"Playing With Fire" An Inter-Agency Working Group Proposal for Connected Vehicle Technology and the DSRC Mandate

Christopher Kolezynski*

INTRODUCTION

The windshield wipers ran and the radio blared as Ben Makuch frantically and unsuccessfully tried to turn down the music. Things would only get worse. Soon, Ben Makuch lost control of the steering, braking, and eventually the transmission while driving a 2014 Jeep Cherokee. Security researchers, Chris Valasek and former NSA hacker, Dr. Charlie Miller engineered the hack. During the interview, Makuch asked Miller "Is there ever a scenario where you think a hacker could get access to a vulnerability in a car…just like this…[causing] a million cars t[o] just turn off? To which Miller shrugged and nonchalantly responded, "I could of done that….I could have made all the transmissions go to neutral for a million cars."[1]

* *Christopher Kolezynski, J.D.* from the Cleveland-Marshall College of Law, May 2018; B.A., Cleveland State University, 2014. Special to thanks to my mother, Marcia Kolezynski, my father, Gary Kolezynski, my sister, Jennifer Kolezynski, and my great aunt Eileen May, for their unconditional support. Further thanks to dear friend, Stephen Vano, who inspired the path I have chosen.

[1] *CYBERWAR: The Zero Day Market*, (Vice Productions Inc. 2016) (Miller was never paid for his work. Although one year later Chrysler changed policy and began a company bounty program paying researchers who found vulnerabilities in their cars. They were the first major American car company to do so).

Miller reported this vulnerability to Chrysler who took 9 months to work on the problem before Miller, in fear for the safety of millions, decided to go public. Chrysler fixed the vulnerability one week later.[2] There are two important lessons to learn from this story: (1) connected vehicles will materially increase the level of risk on the roads; (2) and some companies may not promptly address these risks.

The vulnerability exposed by Miller would have allowed the remote disabling of millions of transmissions because of the Uconnect head unit, a connected vehicle technology, connecting Jeep Cherokees and other vehicles. These head units are installed in Chrysler, Dodge, Jeep, Fiat, and Ram vehicles and provide features such as remote engine start and vehicle unlock from the user's phone as well as in car streaming services, GPS navigation and app sharing. The two security researchers who conducted the study also concluded "the[ir] attack on the entertainment system seem[ed] to work on any Chrysler vehicle with Uconnect from late 2013, all of 2014, and early 2015. [Although] [t]hey've only tested their full set of physical hacks…on a Jeep Cherokee…they believe…most of their attacks could be tweaked to work on any Chrysler vehicle with the vulnerable Uconnect head unit."[3] Jeep and Chrysler are not alone. Some of the most popular vehicles on the road, such as the Toyota Prius and 2014 Ford Fusion, could also

---

[2] *Id.* (Miller explains "car companies are so new to this. Most car companies, you don't even know who you would contact to tell them you found a vulnerability.").

[3] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway With Me In It*, WIRED (July 7, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (last visited Jan 31, 2018).

be subject to these types of hacks.[4] Other hacks have taken advantage of popular connected vehicle technologies, such as Onstar. The Onstar hack allowed remote disabling of the brakes among other attacks and took 5 years to fix.[5] Other

[4] Victoria Woollaston, *The 20 Most Hackable CARS Revealed: Report Lists the Smart Vehicles That Are Most at Risk of Having Their Systems Hijacked*, DAILY MAIL (August 8, 2016), http://www.dailymail.co.uk/sciencetech/article-2719866/The-20-hackable-CARS-revealed-Report-lists-smart-vehicles-risk-having-systems-hijacked.html#ixzz4LNTrEGFG (last visited Jan 31, 2018) (*citing*, Charlie Miller & Chris Valasek, *A Survey of Remote Automotive Attack Surfaces*, Black Hat Security Conference in Las Vegas 2014) (These vehicles include; the Cadillac Escalade, Ford Fusion, Dodge Ram 3500, BMW X3, Chrysler 300, Range Rover Evoque, Toyota Prius, Toyota Prius, Infiniti Q50, Audi A8, Infiniti G37, BMW3 Series, BMW i12Dodge Viper, and the Honda Accord LX.In 2013, Chris Valasek and Charlie Miller hacked a 2010 Toyota Prius and changed speedometer readings resulting in triggering of the cars collision protection features, disabled braking, and controlled the horn on the vehicle.). *See* also Babb, P., *Video: Watch what happens when a Prius gets hacked*, InfoWorld (Aug. 7, 2013), https://www.infoworld.com/article/2611599/hacking/video--watch-what-happens-when-a-prius-gets-hacked.html (last visited Jan 31, 2018). *See also* Jonathan Vanian, *Security Experts Hack Cars*, Fortune (January 26, 2016), http://fortune.com/2016/01/26/security-experts-hack-cars/ (last visited Jan 31, 2018)*See also* Rob Crilly, *Thousands of cars vulnerable to keyless theft, according to researchers*, The Telegraph (August 8, 2015) https://www.telegraph.co.uk/news/uknews/11808814/Thousands-of-cars-vulnerable-to-keyless-theft-according-to-researchers.html (last visited Feb 4, 2018) (The following vehicles have had their keyless entry hacked allowing for easy theft of the vehicle without enabling the alarm. Audi A3, A4, and A6, BMW 730d, Citreon DS4 Crossback, Ford Galaxy, Ford Eco-Sport, Honda HR-V, Hyundai Santa Fe, Kia Optima, Lexus RX 450, Range Rover Evoque, Renault Traffic, Mazda CX-5, MINI Clubman, Mitsubishi Outlander, Nissan Qashqai +2, Nissan Leaf, Opel Ampera, SsangYong Tivoli XDi, Subaru Levorg, Toyota RAV 4, VW Golf 7 GTD, VW Touran 5T.)

[5] A. Greenberg, *GM Took 5 Years to Fix a Full-Takeover Hack in*

cars that have been hacked include the Mitsubishi Outlander Hybrid,[6] Tesla Model S,[7] and the 2009 Chevy Impala, which was the test vehicle for the Onstar hack.[8]

Millions of Onstar Cars, WIRED (September 10, 2015), https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars (last visited Jan 31, 2018).

[6] Nellie Bowels, *Yet another car can be hacked – this time it's the Mitsubishi Outlander Hybrid*, THE GUARDIAN (June 26, 2016), https://www.theguardian.com/technology/2016/jun/06/mitsubishi-outlander-car-hacked-security (last visited Jan 31, 2018).

[7] Andrea Peterson, *Researchers Remotely Hack Tesla Model S*, THE WASHINGTON POST (September 20, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s (last visited Jan 31, 2018).

[8] Bowels, *supra* note 6 (It took 5 years for GM to fix this particular vulnerability!); *See also* Giles, M., *Thanks To This Device, Stealing Your Car Has Never Been Easier*, POPULAR SCIENCE (August 6, 2015), http://www.popsci.com/thanks-device-stealing-your-car-has-never-been-easier?con=TrueAnthem&dom=fb&src=SOC&utm_campaign=&utm_content=588e19b8f6d7a10006969bd2&utm_medium=&utm_source (last visited Jan 31, 2018).

