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 Communications Service in the 5.850-	)	
5.9925 GHz Band (5.9 GHz Band)	)	RM-_____

PETITION FOR RULEMAKING AND REQUEST FOR EMERGENCY STAY OF OPERATION OF DEDICATED SHORT-RANGE COMMUNICATIONS SERVICE IN THE 5.850-5.9925 GHZ BAND (5.9 GHZ BAND)

Harold Feld
John Gasparini
Public Knowledge
1818 N St. NW, Suite 410
Washington, DC 20036
(202) 861-0020

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

June 28, 2016

Pursuant to Rule 1.401, Public Knowledge and Open Technology Institute at New America ("Petitioners") file this Petition for Rulemaking and Request for Emergency Stay of Operation of the Dedicated Short-Range Communications ("DSRC") in the 5.9 GHz Band.[1] The DSRC service lacks rules to protect user privacy or to protect DSRC units from malware or other forms of cybersecurity attacks. Because General Motors ("GM") has announced an intent to deploy DSRC units in some model cars this fall,[2] the Commission must immediately prohibit use of DSRC until it adopts service rules protecting the cybersecurity and privacy of DSRC users – and DSRC operators demonstrate compliance with those rules.

Petitioners stresses that the cybersecurity and privacy vulnerabilities identified below are independent of the Commission's examination of whether or not to permit shared use by Part 15 devices in the DSRC band. The security vulnerabilities and the need for Commission action are intrinsic to the existing DSRC service, and magnified by the impending mandate from the National Highway Traffic Safety Administration ("NHTSA") to require all car manufacturers to include DSRC units in all new cars.[3] Whether or not the Commission allows operation of unlicensed devices in all or part of the DSRC band on a non-interfering basis, the FCC must impose adequate cybersecurity and privacy protections before allowing automakers to activate any DSRC systems.

[1] 47 C.F.R. § 1.401.
[2] Press Release, Cadillac to Introduce Advanced 'Intelligent and Connected' Vehicle Technologies on Select 2017 Models (Sept. 7, 2014), http://media.cadillac.com/media/us/en/cadillac/news.detail.html/content/Pages/news/us/en/2014/Sep/0907-its-overview.html.
[3] Chaminda Basnayake, *Connected Vehicles: Road-ready yet?* GPS World (May 10, 2016), http://gpsworld.com/connected-vehicles-road-ready-yet/.

SUMMARY

In 1999, the Commission authorized an allocation of 75 MHz for "Dedicated Short-Range Communication" ("DSRC").[4] Envisioned as part of a broader "Intelligent Transportation Service" network that paralleled the emerging public Internet, the auto industry and the Department of Transportation urged the FCC to adopt DSRC rules that enabled both non-commercial life and safety applications, and commercial applications such as mobile payments to gas stations, remote management of rental cars, and other undetermined commercial services.[5]

Unfortunately, the Commission did not at that time consider the implications of DSRC either for privacy or cybersecurity. The ability of DSRC units to monitor and report detailed personal information about location and driving habits of individuals raise enormous concerns for personal privacy. When coupled with storage of financial information and purchasing information through future mobile payment applications, or the use of DSRC streaming capability for delivering advertising or entertainment,[6] the substantial risk DSRC creates to personal privacy grows exponentially.

Far more troubling, however, is the way in which the failure to impose adequate cybersecurity obligations on DSRC licensees and operators threatens the safety of our national roadways. Over the last year, a number of high profile hacking incidents have highlighted the extraordinary vulnerability of cars to cyberattacks. Hackers have demonstrated the ability to seize control of braking, steering, and acceleration functions, which would allow a hacker to

[4] *See* In the Matter of Amendment of Parts 2 & 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 Services, *Report and Order*, 14 F.C.C. Rcd. 18221 (1999) ("1999 DSRC Order").
[5] *See* In the Matter of Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band), *Report and Order*, 19 F.C.C. Rcd. 2458 (2004) ("2004 DSRC Service Rules").
[6] *See* Michael Calabrese, *Spectrum Silos to Gigabit Wifi: Sharing the 5.9 GHz 'Car Band'* at 19-22 (Jan. 2016) ("Calabrese Report"), *available at* https://www.newamerica.org/oti/policy-papers/spectrum-silos-to-gigabit-wi-fi/.

remotely crash vehicles.[7] One report from Intel chronicled ***14 different ways*** a hacker can gain access to a car's operating system.[8] In March 2016, the Federal Bureau of Investigation ("FBI") and the Department of Transportation ("DoT") issued a joint Public Service Announcement warning car owners about the increasing vulnerability of their cars to "remote exploits" (i.e., cyberattacks).[9]

Even more troubling, Congressional reports have concluded that the car industry lacks the capacity or the culture to respond effectively to these threats.[10] To the contrary, as the Markey Report found, the culture of the car industry encourages bad behavior on privacy, lax cybersecurity, discourages auto manufacturers from publicizing and sharing information on potential vulnerabilities, and erects barriers to the ability of auto manufacturers to push out timely cybersecurity updates.

To date, the one thing that has prevented cyberterrorists from creating a "car zombie apocalypse" by infecting thousands of cars with malware designed to crash them into crowds or one another has been the inability of cars to communicate with each other. As one expert explained:

> "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

---

[7] *See, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, Wired (Jul. 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[8] 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.
[9] 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.
[10] *See, e.g.,* Senator Ed Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (Feb. 2015) ("Markey Report"), *available at* https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity 2.pdf; 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"), *available at* http://www.gao.gov/products/GAO-16-350.

> Ford. "You can do it on a one-car basis. You can't yet do it on a 100,000-car basis."[11]

DSRC provides precisely this capability to "weaponize" the vulnerability of cars through vehicle-to-vehicle communication ("V2V"). DSRC depends on high-speed, low-latency communication between vehicles, and must be linked directly to critical functions like acceleration, braking, and steering, in order to facilitate the supposed benefits to life and safety brought about by DSRC. DSRC units provide an access route for malware to spread directly from car to car, enabling hackers to steal the personal information of drivers and leaving cars open to "ransomware" or coordinated terrorist attack. When combined with the impending NHTSA mandate to require that ***all*** new model cars have DSRC units installed, the number of cars capable of spreading malware will grow exponentially over time. Only by acting now, before the auto industry can deploy any DSRC units, can the Commission adequately protect the public.

