networks.30

Singling DSRC out for pre-launch cybersecurity mandates that must be met before DSRC operators can make authorized use of their spectrum turns the Commission’s approach in the Spectrum Frontiers Order on its head. It also would be unfairly prejudicial to DSRC operators, particularly GM, and lay waste to the enormous industry-government-academia partnership that has provided new V2V safety advances with built-in security and privacy technologies. DSRC operators have been using their licensed spectrum to develop and test DSRC V2V technology, and GM will be deploying DSRC V2V technology in its Model Year 2017 Cadillac CTS. Prohibiting DSRC deployment for years while agency proceedings unfold would not benefit the public, instead it would deny the public access to this important technology.31

IV. PETITIONERS’ REQUEST FOR AN “EMERGENCY” STAY IS PROCEDURALLY DEFECTIVE.

Petitioner's request for an emergency stay is procedurally defective and does not come close to meeting the demanding test for extraordinary relief. Accordingly, Petitioners’ “emergency” stay request must be denied.

Petitioners’ stay request faces three fatal problems. First, Petitioners do not address – let alone establish – the stringent standard for the extraordinary relief they seek. The Commission requires that any petitioner seeking the “extraordinary remedy of a stay” must show that: (1) it is likely to prevail on the merits; (2) it will suffer irreparable harm absent the grant of preliminary relief; (3) other interested parties will not be harmed if the stay is granted; and (4) the public

---

30 Id. at ¶ 256.
31 Prohibiting DSRC deployment would also support the commercial interests that Petitioners fear losing from DSRC’s success.
interest would favor grant of the stay.\footnote{Rates for Interstate Inmate Calling Services, Order Denying Stay Requests, 31 FCC Rcd 261 (2016).} The Petitioner’s brief does not even attempt to make these showings. Absent a showing by Petitioners on each of these elements, the Commission cannot grant a stay, even assuming it were otherwise appropriate, which is not the case.

Second, the stay is improper because the DSRC rules took effect more than a decade ago. A stay cannot preserve a state of affairs that long ago ceased to exist.\footnote{See Graddick v. Alabama, 453 U.S. 928, 936 (1981) (“Ordinary linguistic usage suggests that an order, once executed, cannot be ‘stayed.’ Affirmative action then becomes necessary to restore the status quo.”); Reed v. Rhodes, 472 F. Supp. 603, 605 (N.D. Oho. 1979) (“A stay does not reverse, annul, undo, or suspend what has already been done.”).} Operation of DSRC is not irreparable harm as the Petitioners contend; it is the status quo. Because Petitioners seek to change the status quo through a stay, their request is procedurally defective and must be denied.

Third, the Commission’s rules require that “any request to stay the effectiveness of any decision or order of the Commission shall be filed as a separate pleading.”\footnote{47 C.F.R. § 1.44(e).} Requests not filed as a separate pleading “will not be considered by the Commission.”\footnote{Id.} Petitioners disregard this rule entirely by combining their requests for rulemaking and for emergency stay in the same pleading. In the absence of a separately filed stay request, Petitioners’ request is procedurally defective and must be dismissed.
V. THE LEGALLY DEFECTIVE PETITION IS BASED UPON A FALSE PREMISE REGARDING THE NEED FOR PRESCRIPTIVE PRIVACY AND CYBERSECURITY RULES FOR DSRC OPERATORS.