> "Samy Kamkar is a car buff. The cyber security expert enjoys tinkering, particularly in the intersection of automation and the Internet of Things. "I love the new technology that car companies are introducing," he says, "but I worry whether the manufacturers are actually paying attention to the security of these connected vehicles." That's why, last week, he unveiled a recent four-wheel hack of a friend's Chevy Volt, cracking the OnStar, which is owned by General Motors, through a device he built called OwnStar."
> *Id.*

The advancement of connected vehicle technology brings with it new risks. One potentially catastrophic risk would be for millions of cars to be remotely hijacked, leading to a disaster approaching the scale of the September 11 attacks.[9] While such a scenario is hopefully remote, it remains a possibility because of a proposed mandate of Vehicle-to-Vehicle technology by the National Highway Traffic and Safety Administration ("NHTSA").[10] NHTSA proposed in 2014 to mandate the use of Dedicated Short Range Communication ("DSRC") devices in all new light vehicles.[11]

These DSRC devices are a connected vehicle technology, utilizing the 5.9 GHz bandwidth, allowing vehicles to transmit Basic Safety Messages between each other. This information includes messaging about road conditions and nearby vehicles. Never before have vehicles been connected on such a wide scale.

"[T]he one thing that has prevented cyberterrorists from…infecting thousands of cars with malware designed to crash them…has been the inability of cars to communicate with each other…You can do it on a one-car basis. You can't yet do it on a 100,000-car basis."[12] On March 17, 2016, the

---

[9] Kohler & Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 Santa Clara High Tech. L.J. 99, 133 (2015).

[10] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 161 (proposed Aug. 20,2014) (to be codified at 49 C.F.R. pt. 571).

[11] *Id.*; *See also* Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 82 Fed. Reg., 3860 (proposed Jan. 12, 2017) (explaining, "[l]ight vehicles include passenger cars, vans, minivans, sport utility vehicles, crossover utility vehicles and light pickup trucks with a gross vehicle weight rating less than or equal to 10,000 pounds.").

[12] Open Technology Institute & Public Knowledge, *Petition for*

Federal Bureau of Investigation ("FBI") released a public announcement warning "the general public and manufacturers…to maintain awareness of…cybersecurity threats related to connected vehicle technologies[13] The FBI explained, "[m]odern motor vehicles often include new connected vehicle technologies that aim to provide…added safety features…[and] [a]ftermarket devices are also providing consumers with new features to monitor the status of their vehicles….[However, because of] this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats."[14] In an example case discussed in the announcement, NHTSA had to recall over one million vehicles as a result of the discovery of multiple remote exploits.[15]

As an effect of the DSRC mandate, the Federal Communications Commission ("FCC") was petitioned to issue a stay on operation of the connected vehicle technology. The requested emergency stay would work by not allowing operation of DSRC devices in the 5.9ghz bandwidth, which falls under FCC jurisdiction.[16] The petition explains, "[t]he DSRC service lacks rules to protect

---

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), iv-v (June 28, 2016).

[13] FBI, *Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits*, (March 17, 2016), https://www.ic3.gov/media/2016/160317.aspx (last visited Jan 31, 2018).

[14] *Id.*

[15] *Id.*

[16] Open Technology Institute & Public Knowledge, *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)* (June 28, 2016).

user privacy or to protect DSRC units from malware or other forms of cybersecurity attacks." The FCC took notice of this petition and opened the issue for public comment on July 25, 2016.[17]

The problem this inevitably creates is one of agency jurisdiction. NHTSA asserted in their 2014 Advanced Notice of Proposed Rulemaking that "the agency was confident its existing legal authority would cover [V2V Technologies]."[18] However, the FCC has jurisdiction over "wire and radio,"[19] specifically the 5.9 GHz band utilized by DSRC devices. Even more complicating, the Federal Trade Commission has jurisdiction over "unfair and deceptive trade practices [including data security] in or affecting commerce"[20] and NHTSA has jurisdiction over the motor vehicle equipment[21] that creates this data. Therefore, the vehicles themselves, their component technologies, and the data they create could be subject to FTC, FCC, and NHTSA regulations.

This evolving presence of connected vehicle technology will inevitably lead to potential jurisdictional hurdles, duplicative, potentially inconsistent regulations, and endangered consumers. As more capabilities, connectivity, and features are added the attack surface will widen[22] and the amount of vulnerabilities will increase. On

---

[17] Lydia Beyoud, *FCC Studying Cybersecurity of Connected Vehicle Tech*, BLOOMBERG BNA (July 27, 2016), http://www.bna.com/fcc-studying-cybersecurity-n73014445537 (last visited Jan 31, 2018).
[18] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 161 (proposed Aug. 20,2014) (to be codified at 49 C.F.R. pt. 571).
[19] 47 U.S.C. § 151 (2017).
[20] 15 U.S.C § 45(a) (2012).
[21] 49 U.S.C. § 30101 (2013).
[22] Greg Rogers, *NHTSA's Proposed Rule Requires Cars to Talk to Each Other*, Eno Transportation Weekly (Dec. 16, 2016),

the bright side, connected vehicle technologies, specifically the current DSRC mandate, presents an opportunity to promote a collaborative regulatory approach through an inter-agency working group.

The remainder of this article will be divided into four (4) parts. First, the history of DSRC rulemaking, including discussion of the security and privacy risks associated with connected vehicle technology, and the security and privacy risks specific to the current Notice of Proposed Rulemaking will be explored. Second, I will propose an Inter-Agency Working Group composed of the FCC, FTC, and NHTSA to build upon the current rulemaking. In doing so, I will explore the history of Inter-Agency Working Groups in relation to emerging technologies, the benefits of joint policymaking and explain the benefits of involving FTC and FCC expertise in the rulemaking process. Third, I will review agency jurisdiction and review how it applies to DSRC. Finally, I will conclude the best approach to the problem is the development of an Inter-Agency Working Group, including the FTC, FCC, and NHTSA because as it stands, vehicles equipped under current DSRC rules, would simply be "*Unsafe at Any Speed*."[23]

---

https://www.enotrans.org/article/nhtsas-proposed-rule-requires-cars-talk (last visited Jan 31, 2018) (explaining "[f]or each node that is added to a network, there is a new set of vulnerabilities. Deploying hundreds of thousands, and eventually millions, of vehicles that are connected to a single communications network creates a slew of vulnerabilities.").

[23] RALPH NADER, UNSAFE AT ANY SPEED: THE DESIGNED-IN DANGERS OF THE AMERICAN AUTOMOBILE, (1965).

I. DSRC RULEMAKING: SECURITY AND PRIVACY RISKS

A. History

In August 2014, NHTSA issued an Advanced Notice of Proposed Rulemaking for mandating DSRC devices in all new light cars.[24] After collecting 926 comments, some of which focused on the danger of such a network being hacked,[25] NHTSA submitted a Notice for Proposed Rulemaking to the Office of Management and Budget in January 2016.[26] The Notice for Proposed Rulemaking was issued in December 2016.[27] The summary explains, "This rulemaking would require that all light vehicles be capable of V2V communication by use of on-board dedicated short-range radio communication (DSRC) devices, which would broadcast messages about a vehicle's speed, heading, brake status, and other information to other vehicles and receive the same information from the messages with extended range and ´line-of-sight´ capabilities."[28] NHTSA explained in a Press Release following the Notice of the Proposed Rule that the goal of the technology is to prevent "hundreds of thousands of crashes."[29] In support of this claim, NHTSA

---

[24] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 161 (proposed Aug. 20, 2014) (to be codified at 49 C.F.R. pt. 571).
[25] *Id.* at https://www.regulations.gov/document?D=NHTSA-2014-0022-0002.
[26] Federal Motor Vehicle Safety Standards 150 - Vehicle-to-Vehicle (V2V) Communication, 79 Fed. Reg. 161 (proposed January 12, 2016) (to be codified at 49 C.F.R. 571.150).
[27] Federal Motor Vehicle Safety Standards; V2V Communications, 49 CFR Part 571 (proposed Dec. 13 2016) (to be codified at 49 CFR pt. 571).
[28] *Id*. at https://www.regulations.gov/docket?D=NHTSA-2016-0126.
[29] *U.S. DOT advances deployment of Connected Vehicle Technology to*

states that "V2V communications can detect developing threat situations hundreds of yards away, and often in situations in which the driver and on-board sensors alone cannot detect the threat."[30] The technology works by "requiring V2V devices to "speak the same language" through standardized messaging."[31] The most recent Notice of Proposed Rulemaking has received 463 comments and the public comment period ends on April 12, 2017.[32]

The cybersecurity concerns about implementing this technology can be categorized into two broad categories: security and privacy.