NHTSA LACKS CLEAR AUTHORITY AND LACKS THE NECESSARY EXPERTISE

As part of its rulemaking to mandate that all future cars include DSRC units, NHTSA has extensively considered both cybersecurity and privacy issues.[12] These efforts are insufficient for several reasons. First, while NHTSA exercises authority over life and safety, it is not a general purpose regulator of the automobile industry. Additionally, not all entities eligible for DSRC licenses are subject to NHTSA jurisdiction. This makes NHTSA's authority to impose necessary cybersecurity and privacy regulations for the DSRC service – particularly with regard to mobile

[11] 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/.
[12] NHTSA, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application* (Aug. 2014), *available at* http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

payments, advertising, streaming entertainment services, and other for-profit activities – extremely uncertain.

Additionally, as the GAO recently found, NHTSA lacks critical expertise in cybersecurity and privacy to effective protect the auto industry from cyber threats.[13] Indeed, NHTSA itself states that it will not have a clear position on whether there is even a need for cybersecurity standards in vehicles ***until 2018***.[14] Nevertheless, GM intends to deploy DSRC-equipped cars within the next few months, leaving drivers vulnerable to cyber-attacks and privacy violations without any NHTSA protection.

Nor does NHTSA have the expertise in wireless technology, cybersecurity, and network privacy that the FCC possesses. Since publishing the National Broadband Plan in 2010, the FCC has focused on cybersecurity and privacy as critical elements in life and safety systems.[15] Indeed, as described below, the cybersecurity and privacy provisions discussed by NHTSA in its 2014 Report, while impressive on the surface, suffer from significant limitations and inconsistencies which – unless the FCC acts immediately to adopt appropriate service rules – will leave the public dangerously vulnerable.

THE FCC SHOULD PROHIBIT COMMERCIAL OPERATIONS ON DSRC, IMPOSE CYBERSECURITY AND PRIVACY STANDARDS, REQUIRE LICENSEES TO SUBMIT A COMPLIANCE PLAN FOR FUTURE UPDATES, AND ADOPT DATA BREACH NOTIFICATION OBLIGATIONS.

As explained in detail below, the FCC needs to take the following steps to secure the DSRC service and prevent the NHTSA's impending DSRC mandate from becoming the primary

[13] *See* GAO Report at 32-43.
[14] *See* GAO Report at ii ("NHTSA is examining the need for government standards or regulations regarding vehicle cybersecurity. However, officials estimated that the agency ill not make a final determination on this need until at least 2018.")
[15] In the Matter of Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114, *Fourth Report and Order*, 30 FCC Rcd. 1269, ¶ 68 (2015) ("911 Geolocation Order"); In the Matter of Technology Transitions, GN

vector for spreading viruses and other malware through the literal highway rather than simply the information highway.

Prohibit commercial operation by the DSRC service. The Commission does not, as a general rule and as a matter of well-established public policy, permit life and safety allocations to engage in commercial operations with public safety spectrum. Commercial operations on life and safety spectrum not only represent an unjustified windfall, but detract from the ability to effectively perform the life and safety mission central to the allocation.

Here, the use of commercial activity on DSRC spectrum creates a host of vulnerabilities. It requires that the car operating system receive instructions from unsecured, private entities outside the NHSTA life and safety network and security system. For example, to provide mobile payment services, DSRC-equipped cars will need to support existing mobile payment platforms, including all their security vulnerabilities. Additionally, to make mobile payments through DSRC units installed in cars, drivers will need to expose their financial information to the automobile operating system and the DSRC unit. This creates a digital record of the most sensitive financial information for either the automobile industry or future hackers to collect and exploit.

By prohibiting any commercial activity on DSRC-allocated spectrum, the Commission would follow both best cybersecurity practices and best spectrum policy practices. As Commissioner O'Rielly recently observed, it is the safety of life features of DSRC that warrant protection.[16] Since the initial authorization of DSRC in 1999, every major spectrum policy document has condemned the approach adopted by the Commission of allocating exclusive

---

Docket No. 13-5, *Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking*, FCC 15-97, ¶ 208 (2015) ("Tech Transitions Order").

bands for commercial purposes without an auction.[17] Authorizing DSRC for commercial uses is not merely an anachronism, it is a dangerous anachronism that heightens the danger of mass cyberattack with no offsetting benefits.

Require DSRC licensees to submit a cybersecurity and privacy plan before going live with DSRC units. Since the Commission recognized the importance of cybersecurity and privacy in the 2010 National Broadband Plan, the Commission has increasingly required that licensees demonstrate that new technologies will include protections for cybersecurity and for privacy protection. This includes safety of life services.[18] The Commission should update its 2004 service rules by requiring that DSRC licensees present a plan for ongoing cybersecurity updates and privacy protection that is both adequate today and will remain adequate going forward.

Impose data-breach notification rules and liability for failure to maintain adequate privacy protection and cybersecurity. In the context of Customer Proprietary Network Information ("CPNI"), the Commission has imposed obligations on licensees to maintain appropriate precautions; to notify law enforcement, the Commission, and customers in the event of a data breach; and, to take necessary steps to remediate problems as soon as they come to the attention of the licensee.[19] The Commission should use its authority under Section 303(b) and 303(r) to impose similar obligations on DSRC licensees. Although DSRC is not a common carrier service and thus automatically covered by Section 222, no one can doubt that protecting

---

[16] *See* Commissioner Michael O'Rielly, *Defining Auto Safety of Life in 5.9 GHz*, FCC Blog (June 8, 2016), https://www.fcc.gov/news-events/blog/2016/06/08/defining-auto-safety-life-59-ghz.
[17] Cite spectrum task force, National Broadband Report, PCAST Report
[18] *See* 911 Geolocation Order at ¶¶ 69-70.
[19] In the Matter of Lifeline and Link Up Reform and Modernization, WC Docket No. 11-42, *Order*, DA 14-785 (2014) ("2014 Lifeline Order").

the privacy and security of America's drivers serves "the public interest, convenience and necessity."[20]

If auto manufacturers and NHTSA insist on installing a DSRC unit in ever car, truck or motorcycle capable of spreading malware and capturing the private information of every single American, a device that will follow us not merely on the roads, but into our driveways and garages, then the Commission must act. It must act immediately, before GM or other manufacturers can release unprotected versions of DSRC and create a permanent security hole in the system.

