August 24, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20553

Re: *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

The undersigned privacy and consumer advocates write to support the above captioned Petition for Rulemaking ("Petition"). Although the National Highway Traffic Safety Administration (NHTSA) 2014 Technical Report and Advanced Notice of Proposed Rulemaking include highly laudable "privacy by design" proposals, these proposals are inadequate to fully protect consumers. As detailed both in the Petition and in the attached letter from Senator Edward J. Markey (D-MA) and Senator Richard Blumenthal,[1] only grant of the Petition can adequately protect the public.

"Facebook On Wheels"

ITS America, the trade association representing the interests of the auto industry and other commercial DSRC interests, has made it clear that it intends to deploy commercial services on the 45 MHz of DSRC spectrum not exclusively allocated to life and safety traffic, public safety messages, or the mandatory "control channel" required under the FCC's DSRC rules standard. When asked by Politico reporter Margaret McGill whether NHTSA's privacy-by-design protections would apply to any commercial applications run on DSRC spectrum, ITS America Vice President Steven Bayless replied:

> "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."

Americans do not need to have 'Facebook on Wheels' imposed on them by government fiat in the name of public safety. Absent Commission action on the Petition, DSRC licensees will have the freedom to install any commercial application they chose on the consumer's government mandated DSRC device. Without Commission action on the Petition, DSRC licensees are free to partner with any commercial data broker, advertiser or any other third party with virtually no notice to consumers and no need to obtain consumer permission – or even provide consumers with a means of opting out of these commercial arrangements.

[1] Available at http://www.markey.senate.gov/imo/media/doc/2016-08-04-Markey-Blumenthal-Cybersecurity-cars-FCC.pdf

As documented by Senator Markey last year, the auto industry already uses technology to collect personal information on consumers without notice and without adequate protections.[2] Permitting DSRC to operate commercial applications on what is being sold to the American public as mandatory safety systems will only further aggravate the problems of maintaining privacy for America's drivers and passengers.

Cybersecurity Threats

The 2015 Markey Report also detailed the shocking inability of the auto industry generally to handle to handle cybersecurity threats.[3] This diagnosis has been confirmed by numerous private sector reports. A recent report by Intel identified 14 different ways a hacker can gain access to a car's operating system.[4] The auto industry is ill equipped to properly address these vulnerabilities. Former Ford technologist, John Ellis, recently highlighted this fact in an article for the Washington Post. "I'm scared because car manufacturers don't get software. This isn't a car problem. It's a software and business model problem."[5] The Government Accountability Office issued a report in January 2016, quoting NHTSA a saying it does not expect to even define NHTSA's roll in cybersecurity for cars until 2018.[6]

DSRC units provide an access route for malware to spread directly from car to car, enabling hackers to steal the personal information of drivers. Theses concerns are amplified in light of the impending NHTSA mandate, requiring all new model vehicles have DSRC units installed. As more cars hit the road with this technology, it becomes exponentially easier for hackers to spread malware not just from car to car, but into our nation's transportation infrastructure.

When asked about the security of DSRC Steven Bayless, ITS VP for Technology Markets, responded "[w]hat's being exchanged between vehicles is just data." "There's no possibility of a virus being spread between cars."[7] If the primary DSRC trade association

---

[2] Senator Ed Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (2015), *available at* http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[3] *Id.*

[4] Intel, *Automotive Security Best Practices: Recommendations for security and privacy in the era of the next-generation car* (2015) ("Intel Whitepaper"), *available at* http://www.intel.com/content/www/us/en/automotive/automotive-security-best-practices-white-paper.html.

[5] Craig Timberg, *Hacks on the Highway*, The Washington Post (July 22, 2015), *available at* http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/.

[6] 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*, ii (Mar. 2016), *available at* http://www.gao.gov/assets/680/676064.pdf.

[7] Margaret McGill, *Latest privacy debate: Crash-avoidance technology*, PoliticoPro (June 28, 2016) *available at*

doesn't understand that a virus is, at its core, data, it surely cannot be trusted to protect consumer's privacy.

The FCC Should Grant The Petition

As Commissioner O'Reilly has said, there is simply no justification for allowing the auto industry to use spectrum allocated for the protection of life and safety for commercial applications.[8] As shown in the Petition, allowing automakers to offer commercial applications on DSRC compromises the public safety mission of the DSRC service by compromising user privacy and by creating a path for the spread of malware from one infected car to the entire DSRC network.

We therefore ask the Commission to grant the Petition, including the request that the Commission stay operation of DSRC devices until the privacy and adequacy of the cybersecurity concerns are addressed.

Sincerely,

/s/ Connie Stewart
Executive Director
California Center for Rural Policy

/s/Katharina Kopp
Deputy Director, Director of Policy
Center for Digital Democracy

/s/Dee Davis
President
Center for Rural Strategies

/s/Linda Sherry
Director, National Priorities
Consumer Action

/s/Susan Grant
Dir. of Consumer Protection and Privacy
Consumer Federation of America

/s/John Simpson
Privacy Project Director
Consumer Watchdog

/s/Jeremy Gillula
Senior Staff Technologist
Electronic Frontier Foundation

/s/Claire Gartland
EPIC Consumer Protection Counsel
Electronic Privacy Information Center

/s/ Paul Goodman
Senior Legal Counsel
The Greenlining Institute

/s/Christopher Mitchell
Director, Community Broadband Networks
Institute for Local Self Reliance

---

https://www.politicopro.com/technology/story/2016/06/latest-privacy-debate-crash-avoidance-echnology-117891

[8] Michael O'Reilly, "Defining Auto Safety of Life in 5.9 GHz," FCC Blog (June 8, 2016). Available at: https://www.fcc.gov/news-events/blog/2016/06/08/defining-auto-safety-life-59-ghz (last visited August 18, 2016).

/s/Dr. Nicol Turner-Lee
Vice President
Multicultural Media, Telecom and Internet Council

/s/Andy Lomeli
Policy Associate
National Hispanic Media Coalition

/s/Michael Calabrese
Director, Wireless Future Project
Open Technology Institute

/s/Meghan Land
Staff Attorney
Privacy Rights Clearinghouse

/s/Harold Feld
Senior Vice President
Public Knowledge

/s/ Matthew R. Rantanen
Director of Technology
Southern California Tribal Digital Village

/s/Ed Mierzwinski
Consumer Program Director
U.S. PIRG

/s/Pam Dixon
Executive Director
World Privacy Forum

/s/Sascha Meinrath
Director
X – Lab