B. Security Risks and Increasing the Attack Surface

Security concerns arise from the technologies used to connect vehicles. For example, one report from a leading security company suggests there may be fourteen (14) different ways a hacker could gain access to a car's operating system alone.[33] Other possibilities exist too, as one

---

prevent hundreds of thousands of crashes, (2016), https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands (last visited Dec. 28, 2017).

[30] *Id.*

[31] *Id.*

[32] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017), available at https://www.regulations.gov/docket?D=NHTSA-2016-0126.

[33] Open Technology Institute & Public Knowledge, *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*), iv (June 28, 2016) (*citing*, Intel, *Automotive Security Best Practices: Recommendations for security and privacy in the era of the next generation car (2015)* ("Intel Whitepaper"), available at

overarching concern of any new technology is its expansion of the attack surface, which, in the case of connected cars, would be significant in light of the component technologies involved.

The FBI and DOT acknowledged this possibility noting in a Public Service Announcement that cars are becoming increasingly more vulnerable through "remote exploits."[34] Despite these warnings, NHTSA continues to push DSRC technology forward.[35] The State Department of Transportation of California ("CALTRANS") identified one such example: "the DSRC system is designed to use predetermined message structures to identify current highway and vehicle conditions. These message structures do not include the ability to install malware … from one car to another."[36]

---

http://www.intel.com/content/www/us/en/automotive/automotive-security-best-practices-white-paper.html (last visited Jan 31, 2018).

[34] *Id.*; *See also* Senator Ed Markey, *Tracking & Hacking: Security and Privacy Risks Put American Drivers at Risk*,(Feb. 2015), available at http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport- Tracking_Hacking_CarSecurity%202.pdf. (The 2015 Markey Report found that "[m]ost automobile manufacturers were unaware of or unable to report on past hacking incidents. Security measures to prevent remote access to vehicle electronics [wer]e inconsistent and haphazard across all auto manufacturers…[and] [o]nly two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.").

[35] Senator Ed Markey, *Tracking & Hacking: Security and Privacy Risks Put American Drivers at Risk* (Feb. 2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport- Tracking_Hacking_CarSecurity%202.pdf. (last visited Jan 31, 2018).

[36] Comments of the State of California Department of Transportation, *In the Matter of Open Technology Institute & Public Knowledge,*

Malware is data or computer code just like any other software. It does not identify itself as malware, unless assigned a signature by antivirus companies or is otherwise detectable, and is often injected into pdf or word documents as seen in phishing attacks via email. Furthermore, much malware is designed to be covert. This can be done through encryption and other methodologies. Zero-day exploits are by definition undetectable because no one is aware that the vulnerabilities they exploit even exist.[37] Some of the covert qualities found in worms, a type of malware, include polymorphic or metamorphic features.[38] Every new copy made of a polymorphic worm, is done so using slightly modified code. Metamorphic worms can rewrite their own code and change their behavior. Both of these serve to hide detection.[39]

Certainly, one could design malware to emulate the predetermined message structures used to communicate with other vehicles. Furthermore, radio, specifically the 900 MHz band, has already been used to transmit data while the adversary remains nearly undetectable.[40] One example specific to DSRC is the delay of Basic Safety Messages caused by harmful interference. The Alliance of Automobile Manufacturers and Association of Automobile

---

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), 9 (August 19, 2016).

[37] WILLAM STALLINGS & LAWRIE BROWN, COMPUTER SECURITY PRINCIPLES AND PRACTICE, 216 (3d. 2015).

[38] *Id*.

[39] *Id*.

[40] Lucia Constantin, *Hackers show off long-distance Wi-Fi radio proxy at DEF CON*, PC WORLD (August 10, 2015), http://www.pcworld.com/article/2968232/security/hackers-show-off-longdistance-wifi-radio-proxy-at-def-con.html (last visited Jan 31, 2018).

Manufacturers wrote to the FCC in 2013 about their concerns regarding harmful interference caused by U-NII-3 and U-NII-4 devices.[41] When one company was asked about cybersecurity protections for DSRC units, they responded "[w]hat's being exchanged between vehicles is just data . . . There's no possibility of a virus being spread between cars.'" However, all information exchanged through a computer network is ""just data" – viruses included….[and] [c]ybercriminals and terrorists…will use this attack vector…exchanging "just data" to potentially devastating effect."[42] The United States Government Accountability Office ("GAO") report on Vehicle-to-Vehicle technologies states that "[o]f the 21 experts…interviewed, 12 cited the technical development of a V2V communication security system as a great or very great challenge to the deployment of V2V technologies."[43]

Moreover, due to the projected growth of connectivity among cars, there is a strong likelihood attackers will focus on obtaining financial gain through hacking vehicles. This may be achieved in several different ways: remote unlocking and theft of vehicles, ransoming control of the vehicle until receipt of payment through untraceable bitcoin, accessing data located on driver's cell

---

[41] The Alliance of Automobile Manufacturers and Association of Automobile Manufacturers *5.9 GHz DSRC Connected Vehicles for Intelligent Transportation Systems*, (Sep. 13, 2013) https://ecfsapi.fcc.gov/file/7520943378.pdf.

[42] Comments of Public Knowledge et al., *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)*, 3 (August 24, 2016).

[43] US Gov't Accountability Off., Intelligent Transportation Systems: Vehicle to Vehicle Technologies Offer Safety Benefits but a Variety of Deployment Challenges Exist GAO-14-13, at 21 (2013).

phones through USB ports in the vehicle, or listening to conversations inside a vehicle via Bluetooth connectivity.[44]

C. Privacy Risks

Privacy concerns are raised by the transmission of data between cars, the type of data gathered, where that data is stored, and how it is used. In order to protect data in transmission, especially personal identification information, data will "need to be robustly anonymized, strongly encrypted, and securely protected to avoid being vulnerable."[45] Auto manufacturers who sell their vehicles in other countries, such as Europe, may have to meet even more stringent standards regarding the data created by connected vehicle technology. One threat presented by connected vehicle data is that "information…can be correlated with other information…., including the location where the vehicle is regularly parked overnight, … to profile the likely user…and to predict the user's actions."[46]

The Markey Report, published by Senator Edward Markey in 2015, was developed by surveying 16 major automobile manufacturers regarding the cybersecurity and privacy protections of connected vehicle technologies. The Report found that the majority of auto manufacturers offered technology features that gathered and sent data to a data center, sometimes run by a third party.[47] Most of these

---

[44] Burke Katie, *What do car hackers really want? Security threats are mostly about money*, AUTOMOTIVENEWS (October17,2016) http://www.autonews.com/article/20161017/OEM06/310179880/what-do-car-hackers-really-want (last visited Jan 31, 2018).

[45] Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 Santa Clara L. Rev. 1171, 1205 (2012).

[46] *Id.* at 1196.