[20] 47 U.S.C. § 303(r).

TABLE OF CONTENTS

ARGUMENT

I. INTRODUCTION

Pursuant to Rule 1.401, Public Knowledge and Open Technology Institute at New America ("Petitioners") file this Petition for Rulemaking and Request for Emergency Stay of Operation of the Dedicated Short-Range Communications ("DSRC") in the 5.9 GHz Band.[21] The DSRC service lacks rules to protect user privacy or to protect DSRC units from malware or other forms of cybersecurity attacks. Because General Motors has announced an intent to deploy DSRC units in some model cars this fall,[22] the Commission must immediately prohibit use of DSRC until the Commission adopts service rules protecting the cybersecurity and privacy of users, and DSRC operators demonstrate compliance with those rules.

Petitioners stress that the cybersecurity and privacy vulnerabilities identified below are independent of the Commission's examination of whether or not to permit shared use by Part 15 devices in the DSRC band. The security vulnerabilities and the need for Commission action are intrinsic to the existing DSRC service, and magnified by the impending mandate from the National Highway Traffic Safety Administration ("NHTSA") to require all car manufacturers to include DSRC units in all new cars.[23] Whether or not the Commission allows operation of unlicensed devices in all or part of the DSRC band on a non-interfering basis, the FCC must impose adequate cybersecurity and privacy protections before allowing automakers to activate any DSRC systems.

---

[21] 47 C.F.R. § 1.401.

[22] Press Release, Cadillac to Introduce Advanced 'Intelligent and Connected' Vehicle Technologies on Select 2017 Models (Sept. 7, 2014), http://media.cadillac.com/media/us/en/cadillac/news.detail.html/content/Pages/news/us/en/2014/Sep/0907-its-overview.html.

II. INTEREST OF PETITIONERS

Public Knowledge is a nonprofit technology policy organization that promotes freedom of expression, an open internet, and access to affordable communications tools and public works. As part of that mission, Public Knowledge advocates on behalf of consumer interests for balanced and pro-competitive communications policies by participating in regulatory proceedings and, where appropriate, engaging in legal action. Communications law, and particularly matters relating to spectrum policy, is a subject area in which Public Knowledge has both strong interests and substantial expertise.

Open Technology Institute at New America works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

III. CYBERSECURITY THREATS FROM CONNECTED VEHICLES ARE REAL, AND ARE AMPLIFIED BY DSRC.

As technology increasingly permeates the vehicles populating our nation's roadways, the number of attack vectors for cyberthreats increases. A report from Intel recently identified at least 15 exposed attack surfaces on modern vehicles, including smartphones, bluetooth and WiFi features, tire-pressure monitoring systems, and the numerous engine control units ("ECUs") that combine to form the brain of a modern automobile.[24] These systems are linked together to facilitate safety features like automatic braking, collision avoidance, and blind spot monitoring, by legacy systems called controller area networks ("CANs"). As noted by the Washington Post,

---

[23] Chaminda Basnayake, *Connected Vehicles: Road-ready yet?* GPS World (May 10, 2016), http://gpsworld.com/connected-vehicles-road-ready-yet/.

these CAN networks don't include any authentication security, meaning that "onboard computers typically have no way to know whether a given command originates from the car's engine control unit, from a mechanic, or from a hacker."[25] A hacker who compromises any one of a modern car's wireless entry points ("WEPs"), then, would be able to exploit that weakness to send messages to other, interconnected parts of the car, using the CAN.

This problem is disturbing on its own, and is not a fantasy - it is a reality. Researchers have demonstrated an ability to use vulnerabilities in recent-model-year road cars to seize control of braking and steering, and disable engines, remotely.[26] As a result, Fiat Chrysler recalled 1.4 million vehicles for security updates. Researches noted, however, that "They really just patched one vulnerability, but they didn't fix the systemic issues."[27] As the GAO reported recently, knowledge of these vulnerabilities is not new. In 2011, university researchers were able to remotely control brakes and engine functions in two General Motors models using vulnerabilities in short- and long-range wireless connections. The threat of cyberattacks on automobiles is real, and cars are vulnerable. As Tufts University researcher Kathleen Fisher put it to the Washington Post, "If we've learned anything from the Internet, it's that [hacking is] clearly going to happen."[28]

The situation has become so acute that the Federal Bureau of Investigation and the DoT issued a joint Public Service Announcement in March 2016.[29] Titled "Motor Vehicles Increasingly Vulnerable To Remote Exploits," the alert cautioned drivers to protect themselves by (in addition to other precautions) "exercise[ing] discretion when connecting third party

---

[24] *See* Intel Whitepaper at 5.
[25] *See* Timberg, *supra* note 12.
[26] Jeep hacking incident
[27] Timberg, *supra* note 12.
[28] *Id.*

devices to your vehicle." DSRC, however, ***requires*** that all automobiles with DSRC units communicate automatically with all other DSRC devices – making it impossible for drivers to comply with the FBI and DoT security advice.

One of the things we've learned from the growth and development of the Internet is that some of the most impactful cyberattacks come not only in the form of individual, targeted hacks, but in expansive, self-perpetuating viruses and worms which spread through interconnected networks and widespread vulnerabilities. The potential threat from automobile hacking is currently relatively limited, as cars must be targeted individually while in motion. DSRC threatens to open a whole new attack vector, allowing hackers to infect multiple cars, or develop tools which spread from vehicle to vehicle through the necessary two-way communications paths on which DSRC depends for its life-and-safety tasks. As the Post put it, "Imagine a single infected WiFi beacon on a stretch of highway delivering a virus to every passing vehicle."[30] DSRC takes this threat one step further. DSRC systems will not only sit by the side of the road, but also travel with every DSRC-equipped car, actively seeking out other DSRC-equipped cars with which to communicate.