GM has devoted substantial resources and implemented significant organizational and technical measures to protect privacy and address cybersecurity issues.\(^3^6\) As pointed out above, the automotive industry has worked for years with government and academia to advance V2V technology, including its security and privacy technology. Going further, the automotive industry has responded to evolving privacy issues by developing voluntary privacy protection measures such as the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services based upon the well-established Fair Information Practice Principles.\(^3^7\)

Petitioners’ scare tactics and unfounded predictions of “rapid and straightforward spread of malware, ransomware, or other forms of destructive software and coordinated cyberattacks” and, ultimately, a “car zombie apocalypse” are a sign of desperation and do not warrant a rulemaking.\(^3^8\) Indeed, Petitioners’ concerns about data privacy and cybersecurity associated with DSRC ring hollow in light of their failure to raise such concerns with NHTSA. Nearly two years ago, in its Advanced Notice of Proposed Rulemaking (“ANPRM”) on V2V

---

\(^3^6\) GM was the first auto manufacturer to create an integrated and dedicated global organization focused on minimizing the risks of unauthorized access to vehicles and customer data. GM has collaborated with experts in the defense and aerospace industries, government organizations, academia and industry consortiums on best practices and key lessons. GM also has launched a Security Vulnerability Disclosure Program, through which security researchers not working with GM can report via a secure website portal any security bugs or vulnerabilities they uncover related to the company’s products or services.


\(^3^8\) Petition at 5.
communications, NHTSA sought comment on privacy and cybersecurity issues.\(^39\) Although NHTSA received a wealth of comments in that proceeding, Petitioners stood on the sidelines, keeping silent on the “substantial risk” that they assert DSRC poses to personal privacy and cybersecurity.\(^40\) To the extent Petitioners were concerned about the implications of DSRC either for privacy or cybersecurity, they should have timely brought such concerns to NHTSA’s attention; that Petitioners failed to do so speaks volumes about their true intentions in requesting the Commission to stop the deployment of DSRC technology, despite its obvious public safety benefits.\(^41\)

Finally, NHTSA estimates that use of DSRC technology could potentially mitigate 80 percent of non-impaired crashes, reducing costs to our nation’s economy by $871 billion each year.\(^42\) With so much at stake, and backed by a substantial industry-government-academia


\(^{40}\) Petition at iii-iv.

\(^{41}\) Petitioners’ complaints about NHTSA’s ability to address cybersecurity issues in a timely and appropriate manner are unfounded. Petition at 5-6. Petitioners ignore NHTSA’s efforts in this space, which include establishing a new division in 2012 – Electronic Systems Safety Research – to conduct research on the safety, security, and reliability of electronic vehicle systems and consulting with other government agencies, vehicle manufacturers, suppliers, and the public on cybersecurity issues. See NHTSA and Vehicle Cybersecurity, available at http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity. Petitioners also mischaracterize the findings of the Government Accounting Office (“GAO”), which did not find, as Petitioners’ claim, that “NHTSA lacks critical expertise in cybersecurity and privacy to effective [sic] protect the auto industry from cyber threats.” Petition at iv (citing Government Accountability Office Report to Congressional Requesters, Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack (Mar. 2016) (“GAO Report”)). On the contrary, GAO’s only recommendation concerned defining and documenting NHTSA’s role and responsibilities in the event of a real-world cyberattack and how the agency “would coordinate with other federal agencies and stakeholders involved in the response.” Id. at 43-44.

commitment to develop DSRC V2V technology, GM believes that the time has come to make these benefits available to the public.

VI. CONCLUSION.

For the foregoing reasons, the Commission should deny the Petition.

Respectfully submitted,

GENERAL MOTORS COMPANY

By: /s/ Harry Lightsey
Harry Lightsey
Executive Director, Connected Customer,
Public Policy
GENERAL MOTORS COMPANY
25 Massachusetts Avenue N.W.
Suite 400
Washington, D.C. 20001

August 24, 2016
CERTIFICATE OF SERVICE

I, Patricia Destajo, hereby certify that on this 24th day of August, 2016, I caused a true and correct copy of the foregoing to be served by overnight mail on:

Michael Calabrese  
Director, Wireless Future Project  
Open Technology Institute at New America  
740 Fifteenth Street N.W. – 9th Floor  
Washington, D.C. 20005

Harold Feld  
Senior Vice President  
Public Knowledge  
1818 N St. N.W., Suite 410  
Washington, D.C. 20036

/s/ Patricia Destajo