[47] Markey, *supra*, *Tracking & Hacking: Security and Privacy Risks Put*

manufacturers could not describe measures that were in place to protect the data, although many utilized the data in a variety of ways.[48] Furthermore, "[c]ustomers [we]re often not explicitly made aware of data collection and, when they [we]re, they often cannot opt out without disabling valuable features, such as navigation."[49] Such poor data protection practices have already resulted in telecommunications companies being fined millions of dollars by the FCC.[50] One independent commentator has called for the NHTSA to conduct a more comprehensive analysis of these privacy concerns to ensure personally identifiable information is not collected without proper consent."[51]

American Drivers at Risk, (Feb 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (last visited Jan 31, 2018).

[48] *Id.*

[49] *Id*. (The SPY Car Act explicitly addresses the concern over loss of navigation features when opting out of data collection); *See supra* note 32.

[50] ENFORCEMENT BUREAU, *FCC Plans $10M Fine For Carriers That Breached Consumer Privacy*, FCC (Oct. 24, 2014), https://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy. *See also* Daniel J Solove & Paul M. Schwartz, *Privacy Law Fundamentals*, IAPP 2 (2011); Max Green, *15 of the biggest data breach settlements and HIPAA fines*, Becker's Health IT & CIO REVIEW (October 14, 2015), http://www.beckershospitalreview.com/healthcare-information-technology/15-of-the-biggest-data-breach-settlements-hipaa-fines.html; Aruna Viswanatha, *Morgan Stanley Fined 1 Million for Client Data Breach*, THE WALL ST. JOURNAL (June 8, 2016) (As the above articles illustrate, failure to account for attacks and subsequent data breaches could just as easily lead to massive liability for auto companies through privacy based tort actions or general negligence), http://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374.

[51] Comments of the Electronic Privacy Information Center, Federal

As a result of the growing concern for privacy issues related to vehicle created data, other efforts to protect the public have also been proposed. Senators Ed Markey and Richard Blumenthal introduced the Security and Privacy in Your Car Act ("SPY Car Act") to the Senate on July 21, 2015. The SPY Car Act would require the NHTSA to issue regulations that would require vehicles with accessible data or control signals to be capable of detecting, reporting, and stopping attempts to intercept such driving data or [attempt to] control the vehicle."[52] Further, The SPY Car Act would require the Federal Trade Commission to: "(1) require motor vehicles to notify owners or lessees about the collection, transmission, retention, and use of driving data; (2) provide owners or lessees with the option to terminate such data collection and retention…without losing navigation tools…and (3) prohibit manufacturers from using collected information for advertising or marketing purposes without the owner's or lessee's consent." The SPY Car Act takes note of not only security concerns but also addresses concerns over consumer privacy.

Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 161 (comment sent October 20, 2014) (to be codified at 49. C.F.R. 571) ("NHTSA should complete a more detailed privacy and security assessment of V2V communications. Additionally, NHTSA should: (1) not collect PII without the express, written authorization of the vehicle owner; (2) ensure that no data will be stored either locally or remotely; (3) require end-to-end encryption of V2V communications, including the basic safety messages ("BSMs"); (4) require end-to-end anonymity; and (5) require auto manufacturers to adhere to the Consumer Privacy Bill of Rights.").

[52] Security and Privacy in Your Car Act, S. 1806, 114th Cong. (2015).

D. V2V NPRM Security Measures and Concerns

The messaging employed in NHTSA's proposed mandate would have a range around 300 meters.[53] The NPRM proposes to mandate DSRC technology during the manufacturing stage, but also leaves open the possibility of aftermarket installations or the use of handheld devices. The NPRM explains that having these options is integral to reaching "optimal safety benefits of a [vehicle to vehicle] cooperative safety network."[54] However, the inclusion of aftermarket products or handheld devices could introduce additional vulnerabilities.[55] Furthermore, the NPRM refers to two possible future applications of the vehicle to vehicle ("V2V") communication system: "Intersection Movement Assist [and] Left Turn Assist."[56] While both of these

---

[53] Cahill, Kohler & Laurenza, *NHTSA Issues Proposed V2V Crash Avoidance Technology Rule*, LEXOLOGY (Dec. 19,2016), available at http://www.lexology.com/library/detail.aspx?g=22cdefa8-99f2-4dd7-bcc2-caabd953346c.

[54] *Id.*

[55] NHTSA, Vehicle-to-Vehicle Communications: Readiness of V2V Technology for
Application, DOT HS 81214, 29 (August 2014), available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf. ("An aftermarket V2V communication device provides advisories and warnings to the driver of a vehicle similar to those provided by an OEM installed V2V device. These devices, however, may not be as fully integrated into the vehicle as an OEM device…For example, a "self-contained" V2V aftermarket safety device could only connect to a power source, and otherwise would operate independently…Aftermarket V2V devices can be added to a vehicle at a vehicle dealership, as well as by authorized dealers or installers of automotive equipment. Some aftermarket V2V devices (e.g., cell phones with apps) are portable and can be standalone units carried by the operator, the passenger, or pedestrians.").

[56] *Id.*

functions are still limited to providing warnings, there incorporation shows NHTSA's intention of providing for different and additional types of warnings as the V2V communication system progresses. The NPRM notes that V2V and Vehicle to Infrastructure communications are "warnings-only systems."[57] Yet, physical control of a vehicle might be possible if the attacker merely uses V2V to access other onboard computer systems such as the Uconnect head unit exploited by Charlie Miller or the vehicles electronic control unit.[58] For example, if V2V was used as a pathway to access the electronic control unit this might result in the ability to disable braking or the exploitation of other features employed by that electronic control unit. Although this is seemingly more frightening and equally difficult, the danger of vehicles communicating false information should be enough to raise a few eyebrows.

Despite all these risks, security and privacy have not been ignored by NHTSA. "As a networked system, V2V/V2I are intended to employ a secure and reliable communications network, allow only certified devices to access that network, and have a trusted entity (the Security Certificate Management System) to issue, distribute, and, when necessary, revoke device certificates."[59] However, digital certificate systems by and of themselves can contain vulnerabilities. Although Security Certificate Management Systems are slightly different because they deal with certifying devices rather than a user's identity, both share common features such as the reliance on Certificate Authorities. Furthermore, "[d]igital certificates have become one of the latest targets, especially with enterprises relying

[57] *Id.*
[58] *Supra* note 1.
[59] *Supra* note 47.

on certificates more than ever to keep system connections secure."[60]

One vulnerability is caused by the Certificate Authority or the company managing the certificates. Poor management of these certificates is a "primary vulnerability."[61] "The problem is that Certificate Authorities "CAs" can be compromised, as exemplified by incidents at certificate authorities such as DigiNotar, Comodo and DigiCert."[62] Even worse, "if an attacker can usurp control of a certificate, forge a certificate or compromise a certificate, all the benefits offered are made moot."[63] Furthermore, "[t]here are hundreds of CAs issuing digital trust worldwide and the average organization has over 23,000 keys and certificates, according to Ponemon Institute research. When a major CA is breached or when a CA fraudulently issues unauthorized certificates for an organization, attackers can impersonate, surveil and monitor their organizational targets, as well as decrypt traffic and impersonate websites, code or administrators."[64] "If the certificate private key is compromised, the entire PKI environment is compromised."[65]

---

[60] Frank OhlHorst,, *The Hidden Threats of Security Certificates*, BASELINE MAG. (Dec. 4 2012), http://www.baselinemag.com/security/the-hidden-threats-of-security-certificates (last accessed March 6, 2018).

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] Warwick Ashford, *Security pros failing to address digital certificate risks, survey shows*, COMPUTER WEEKLY (Sep. 9, 2015), http://www.computerweekly.com/news/4500253143/Security-pros-failing-to-address-digital-certificate-risks-survey-shows.