Deployment of DSRC without robust cybersecurity protections will present the very real possibility that DSRC-equipped vehicles could spread a virus from one to another, and to every other car whose path they cross as they spread out through the road network. DSRC depends on high-speed, low-latency communication between vehicles, and must be linked directly to critical functions like acceleration, braking, and steering, in order to facilitate the supposed benefits to life and safety brought about by DSRC. A vulnerability in this area would provide attackers with

---

[29] *See* FBI Alert, *supra* note 10; *See also* Andy Greenberg, *The FBI Warns That Car Hacking is a Real Risk,* Wired (Mar. 17, 2016), https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/.
[30] Timberg, *supra* note 12.

a clear path not only to those most safety-critical areas of a car's internal systems, but also a direct path to every other DSRC-equipped car on the road.

DSRC units would thus provide a pathway to the rapid and straightforward spread of malware, ransomware, or other forms of destructive software and coordinated cyberattacks, potentially including terrorist actions. DSRC would allow cyberattacks on vehicles to be weaponized, spreading easily across a common point of attack which is included in all vehicles, by Federal mandate, enabling attacks on an unprecedented scale. This is the sort of "car zombie apocalypse" that the auto industry is simply not equipped to prevent or address, and it would be enabled and streamlined by the deployment, as currently proposed, of DSRC.

IV. THE AUTO INDUSTRY AND ITS REGULATORS ARE NOT EQUIPPED, CULTURALLY OR TECHNOLOGICALLY, TO ADDRESS CYBERSECURITY ISSUES IN AN APPROPRIATE MANNER.

As discussed above, cybersecurity is critical to the continued safety of both modern and next-generation automobiles. Today's cars are already vulnerable, and the vulnerabilities will only increase as the auto industry and NHTSA scramble to secure their grip on this vital spectrum by rushing unsecure, unprepared technology, based on a 15-year-old vision of "smart" cars, to market. In an effort to cement their control and avoid scrutiny, they pair this frantic effort with a plan to mandate that all new cars incorporate this technology, thus locking these critical vulnerabilities into future generations of cars by virtue of DSRC's backwards-compatibility requirement. All this, from an agency and an industry that have not yet shown any capability to handle today's cybersecurity threats, let alone those which will arise in an increasingly connected future.

NHTSA's inability to adequately address cybersecurity concerns is elegantly illustrated by two sentences from a March 2016 GAO report on Vehicle Cybersecurity. In discussing the

government's role in vehicle cybersecurity, the report states that "pursuant to a statutory mandate, NHTSA is examining the need for government standards or regulations regarding vehicle cybersecurity. However, officials estimated that the agency will not make a final determination of this need ***until at least 2018.***"[31] Meanwhile, the auto industry and NHTSA are rushing ahead, attempting to bring first generation, pre-standards vehicles to market and impose this mandate prior to the end of the year. An agency that won't even know if cybersecurity rules are needed, for two more years, wants to mandate connecting all of America's already-vulnerable cars together as soon as possible, without even having decided whether cybersecurity is important enough to justify rules. This is obviously untenable and contrary to the public interest.

The auto industry, meanwhile, has a less than stellar record on cybersecurity. Researchers have already demonstrated that the cars that roll off of industry assembly lines are vulnerable, and industry has, as always, been reactionary in response. They've issued recalls, but done little directly to address the cybersecurity issue. As the Washington Post reported, one researcher wondered "If the industry [had] the right business incentives to improve cybersecurity."[32] A former Ford technologist who now works in consulting observed, in that same article, that "outsiders underestimate how poorly suited the industry is to combat the growing cybersecurity threat." "I'm scared because car manufacturers don't get software. This isn't a car problem. It's a software and business model problem," Fisher told the Post.[33]

Congress is starting to wake up to this reality. Senator Ed Markey's report on automaker cybersecurity and privacy practices was telling, describing in detail "the alarmingly inconsistent

[31] *See* GAO Report at ii (emphasis added).
[32] *See* Timberg, *supra* note 12.
[33] *Id.*

and incomplete status of industry security and privacy practices"[34] The GAO found similar concerns, noting in particular that stakeholders frequently cited "the lack of transparency, communication, and collaboration regarding vehicles' cybersecurity" among auto manufacturers and their suppliers.[35] The report continued:

> "Highlighting the lack of transparency and collaboration that exists among the players in the automotive supply chain, one leading researcher we spoke with stated that 'the most important and interesting commonality' with respect to the vulnerabilities identified in his research was that the vulnerabilities were located precisely at the interfaces where software code written by different supply chain players has to interact."[36]

In other words, the most vulnerable parts of a car, and the area the auto industry is least effective, transparent, collaborative, or communicative in addressing, is the interface (or multiple interfaces) among different systems supplied by different companies. These interface points are precisely the locations where DSRC would be required to integrate not only with key safety-critical systems including brakes, steering, and engine control, but also integrate directly with other vehicles on the road. Here, at those critical points where the addition of DSRC systems would not only provide yet another means of attack to already-vulnerable vehicles, but also a means of attackers leaping from car to car, is the precise sort of interface point which the auto industry most commonly fails to protect.

Other concerns raised by the GAO report include the auto industry's "historical lack of cybersecurity expertise" as a challenge to be considered in looking at vehicle cybersecurity.[37] While the report acknowledges that there are challenges relating to labor availability that make may make the rapid growth of cybersecurity teams within this industry challenging, there is a

[34] *See* Markey Report at 2.
[35] GAO Report at 25.
[36] GAO Report at 26
[37] GAO Report at 27

point missed. These issues are not new. Cybersecurity is not a new concern. It grew out of the Internet and the growth and proliferation of networks. Certainly, the integration of network technology into cars, which began in the 1980s and 1990s, should have sparked concern for cybersecurity. The auto industry, however, has shown itself historically to be backward-looking in its culture, addressing known issues only after problems arise. Even now, as they're beginning to finally catch up with the times and pay attention to cybersecurity, stakeholders protest that it simply may not be worth the money. Stakeholders reported to the GAO general agreement that large-scale innovation and change to address cybersecurity "would comprise a major upfront expense, which ultimately contributes to automakers' continued reliance on legacy systems with inherent security weaknesses, such as CAN."[38] The report continues:

> "In addition, stakeholders noted that automakers may not be able to pass the costs of cybersecurity protections onto consumers as they can with other features, such as connectivity and convenience features. As a result, automakers will have to balance the costs of cybersecurity protections against the risks facing vehicles and consumers' willingness to pay."[39]

This attitude reflects several substantial problems with the auto industry's culture. First and foremost, the phrasing of stakeholder responses suggests a prevailing view within the industry that cybersecurity is a separate feature, to be weighed and balanced against things like connectivity. Cybersecurity must instead be thought of as a necessary component, essential to offering any connectivity or convenience feature. That the industry does not recognize this is troubling, though not as so worrying as the clear indications that industry stakeholders view safety of life attained through cybersecurity as something to be balanced against whether or not consumers will pay for it. It should, again, be an essential prerequisite, akin to the presumption that a car comes with tires, in order to ensure that it can operate safely and reliably on the road.

[38] *Id*.

"Connectivity and convenience" features, as the report describes it, must have cybersecurity baked in from their earliest design, not tacked on later as some form of cost benefit analysis. That the industry fails to grasp this is deeply troubling, and underscores even further how woefully ill-equipped they are to even begin addressing these issues. And yet, they push onward in their zeal to bring products to market, spurred on inexorably by an agency that won't even be able to determine whether or not cybersecurity standards are even necessary, until 2018.

V. THE COMMISSION'S FAILURE TO IMPOSE CYBERSECURITY AND PRIVACY MANDATES IN 2004, WHILE UNDERSTANDABLE, MUST BE REMEDIED IMMEDIATELY.

The Commission allocated the UNII-4 band for DSRC in 1999, and established service rules in 2004.[40] At the time, concern with cybersecurity and privacy had not yet penetrated into the thinking of the average American – or the Commission. In this time before terms like "big data" and "identity theft" became part of the everyday lexicon, no one worried that information about geolocation or driving habits mattered. Nor did anyone imagine that as our cars increasingly became computers on wheels, that malicious hackers could target vital car functions like acceleration and braking in the same way they target our electric grid and banking system.

As a consequence, neither the Commission nor any interested party considered the cybersecurity vulnerabilities and privacy implications as part of the service rules. In authorizing DSRC licensees to offer commercial services that would require drivers to expose highly sensitive private information, such as credit card information, the Commission engaged in no cost/benefit analysis of the potential risks versus the potential benefits to the public interest. Instead, the Commission reflexively blessed proposals made by the auto industry, and assumed that permitting greater use of excess DSRC spectrum would benefit the public interest.

---

[39] *Id.*

As discussed below, developments in the last decade have taught the Commission otherwise. With the impending deployment of DSRC units, and the potential that NHTSA will mandate installation of DSRC units in future automobiles, the Commission must move swiftly to remedy the omission of cybersecurity and privacy protections from the DSRC service rules. Such action is consistent with the Commission's recent joint efforts with the Federal Trade Commission (FTC) to evaluate how CMRS licensees and others in the mobile ecosystem ensure that mobile devices receive timely cybersecurity patches and upgrades to address newly discovered vulnerabilities.[41] Given the potentially deadly consequences of cyberhacking and DSRC, the Commission must act to ensure adequate cybersecurity and privacy protections ***before*** permitting DSRC units to become operational.

A. Beginning with the Pretexting Order in 2007, the FCC has increasingly recognized the importance of embedding cybersecurity and privacy protections in service rules.

The Commission first began to recognize the potential harm from identity theft and the need for cybersecurity regulations in the context of the *2007 Pretexting Order*.[42] There, the Commission observed that third parties were stealing the personal information of landline and mobile telephone subscribers by pretending to be the subscriber. These "pretexters" would then use the stolen information for purposes ranging from identity theft to stalking and threatening bodily harm.[43] As a consequence, the Commission imposed strict limits on the ability of providers to share the information collected with third parties, obligated providers to adopt

---

[40] *See generally* 1999 DSRC Order; 2004 DSRC Service Rules.
[41] *See generally* Joint FCC/FTC Inquiry into Mobile Device Security Updates (May 9, 2016), https://www.fcc.gov/document/fcc-launches-inquiry-mobile-device-security-updates, https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.
[42] In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information, 22 FCC Rcd. 6927 (2007) ("Pretexting Order").
[43] *Id.* at 6947-48.

reasonable security measures, and required that providers notify law enforcement and customers in the event of a data breech.[44]

Over the years, the Commission has become increasingly aware of the need to incorporate cybersecurity and privacy protections in its service rules – and to indoctrinate a culture of cybersecurity and privacy protection throughout the Communications ecosystem. In 2010, the National Broadband Plan recommended that the Commission create a "cybersecurity roadmap."[45] In recent years, the Commission has consistently required service providers to demonstrate adequate capability to protect their networks from cyberattacks and protect the privacy of users. For example, the FCC explicitly sought comment on cybersecurity and privacy when imposing enhanced obligations for Geolocation for 911.[46] The FCC reviewed the capacity of Telcordia to provide adequate cybersecurity protection and privacy protection as a necessary component of the rebid of the contract to administer the Local Number Portability Database.[47] In the Tech Transition Framework, the Commission reaffirmed the importance of cybersecurity and tentatively adopted cybersecurity as one of the factors for consideration in its 214(a) process.[48]

B. The public interest and public-safety considerations in particular require the commission to conduct a rulemaking to protect DSRC users.