[65] Gemalto, *Latest Breaches Expose PKI's Greatest Weakness – Encryption Keys*, (Sep. 22, 2011), http://www.sentinelcloud.com/About/NewsMedia/PKIs-Greatest-

NHTSA touts that its V2V security system complies with NIST standards. However, compliance does not equate to security. A primary example of this was the Target data breach and subsequent theft of consumer information. [66] Target at the time of the breach was compliant with Payment Card Information security standards, yet their security was compromised through the HVAC system. [67] Furthermore, the MITRE Corporation already identified 21 "high-level threats" to the V2V security system in its 2015 technical report to the Department of Transportation.[68]

In a study on Cooperative Adaptive Cruise Control ("CACC") vehicle streams, which employ V2V communication, researchers identified several forms of possible attacks with varying effects on the vehicles in the stream. The researchers pointed to the insider vulnerability which could "cause significant instability in the CACC

Weakness–Encryption-Keys/ (last accessed March 6, 2018).

[66] *See generally* John P. Mello Jr., *Target Breach Lesson: PCI Compliance Isn't Enough*, TECH NEWS WORLD (Mar. 18, 2014), available athttp://www.technewsworld.com/story/80160.html; Aviva Litan., *How PCI failed Target and U.S. Consumers*, GARTNER (Jan. 20, 2014), http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/; Jaikumar Vijayan, *After Target, Neiman Marcus breaches, does PCI compliance mean anything?*, COMPUTER. WORLD (Jan. 24, 2014), http://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html.

[67] *Id.*

[68] MITRE Corporation, *Final Requirements Report*, Dept. of Transportation FHWA-JPO-15-235, ii (Sept. 11, 2015), https://www.regulations.gov/contentStreamer?documentId=NHTSA-2016-0126-0008&attachmentNumber=1&disposition=attachment&contentType=pdf.

vehicle stream."[69] Attacks discussed included "application layer, network layer, system level, and privacy leakage attacks."[70] The researchers explained "[a]ll these attacks can potentially impact the string stability of the system and compromise the safety and privacy of the passengers of the CACC vehicle stream. Such attacks can be launched either by an outsider or insider adversary."[71]

> "In the message falsification attack, the adversary starts listening to the wireless medium, and…manipulates the content…and rebroadcasts it… In the spoofing attack, the adversary impersonates another vehicle in the stream in order to inject fraudulent information into a specific vehicle….In a replay attack, the adversary receives and stores a beacon sent by a member of the stream and tries to replay it at a later point of time with malicious intent. The replayed beacon contains old information which can lead to hazardous effects…the adversary can attempt a Denial-of- Service…attack to overwhelm the communication capability of a vehicle or a group of vehicles, and make them unable to participate properly in a CACC vehicle stream. A known method…is by using a vehicular botnet. Radio jamming to deliberately disrupt communications over small or wide geographic areas…is another possible network layer DoS attack….Another type of attack is tampering with vehicle hardware or

[69] Mani Amoozadeh,et al., *Security Vulnerabilities of Connected Vehicles Streams and their Impact on Cooperative Driving*, 53 IEEE Communications Magazine 6 126, 126 (June 2015), http://ieeexplore.ieee.org/document/7120028/?reload=true.
[70] *Id.*
[71] *Id.* at 127.

> software…done by a malicious insider in the manufacturing level or by an outsider in an unattended vehicle (for instance by replacing or altering certain vehicle sensors). Even if the communication channel is secure, and a state-of-the-art security architecture is deployed…if the on-board hardware/software are tampered with or faulty, then the input information to the system will not be accurate."[72]

The study goes on to note the privacy implications of eavesdropping on the vehicle's CACC stream. "CACC vehicles periodically broadcast beacons that contain[] various information such as the vehicle identity, current vehicle position, speed, acceleration, etc. The availability of this information can compromise…privacy."[73] Such information as position, speed, and acceleration data falls under required data in NHTSA's NPRM. The chart below is from the above study and provides a visual understanding of the types of attacks that may be exercised on a vehicle communication stream such as DSRC.

[72] *Id.* at 127-128.
[73] *Id.* at 128.

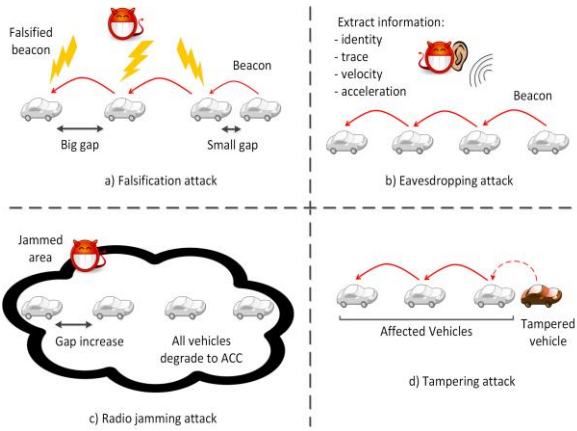

Fig. 2. Security attacks on a CACC vehicle stream.[74]

II. VEHICLE TO VEHICLE COMMUNICATIONS INTER-AGENCY WORKING GROUP

"This is what happens when you put one of every kind of scientist in a room [with] a laser junky."[75] Intellectual Venture Labs, funded by Bill Gates, developed a solution to fight malaria that identified mosquitoes which were prone to carry the disease and remove their wings using a targeted laser. This technology would be applied in a square formation surrounding a village or home, effectively creating a protective net around communities.[76] As

[74] *Id.* at 132.
[75] Pablos Holman, *Top Hacker Shows Us How it's Done*. TEDXMIDWEST (Aug. 30 2012), https://www.youtube.com/watch?v=hqKafI7Amd8. *See also*, *Photonic Fence*, INTELLECTUAL VENTURES, http://www.intellectualventures.com/inventions-patents/our-inventions/photonic-fence/ (last visited Jan. 30 2017).
[76] *Photonic Fence*, *supra* note 75.

Intellectual Venture Labs notes on their website approximately 600,000 people die annually from malaria.[77]

The development and application of this laser-based technology was no small feat.[78] It was primarily successful due to the collaboration of scientists from many different fields. This notion of collaboration breeding innovation applies with equal force to the challenges and opportunities presented by connected cars.

A. Emerging Technologies and Interagency Working Groups

Some have already advocated for new authorities to "aid the safe deployment of new technologies,"[79] and inter-agency working groups have been utilized to address scenarios like those presented by connected cars. For example, one was formed to address differing aspects of drone policy, including the domestic use of unmanned aerial systems by federal law enforcement [80] and the prohibited use

---

[77] *Id.*

[78] Holman, *supra* note 75.

[79] Press Release, Rep. Dan Lipinski, D., Rep. Lipinski Reacts to DOT Autonomous Car Recommendations (Sep. 20, 2016) (https://lipinski.house.gov/press-releases/rep-lipinski-reacts-to-dot-autonomous-car-recommendations/). *See also* NHTSA, FEDERAL AUTOMATED VEHICLES POLICY, (Sep. 2016), https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.

[80] DEPT. OF JUST. POL'Y GUIDANCE, DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS, https://www.justice.gov/file/441266/download.

> The Department's working group was led by the Office of Legal Policy and included the Department's Chief Privacy and Civil Liberties Officer and representatives of the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Criminal Division, the

of drones during wildfires.[81] Another was formed under the Department of Justice to study the department's own domestic use of drones. Ultimately, the working groups resulted in policy guidance that set forth principles to protect privacy and civil rights stemming from the use of drones.[82]

Many other examples of successful working groups exist, with goals including the improvement of drone policy and Internet of Things technologies, of which connected cars are a part. The 2015 White House Presidential Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems was a result

---

> Office of Community Oriented Policing, the Civil Rights Division, the Office of the Deputy Attorney General, the Drug Enforcement Administration, the Federal Bureau of Investigation, the National Security Division, the Executive Office for United States Attorneys, the Office of Justice Programs, the Office of Privacy and Civil Liberties, the United States Marshals Service, and the Office of the Chief Information Officer.
> *Id.*

[81] The Editor, *Federal Agencies Working Together to Combat Unauthorized Drone Use During Wildfire Operations*, UAS VISION (June 14, 2016), http://www.uasvision.com/2016/06/14/federal-agencies-working-together-to-combat-unauthorized-drone-use-during-wildfire-operations/ (explaining "the National Wildfire Coordinating Group, an interagency body of senior fire officials from federal and state wildland fire management organizations, established improved drone incursion notification protocols for wildland firefighters.").

[82] *2015 White House Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, (Feb. 2015), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

of federal interagency collaboration.[83] The Inter-Agency Working Group on Facilities and Infrastructure also formed a Task Force on Unmanned Systems which advised the group on policy and plans related to the use of "Autonomous Underwater Vehicles (AUV), Gliders, Unmanned Aircraft Systems (UAS), Unmanned Surface Vessels (USV) and Lagrangian Platforms."[84]

Another example is the Networking and Information Technology Research and Development Program which consists of several interagency working groups that address research in emerging areas such as the Internet of Things.[85] The Program includes more than a dozen working groups covering research in program areas including:

> "Big Data, Cyber Physical Systems, Cyber Security and Information Assurance, Human

---

[83] *Id. See also* Allyn K. Milojevich, *Proliferation of Unmanned Aerial Systems (Drones) and Policy Challenges on the Horizon: A Policy Memorandum to John P. Holdren*, 8 J. OF SCIENCE, POLICY, AND GOVERNANCE 1 (Feb. 2016) http://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/milojevich_proliferationofdrones.pdf (proposing an interagency working group to develop a comprehensive framework for drone policy). *See also, Lisa Ellman, '05: Polivation Expert Leads at White House and in Drone Policy*, UNIVERSITY OF CHICAGO LAW SCHOOL (Apr. 5 2016), https://www.law.uchicago.edu/news/lisa-ellman-05-polivation-expert-leads-white-house-and-drone-policy (involvement in federal interagency working group on drone policy).

[84] *Interagency Working Group on Facilities and Infrastructure (IWG-FI)*, NAT'L OCEANOGRAPHIC PARTNERSHIP PROGRAM, http://www.nopp.org/about-nopp/committees/iwg-fi/ (last visited Jan. 7, 2017).

[85] Bruce, Correa & Subramanyam, *Internet of Things: Examining Opportunities and Challenges*, WHITE HOUSE BLOG (Aug. 30, 2016), https://www.whitehouse.gov/blog/2016/08/30/internet-things-examining-opportunities-and-challenges.

> Computer Interaction and Information Management, High Confidence Software and Systems, Health Information Technology Research and Development, High End Computing, Large Scale Networking, Joint Engineering Team, Middleware And Grid Interagency Coordination Team, Privacy Research & Development, Robotics and Intelligent Systems, Social Computing, Software Productivity, Sustainability, and Quality, Video and Image Analytics, Wireless Spectrum Research and Development."[86]

The National Institute of Standards and Technology also formed an Inter-Agency Working group to address the growth and expansion of the Internet of Things.[87]

When established, many working groups seek input and collaboration from a variety of sources, including other regulatory agencies. Not only have Inter-Agency Working Groups been formed to address these emerging technologies but the FCC has already collaborated with the Department of Transportation previously to address problems caused by emerging technologies. The Agencies previously collaborated on an issue caused by the increase in consumer cell phones and subsequent use of these devices on aircraft. The Agencies sought to continue the "safe and secure use of

---

[86] *NITRD Coordination Areas*, NETWORKING AND INFO. TECH. RESEARCH AND DEV. PROGRAM, https://www.nitrd.gov/nitrdgroups/index.php?title=Subcommittee_on_Networking_and_Information_Technology_Research_and_Development_(NITRD_Subcommittee) (last visited Jan. 7, 2017).

[87] *CPS Public Working Group*, NIST, https://pages.nist.gov/cpspwg/ (last visited January 7, 2017). *See also* Bruce, Correa & Subramanyam, supra note 85.

consumer communications technology onboard domestic commercial aircraft."[88]

Each working group is uniquely created and has a unique purpose; however, all successful collaborations share certain commonalities. Several characteristics in particular have been identified as indicia of future success.

These approaches included "defining outcomes, measuring performance, and ensuring accountability, establishing leadership approaches, [and] using resources such as funding, staff, and technology" in overcoming collaborative challenges.[89] One key aspect of "defining outcomes" is to "start a group" that includes "the most directly affected participants" and "gradually broaden th[is] group to include other[]" affected or interested parties. When it comes to connected vehicle technology the most directly affected federal agencies include NHTSA, the FCC, and the FTC.[90]

If applied to connected cars, a working group comprised of the key federal stakeholders – including, for example, the FTC, FCC, and NHTSA – could not only address the privacy and security implications of connected vehicle technology, but also resolve the ambiguity presented by overlapping regulatory jurisdictions.[91]

---

[88] FCC, *FCC Announces Agreement with the U.S. Department of Transportation Establishing a Framework for Coordination of Aviation Communications Safety and Security Issues*, (Jan. 29, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-110A1_Rcd.pdf.

[89] Veal et al., *Practical Approaches for Implementing Successful Collaborative Groups*, THE PUBLIC MANAGER (Sept. 15, 2014), https://www.td.org/Publications/Magazines/The-Public-Manager/Archives/2014/Fall/Practical-Approaches-for-Implementing-Successful-Collaborative-Groups.

[90] The FTC, NHTSA, and the FCC are the most directly affected parties based upon their jurisdiction and regulatory missions.

[91] Turrecha, Pulliam & Bruno, *FTC Drives Autonomous Car Reg*

B. Joint Policymaking by the FTC, FCC, and NHTSA

President Obama once joked "[t]he Interior Department is in charge of salmon while they're in freshwater, but the Commerce Department handles them when they're in saltwater. I hear it gets even more complicated once they're smoked." [92] Joint rulemaking provides a solution to this issue of overlapping jurisdiction and involves varying techniques from "following model rules" to the use of "interlocking" and "parallel" rules" and the "adoption of another agency's rules as reference." [93] However, "the best example[s] of such an instrument is joint rulemaking, which typically involves two or more agencies agreeing to adopt a single regulatory preamble and text." [94]

> "Agencies appear to use joint rulemaking on an ad hoc basis to promote uniformity primarily where they perform closely related regulatory missions and where Congress has allocated each of them a role implementing one or a set of related statutes…in certain cases, the agencies jointly promulgating rules do not generally work

Toward Privacy and Security, LEXOLOGY (Nov. 23 2016), http://www.lexology.com/library/detail.aspx?g=f3686e39-1e13-42fd-9ff0-2afa2e5a119e ("The constant slew of innovations and advancements in smart cars has so far left regulators struggling to define new rules to govern this space. The overlapping jurisdictions of three different agencies - …NHTSA, the…FTC, and the…FCC) – with different priorities have only added to the complexity.").

[92] Freeman & Rossi, *Improving Interagency Coordination in Shared Regulatory Space*, 38 ADMIN. & REG. L. NEWS 11, 11 (2013).