The public interest now requires the Commission to amend the service rules for DSRC to reflect the need for robust cybersecurity protection for wireless networks – particularly where personal privacy is at risk. As discussed at length above, the impending activation of the first

---

[44] *Id.* at 6948-52.
[45] National Broadband Plan, Chapter 16.2; *See also* Public Notice, FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap, PS Docket No. 10=146, 25 FCC Rcd. 10570 (2010); *See also* In the Matter of Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, 31 FCC Rcd. 594 (2016).
[46] *See* 911 Geolocation Order at ¶¶ 54-59.
[47] Telcordia Technologies Inc. Petition to Reform Amendment 57 and to Order A Competitive Bidding Process for Number Portability, 30 FCC Rcd. 3082, 3113-36 (2015).
[48] *See* Tech Transitions Order at ¶ 208.

DSRC units exposes all cars equipped with DSRC to cyberattacks from infected cars. GM has informed the Commission that it intends to deploy DSRC in Model Year 2017 Cadillac CTS Vehicles.[49] Only by conducting a new rulemaking to alter the Commission's service rules can the FCC adequately protect the public.

It is imperative that the Commission act immediately, rather than wait for future developments. In light of the facts discussed above, the danger to the public from unregulated DSRC devices transmitting malware from an infected car to any other DSRC-equipped car with which it comes in contact is real and immediate. As discussed at length in the Markey Report, no mechanism currently exists to reliably require GM – or any other car manufacturer deploying DSRC – to take precautions against cyberattacks, to notify consumers in the event new vulnerabilities are discovered, or to act in a timely manner to recall vehicles and install needed upgrades. It lies with the Commission to impose these responsibilities on DSRC licensees, and to do so ***before*** disasters occur.

VI. THE COMMISSION MUST MAKE DSRC A STRICTLY NONCOMMERCIAL SERVICE

The first and foremost vulnerability of DSRC is its use as a commercial service in addition to its primary purpose of being limited to life and safety. As explained in greater detail below, opening DSRC to commercial applications such as mobile payments, streaming advertisements and entertainment or other vehicle management services as discussed by the Commission in its 2004 *DSRC Service Rules Order* needlessly creates exploitable vulnerabilities that would not exist if the Commission limited DSRC to life and safety applications.[50]

[49] *See* June 2016 *Ex Parte* Letter from Auto Alliance & Members, ET Docket No. 13-49 (June 2, 2016), https://ecfsapi.fcc.gov/file/60002091196.pdf.

[50] Indeed, the Commission does not generally permit life and safety allocations to be used for commercial purposes. As discussed at length in the Commission's *800 MHz Rebanding Order*, the Communications Act expressly

A. Permitting commercial activities, such as mobile payments, dramatically increases the likelihood of cyberattacks and privacy violations with no offsetting public interest advantages.

The trade-offs between the openness of the network, the flexibility of use, and the potential vulnerabilities, are well known in cybersecurity. The most secure system is the system that is totally disconnected from all other systems and devices, which avoids adding the complexity of cooperation between entities outside the control of the system operator and reduces the points of entry into the system. But a system that only talks to itself is limited in many ways: it can't get information easily, it can't transmit information easily, it lacks utility for broader purposes, and it significantly reduces the number of people capable of using it.

Additionally, the smaller the number of possible inputs the system will accept, the harder it is for someone to use the interface with the outside world as a way to hack the system. A system interface that will not accept inputs that modify the underlying operating system is more secure than a system that allows the user to download and install software that does. A system that does not allow a user to download applications cannot become infected by applications that perform in ways the user neither understands nor desires. But a device that will not accept software downloads is frozen as a tool. It must either be updated manually or used only for a specific purpose and never modified.

As a paradigmatic example, consider a typical bank ATM network. The bank machine does not communicate with the public Internet, only with the ATM network and the member banks through the ATM network. A nefarious customer cannot easily load a malicious program on a magnetic strip of a pseudo-bank card, because the magnetic strip reader will only accept a very limited set of data inputs – those needed to verify the identity of the cardholder and locate

---

prohibits awarding exclusive use spectrum for commercial purposes for free, even to assist public safety. *See*

the account. But this limitation makes it harder for the bank to offer services. By requiring the customer to physically access a specific machine, and limiting the customer to a basic set of inputs on a keyboard that accepts a limited character set, limits the bank to offering a very limited suite of services – and only to those customers willing to come to the physical location of a bank machine and conduct business in a relatively open space.

By contrast, allowing a customer to access their bank account online through their home computer, via the public Internet, dramatically increases the ability of the customer to use the bank's services. But this enhanced access and utility comes at the cost of security. If the customer's computer is infected with malware, the customer will reveal confidential information to an identity thief, allowing the thief to access the bank's systems as the customer, withdraw money, accumulate credit charges, or otherwise use the access to profit. Additionally, by creating an interface with the public Internet, the bank exposes its systems to a plethora of new and sophisticated direct attacks on its systems. Finally, in the event an of a cyber exploit from a bank employee, the ability to communicate over the public Internet enhances the ability of the rogue employee to share information from the bank or otherwise cause harm.

1. Application of these basic cybersecurity principles to DSRC design

With this trade-off firmly in mind, the Commission should reexamine the fundamental wisdom of allowing DSRC licensees to offer services unrelated to life and safety. The Commission authorized DSRC expressly to "increase the safety and efficiency of the nation's surface transportation system" with particular emphasis on "safety applications such as crash

---

Improving Public Safety Communications in the 800 MHz Band, 19 FCC Rcd. 14969, ¶¶ 72-87 (2004).

avoidance and intersection collision avoidance."[51] It follows that any functions that do not serve these ends that expand the vulnerability of the DSRC-equipped cars should be prohibited.

In requesting the Commission prohibit commercial activity on DSRC spectrum, it is important to emphasize that this is most explicitly ***not*** general-purpose spectrum. To the contrary, DSRC is a unique and valuable allocation of spectrum for the exclusive use of DSRC – explicitly to promoted the public safety goals of collision and crash avoidance. The Commission only authorized commercial activity on DSRC spectrum as a means of promoting deployment of nationwide DSRC-based applications.[52] As discussed in more detail below, this consideration is no longer applicable. Not only did the possibility of offering for-profit services fail to provide proper incentive for DSRC deployment, but the marketplace has provided an abundance of alternative wireless means – using both licensed and unlicensed general purpose spectrum – to provide the relevant services.