[93] Freeman & Rossi, *Agency Coordination in Shared Regulatory Space*, 125HARV. L. REV. 1131, 1165-66 (Mar. 2012).

[94] *Id*. at 1166-67.

> on related issues, yet they share an interest in implementing one particular law."[95]

Such joint rulemaking efforts, although accounting for a minimal amount of total annual rules,[96] have been successful in the past [97] and address the current context most appropriately. The FTC, NHTSA, and the FCC "perform closely related regulatory missions,"[98] "Congress has allocated each of them a role implementing…related statutes"[99] and all "share an interest" in the implementation of connected vehicle technology. Furthermore, such joint policymaking efforts "tend to be more visible and legally enforceable then interagency agreements."[100] In an area where security and privacy are prevalent such visibility and enforceability is tantamount to the success of connected vehicle technology.

---

[95] *Id.* 1167-1168.
[96] *Id*. at 1167.
[97] *Id.* at 1169 (referring to joint EPA-NHTSA rule and Dodd-Frank Act joint rulemaking requirements).
[98] 47 U.S.C. § 151 (2017) ("for the purpose of promoting safety of life and property through the use of wire and radio communications."); 49 U.S.C. § 30101 (2013) ("to reduce traffic accidents and deaths and injuries resulting from traffic accidents."); 15 U.S.C § 45(a) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").
[99] *E.g.*, Markey, *supra* note 48 (the FCC in implementing licensing and servicing rules for the 5.9ghz bandwidth). 49 U.S.C. § 30101 (2013) (NHTSA in implementing DSRC as "motor vehicle equipment" which utilizes this bandwidth to operate). 15 U.S.C § 45(a) (2012) (the FTC in preventing possible "unfair trade practices" using data created by this system.).
[100] Turrecha, Pulliam & Bruno, *supra* note 90, at 1166. *See also* Freeman & Rossi, *supra* note 91, at 12.

One of the great benefits of such joint policy making is the capability to "adopt[] another agency's rules as reference."[101] NHTSA has spent a respectable and considerable amount of time developing V2V and V2I communication systems. The benefit of joint rulemaking will allow adopting of NHTSA's current rules as a foundation from which to begin further collaboration. This will also help alleviate auto manufacturers concerns regarding delay of the technology as well as provide them additional time to prepare for the mandate. Examples of successful joint rulemaking efforts NHSTA has engaged in the past include a joint rule on greenhouse gas emissions formed in conjunction with the Environmental Protection Agency.[102]

NHTSA and the Environmental Protection Agency could have tried to issue compatible rules. However, going through the process of joint rulemaking "made the prospect of successful harmonization much more likely. According to a GAO report reviewing the process, the agencies worked much more closely together than ever before, sharing responsibility for the rule from preamble to conclusion."[103] Other regulations such as the Dodd-Frank Act go so far as to "require[] joint rulemaking in many provisions" due to the overlapping jurisdictional nature of financial regulation. These requirements serve to "minimize potentially inconsistent regulations" while "manag[ing] numerous overlaps" in the sector of financial regulation.[104]

Applied to connected cars, the different expertise of the NHTSA, FTC, and FCC would produce more well-

[101] Turrecha, Pulliam & Bruno, *supra* note 91.
[102] *Id.* at 1169.
[103] *Id.* at 1172-73.
[104] *Id.* at 1168.

rounded regulations. As Freeman and Rossi explain "[o]verlapping delegations are not always inefficient. They can create distinct advantages, including the potential to harness the expertise and competencies of specialized agencies."[105]

As to connected vehicle technology, such a benefit could be realized by allowing decision making to be led by the agency whose expertise and jurisdiction best fit the particular section of the rule in question. For example, decisions on the collection and use of data gathered would be led by the FTC. Decisions regarding the security of the overall communications system, the 5.9ghz bandwidth, would be led by the FCC. Decisions regarding the vehicle itself, such as malware spreading to other systems on the car, would be led by the NHTSA. Despite these possible specializations, all agencies would have the opportunity and discretion to collaborate and make decisions on the holistic framework to ensure its overall suitability to the solution.[106]

---

[105] Freeman & Rossi, *supra* note 92.

[106] An Inter-Agency Working Group would also mitigate the danger of so-called regulatory capture. Ralph Nader framed the issue in a different automobile context: "[w]hile GM's defective parts killed people when air bags failed to open, NHTSA failed when its investigations failed to open despite repeated warnings of deadly problems…Its passive approach to the companies it is supposed to regulate…fits the textbook definition of "regulatory capture"." Identification of regulatory capture can be complicated, often only identifiable by the public with the benefit of hindsight. However, the solution to prevent this risk from coming to fruition is the inter-agency working group model. Ralph Nader, *Safety in name only at NHTSA*, USA TODAY (Sep. 17, 2014), http://www.usatoday.com/story/opinion/2014/09/17/ralph-nader-safety-nhtsa-investigation-regulation-congress-gm-stalled-column/15801047/. "A report from the House Energy and Commerce committee…found that NHTSA's incompetence played a role in allowing the General Motors ignition switch crisis to go undetected for years, and says that

GAO reports on NHTSA also establish some concern as to their ability to regulate this area alone.[107]

C. Why the FCC?

If the proposal for an inter-agency working group is to be followed, its composition is critical. The FCC has extensive experience working on cybersecurity and privacy issues.[108] DSRC uses the 5.9GHz bandwidth which "the FCC is responsible for the entirety of"[109] and "the FCC's

---

the agency continues to lag behind in its efforts to improve its performance." *See* STAFF REPORT ON THE GM IGNITION SWITCH RECALL: REVIEW OF NHTSA U.S. H.R. COMM. ON ENERGY AND COMMERCE, (Sep. 16, 2014), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20140915GMFootnotes/NHTSAreportfinal.pdf.

[107] The United States Government Accountability Office found that NHTSA did not have the critical knowledge and expertise in security or privacy that is needed to protect the auto industry from cyber threats. "NHTSA itself state[d] that it will not have a clear position on whether there is even a need for cybersecurity standards in vehicles until 2018." Furthermore, "[T]he 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." Open Technology Institute & Public Knowledge, *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)*, iv (June 28, 2016).

[108] Electronic Privacy Information Center, Comment Letter on Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications (Oct. 20, 2014), https://epic.org/apa/comments/EPIC-NHTSA-V2V-Comments.pdf.

[109] *Understanding the Difference Between NHTSA and the FCC's Definitions of DSRC*, PUBLIC KNOWLEDGE 2, https://www.publicknowledge.org/assets/uploads/documents/1Pager_-

service rules for the band serve as the backdrop against which NHTSA's DSRC standards are deployed. Th[ese] service rules govern basics of the safety services…as well as any noncommercial services deployed in the majority of the band."[110] In allocating the 5.850-5.925 GHz spectrum for DSRC devices, the FCC reserved the right to take "whatever action is necessary to implement the standards related to DSRC use."[111]

The FCC is also heavily focused on cybersecurity and has aggressively sought to protect the privacy[112] and security of consumers. In 2014, the FCC fined two telecommunications companies $10 million dollars for not protecting consumer's financial data.[113] At the time FCC

_NHTSA_vs_FCC_DSRC.pdf.

[110] *Id*.

[111] *In the Matter of 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 Services, Report and Order*, ET Docket No. 98-95, 14 FCC Rcd. 18221 (1999) (explaining "[w]e defer consideration of licensing and service rules and spectrum channelization plans to a later proceeding because standards addressing such matters are still under development by the Department of Transportation. Once such standards are developed, the Commission could take whatever action is necessary to implement the standards related to DSRC use.").