While there is no doubt that auto manufacturers would find the ability to offer commercial services – including those that depend on harvesting the personal information of drivers without their knowledge or consent – highly profitable, that is not the question. The question is whether continuing to permit auto manufacturers to provide commercial services over licenses allocated to them for the express purpose of protecting life and safety needlessly increases the vulnerability of DSRC-equipped cars to cyberattack, or needlessly violates the privacy of drivers and passengers.

[51] *See* 2004 DSRC Service Rules at ¶ 14.
[52] *Id.* at ¶ 16.

2. The ability to offer commercial services requires providers to increase both the vulnerability to cyberattack and the risk of privacy violations.

To offer commercial services, DSRC systems must transmit to devices and networks outside the protected confines of the DSRC system (and the vulnerable environment of the automobile) and take a range of inputs capable of directly impacting the operation of the vehicle. Appendix C of the 2004 *DSRC Order* lists proposed commercial operations for DSRC licensees.[53] A review shows how DSRC would need to accommodate numerous inputs that would give rise to exploitable weaknesses due to the need to accommodate a wide range of operating systems and inputs. For example, "Electronic Payments" requires that DSRC units have the capability to talk to any gas pump, drive through window, or parking lot – as well as an ability to interface with credit cards and other mobile payment systems.[54] "Commercial Vehicle Operation" explicitly contemplates tracking sensitive travel data and "CVO Truck Stop Data Transfer."[55]

Permitting DSRC licensees to conduct such operations requires DSRC systems to circumvent the highly constrained system described in the NHTSA 2014 Report and its picture of multiple certification authorities carefully curated by the auto industry under the watchful supervision of NHTSA. The ability to conduct these transactions, or explore additional lines of businesses such as video streaming and advertising, requires DSRC licensees to architect systems that are sufficiently open and flexible to enable such commercial activity.

Worse, the ability to provide these commercial services creates a financial incentive for DSRC licensees to increase risks and vulnerabilities, prioritizing the potential for profit over the public safety mission for which the Commisison allocated the spectrum. Indeed, the Markey

[53] *See* 2004 DSRC Service Rules at Appendix C.
[54] *Id.*

Report chronicles exactly this kind of reckless behavior with regard to cybersecurity user privacy.[56] In the absence of FCC service rules, it is logical to conclude that the automobile will once again fail to provide adequate cybersecurity and privacy protections when exploiting the commercial potential of DSRC.

Again, it is important to stress that this is not flexible- use unlicensed spectrum open to everyone on equal terms. Nor is this exclusively licensed flexible use spectrum for which auto manufacturers have paid billions at auction. Auto manufacturers have received this exclusive allocation for free, and for DSRC use alone. This allocation of billions of dollars worth of spectrum rights is justified solely by the public interest value of the life and safety functions of DSRC. Where commercial use of this free spectrum actually ***creates*** threats to life and safety in the form of increased vulnerability to cyberattacks, the Commission must act to restrict this activity so as to ensure that the spectrum allocation serves its proper use and does not endanger the public.

B. Other technologies available in the marketplace provide more immediate protection from potential collisions, and provide adequate safety without creating new cybersecurity vulnerabilities

Delay in the deployment of DSRC will not significantly impact public safety. The marketplace has already adopted a host of new technologies that are both more effective than DSRC in preventing collisions, and which do not create the same cyber-vulnerabilities or risks to user privacy. For example, car radar systems using unlicensed spectrum have been increasingly deployed since the Commission in 2012 adopted new rules to facilitate these systems.[57] Collision

---

[55] *Id.*
[56] *See* Markey Report, *supra* note 11.
[57] *See* Amendment of Sections 15.35 and 15.253 of the Commission's Rules Regarding Operation of Radar Systems in the 76-77 GHz Band, Report and Order, ET Dockets No. 11-90 and 10-28, 27 FCC Rcd 7880, 7885 (2012) ("Vehicular Radar R&O").

and crash avoidance systems using technologies such as LIDAR, ultra-wideband, and vehicular cameras are likewise already being far more aggressively deployed in the marketplace. Deployment of DSRC units offers only incremental improvement over these technologies that the market has already developed and embraced.[58]

Not only have these technologies been embraced by the market, but they do not create nearly the same level of cybersecurity threat. Car radars, for example, are designed to receive a very limited set of inputs – a return wave form. It is not possible to spread malware through a car's radar system because the car cannot download software through its radar system. Similarly, a car cannot receive a virus through its rear-view camera. Not only are collision and crash avoidance systems based on these technologies therefore more secure, but they demonstrate the principle of limiting inputs as a means of enhancing security.

Additionally, to the extent DSRC deployment offers incremental improvement, delaying deployment until the Commission establishes adequate cybersecruity and privacy protections will have little impact at this stage. Unlike the technologies discussed above, which provide protection for an individual car, DSRC provides no protection unless the approaching car or obstacle is also equipped with a DSRC transmitter. Accordingly, delaying GM's "pre-cybersecurity standards" launch will have no impact on the overall safety of vehicles on the road today, nor will it significantly delay any future beneficial impact of DSRC.[59]

---

[58] *See* Calabrese Report, *supra* note 7.

[59] It is reasonable to ask, in light of the availability of more secure and more immediately effective alternatives, why the DSRC service remains necessary. Whatever it's potential benefits when authorized in 1999, a wealth of alternatives for both the life & safety and commercial services are now available in the marketplace – and without the need for an extensive government mandate from NHTSA. This Petition, however, assumes that DSRC will remain the choice of NHTSA no matter what superior alternatives may already exist in the marketplace. Accordingly, the Commission must therefore act to create service rules to minimize the risks created by the potential NHTSA mandate.

C. Based on auto industry and NHTSA filings and testimony in related proceedings, a non-commercial condition will not impact incentives to deploy, or be otherwise contrary to the public interest

Finally, it is noteworthy that neither the auto industry nor NHTSA has asserted any public interest value in offering commercial services over DSRC spectrum. To the contrary, both the auto industry and NHTSA have repeatedly asserted that their sole concern lies with protecting the life and safety of vehicular traffic. While the auto industry has never affirmatively disavowed its intent to profit from the free allocation of exclusive use spectrum, neither the auto industry or NHTSA have asserted that the ability to offer commercial services remains necessary to foster deployment of DSRC technology.

If anything, both the auto industry and NHTSA have reached the opposite conclusion. In proposing to mandate DSRC in all automobiles going forward, regardless of market adoption or user preference for more immediately effective and less risky alternatives, NHTSA and the auto industry acknowledge that the market has failed. Despite widespread support by major auto manufacturers, combined with the ability to offer commercial services, not a single DSRC unit has been deployed or activated in the United States since the service was authorized and rules established in 2004. In its 2014 ANPRM, NHTSA tentatively concluded that the only way to ensure sufficient deployment of DSRC to achieve effectiveness was to overrule the market decision to adopt alternatives and impose DSRC on the industry as a matter of federal law.[60]

Setting aside the wisdom of this policy, it is clear that there is no public interest value in continuing to allow auto makers to enjoy a spectrum windfall by offering commercial services unrelated to the core life and safety purposes of the spectrum. Given that these commercial

[60] *See generally* National Highway Traffic Safety Administration, *Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications*, Docket No. NHTSA-2014-0022, *Advance Notice of Proposed Rulemaking*, 79 Fed. Reg. 49270 (Aug. 20, 2014).

operations enhance the risk of cyber attack, and provide an incentive to auto manufacturers to collect the private information of drivers and passengers without their knowledge or consent, the Commission should modify the DSRC service rules to prohibit commercial services from being offered on the band.

VII. THE COMMISSION MUST ADOPT RULES THAT ADEQUATELY PROVIDE CYBERSECURITY MEASURES AND PROTECT DSRC-EQUIPPED VEHICLES FROM CYBERATTACK, AS WELL AS PROTECT USER PRIVACY.

A non-commercial condition, while significantly reducing the vulnerability to cyberattack and diminishing incentive to violate customer privacy, is not itself sufficient. Even as a service dedicated purely to life and safety, DSRC has the capacity to spread malware among infected cars – providing a vector for a mass hack attack. Accordingly, the Commission must adopt the following additional rules.

A. DSRC Licensees must submit a cybersecurity and privacy plan before activating their DSRC system

It is entirely possible that GM, or another DSRC licensee, has already developed suitable cybersecurity plans that adequately protect all operations of their DSRC system. The purpose of this Petition for Rulemaking is to ask the Commission to establish rules necessary to minimize the risk and ensure that adequate protections are taken. While the track record of the auto industry (and NHTSA) to date do not inspire confidence, the recent GAO Report does indicate that some manufactuers are "more advanced in their plans" than others.

To ensure that licensees are adequately aware of the threat, and taking appropriate steps to protect the public, the Commission should require every licensee[61] to submit a cybersecurity and privacy plan prior to deploying and activating DSRC units. This will force DSRC licensees

to consider the potential threats to their systems and develop plans for updating their security when new vulnerabilities are discovered. Additionally, it will provide a means by which the Commission can hold DSRC licensees accountable if they fail to follow their submitted plan.

B. The Commission should model data breach and privacy rules on the highly successful model adopted in the 2007 Pre-Texting Order

The CPNI Rules adopted by the Commission in 2007 have provided subscribers to telephone and VOIP services with significant protections. Granted, DSRC is not a Title II service, nor would the Commission's CPNI regulations[62] precisely fit the information that DSRC licensees contemplate collecting.

Nevertheless, the CPNI rules provide a good model for the Commission to adopt. In particular, DSRC licensees that collect personal information should be required to provide notice to purchasers of DSRC-equipped automobiles regarding the nature of the information collected, how the DSRC licensee intends to use the information, obtain affirmative consent from the purchaser before using the information for purposes other than those related to life and safety.

Additionally, if DSRC licensees store information collected from drivers and or passengers in DSRC-equipped cars, they must protect that information using technology that meets the generally expected standards for information storage and protection. In the event of a data breech, DSRC licensees should be obligated to notify law enforcement and the Commission, and then notify individuals potentially impacted by the breach.

---

[61] "Licensee" refers to any entity holding a license under Part 90 of the Commissions rules, 47 C.F.R. §§ 90.371 *et seq.*, or who is responsible for the manufacture and deployment of any device authorized and deployed under the license rule regulations at 47 C.F.R. §§ 95.1501 *et seq.*

[62] 47 CFR §§ 64.2001 *et seq.*

C. DSRC licensees must have an obligation to continually upgrade their systems to protect against cyberattacks

As the Commission has recently recognized with regard to mobile services, it is vitally important to ensure that consumers receive timely security updates when vulnerabilities are discovered.[63] As part of the obligations of DSRC licensees, the Commission should impose on DSRC licensees a continuing obligation to update their systems as new vulnerabilities are discovered. This is particularly critical in the case of DSRC, as many consumers own their cars for 10 years or more. As the GAO report acknowledged, industry stakeholders are in agreement on the importance of maintaining constant vigilance and providing timely security upgrades.[64]

VIII. CONCLUSION

Since the National Broadband Plan in 2010, the Commission has increasingly recognized the importance of imposing cybersecurity protections and privacy protections in every service it authorizes. Nowhere is this more important than DSRC. If NHTSA adopts its proposed mandate, DSRC will provide a potential vulnerability to millions of cars – creating an irresistible target for terrorist and other bad actors.

WHEREFORE, the Commission should adopt the rules proposed in this Petition.

Respectfully Submitted,

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

/s/ Harold Feld
Senior Vice President
Public Knowledge
1818 N St. NW, Suite 410
Washington, D.C. 20036
(202) 861-0020

June 28, 2016

[63] *See* FCC News Release, *FCC Wireless Telecommunications Bureau Launches Inquiry Into Mobile Device Security Updates* (2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-339256A1.pdf.
[64] *See* GAO Report at 21-22.