[112] *See* Nat'l Cable & Telecommunications Ass'n v. Fed. Commc'n Comm'n, 555 F.3d 996 (D.C. Cir. 2009) (upholding the Commission's order for consent opt-in scheme in response to rise in third party data brokers). Note that automakers utilizing connected vehicle or wireless technology already store data, sometimes in third party data centers. *Supra* note 32.

[113] Press Release, Federal Communications Commission, FCC Plans $10M Fine For Carriers That Breached Consumer Privacy (Oct. 24, 2014), available at http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches. *See also* Brian Fung, *With a $10 million fine, the FCC is leaping into data security for the first time*, THE WASHINGTON POST (Oct. 24, 2014),

official Travis Leblanc warned it wouldn't be the last data security action by the FCC; additional enforcement actions have supported this posture[114] Furthermore, at a time when the FCC is refreshing the record on sharing techniques in the 5.850-5.925 GHz band that would allow commercial applications to utilize the bandwidth alongside life and safety systems[115] deployment of such devices at this time would present unique challenges.

More importantly, the FCC has jurisdiction over "wire and radio," including the 5.9 GHz bandwidth.[116] The FCC has a "broad scope of authority"[117] and therefore should have a role in regulating DSRC to fulfill its statutory

---

https://www.washingtonpost.com/news/the-switch/wp/2014/10/24/with-a-10-million-fine-the-fcc-is-leaping-into-data-security-for-the-first-time.

[114] *Id*. *See also* Fed. Commc'n Comm'n, *AT&T to Pay $25 Million To Settle Consumer Privacy Investigation: FCC's Largest Data Security Enforcement Action*, FCC, (Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf.

[115] *The Commission Seeks to Update and Refresh the Record in the "Unlicensed National Information Infrastructure (U_NII) Devices in the 5 GHz Band" Proceeding*, ET Docket No. 13-49, Public Notice, 31 FCC Rcd. 6130 (2016).

[116] 47 U.S.C. § 151 (2017).

[117] FCC v. Midwest Video Corp., 440 US 689, 696 (1979) (citing FCC v. Pottsville Broadcasting Co., 309 US 134, 138 (1940)) ("Congress meant to confer broad authority on the Commission…so as to "maintain through appropriate administrative control, a grip on the dynamic aspects of radio transmission""). *See also* Cooperative Comm. Inc. v. AT&T Corp., 867 F.Supp. 1151, 1516 (D. Utah 1994) (finding that "in enacting the Communications Act, it is manifest that Congress intended to occupy the field of telecommunications, in order to make available to all people of the United States a rapid, efficient, reasonably-priced communications service, governed by one uniform regulatory scheme" and holding that state tort law claims were not barred due to savings clause in Communications Act).

mandate.[118] Additionally, the FCC has ancillary jurisdiction over the "regulated subject" in question, i.e., DSRC devices using the 5.9GHz bandwidth.

D. Why The FTC?

The Federal Trade Commission has extensive experience in data security, bringing over 60 enforcement actions since 2002.[119] 50 of these actions led to settlements.[120] Jessica Rich, the Director of the Bureau of Consumer Protection explains that "data security enforcement remains a critical FTC priority"[121] and, as such,

---

[118] American Broadcasting Co. v. F.C.C., 191 F.2d 492, 498 (D.C. Cir. 1951) (reasoning "[t]he purpose of Congress in establishing the Commission was to set up an expert agency capable of coping with the ever-changing and constantly-increasing problems of a booming industry" and upholding Commission's authority to regulate broadcast frequency allocation but reversing Commission's orders on other grounds). *See also Pottsville*, *supra* note 117 at 138 ("Underlying the whole law is recognition of the rapidly fluctuating factors characteristic of the evolution of broadcasting and of the corresponding requirement that the administrative process possess sufficient flexibility to adjust itself to these factors").

[119] David Gerber, *FTC: Bad Cybersecurity Is an Unfair Trade Practice*, OFFIT KURMAN (Sept. 12, 2016), http://www.offitkurman.com/ftc-bad-cybersecurity-is-an-unfair-trade-practice/. *See also* Cases and Proceedings Advanced Search: Consumer Protection Data Security from January 1, 2002 to December 31, 2017 (duplicating this search on the FTC website will return the aforementioned results.)

[120] Soyong Cho & Andrew L. Caplan, *Cybersecurity Lessons Learned From the FTC's Enforcement History*, K & L GATES 2 (Dec. 2014), http://m.klgates.com/files/Publication/eeb01ded-7e7e-4e1a-a055-b50d1b66387a/Presentation/PublicationAttachment/46b8860d-63fd-48af-aaf0-bbfd00f7a9ed/Cybersecurity_Alert_122214.pdf.

[121] *Id.*

many have viewed the FTC as the "primary federal data security regulator."[122]

Another emerging technology that shows the potential benefits of the FTC's role on the proposed inter-agency working group is the Internet of Things. The FTC deals extensively with the Internet of Things which connects our world more every day. This year the largest distributed denial of service attack in history occurred with the aid of the Internet of Things. These devices provided for the formation of a botnet which sent approximately 665 Gb worth of packets each second towards the servers that ran the website Krebs on Security.[123] This is the equivalent of a hard drive on a modern laptop being completely filled with data every second. Another famous attack utilizing the botnet nicknamed Mirai took advantage of Internet of Things

---

[122] Ryan T. Bergsieker, Richard H. Cunningham & and Lindsey Young, *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 THE COLO. LAW 39, 39 (2015). Furthermore, "FTC attention has regularly focused on data encryption. In more than half of cases requiring data or security programs, the FTC addressed the defendant's encryption protocols." Such experience would be useful in reviewing encryption methodologies used in Connected Vehicle Technology. The FTC's experience with connected technologies also speaks volumes about the possible benefit of their participation in rulemaking. *See* Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, THE PRIVACY ADVISOR (Sept. 19, 2014), https://iapp.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices/.

[123] Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KREBSONSECURITY (Sept. 21 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. *See also* Eduard Kovacs, *Brian Krebs' Blog Hit by 665 Gbps DDoS Attack*, SECURITY WEEK (Sept. 21, 2016), http://www.securityweek.com/brian-krebs-blog-hit-665-gbps-ddos-attack.

devices such as CCTV's and digital video recorders to flood and interrupt services provided by the domain name service provider Dyn.[124] As a result, many highly trafficked websites including Twitter and Spotify were unable to stay up and running.[125]

> "The FTC hasn't been silent on Internet of Things security. In a speech at the Consumer Electronics Show (CES) in 2015, Ramirez called on companies making IoT products to limit the data they collect and destroy it when it is no longer needed. Companies exploring the Internet of Things market should appoint a security lead to manage privacy and security issues during product development. And IoT product companies should clearly explain to consumers when their data is being sold to marketing firms or used in ways they may not expect, Ramirez recommended…. The FTC under Ramirez has been among the most aggressive federal agencies in addressing the security and privacy challenges of the IoT. In addition to sponsoring conferences to discuss the impact of connected devices, the agency has put its foot forward to enforce laws about the collection and sharing of geolocation information. It has also issued fines to companies

---

[124] Paul, *Lawmakers to FTC: Do Something about Internet of Things Security*, SECURITY LEDGER (Nov. 8, 2016), https://securityledger.com/2016/11/lawmakers-to-ftc-do-something-about-internet-of-things-security/. *See also* Letter from Frank Pallone Jr., Member, Comm. on Energy and Commerce, Jan Schakowsky, Member, Subcomm. on Commerce, Mfg., and Trade, to Edith Ramirez, Chairwoman, Fed. Trade Comm'n (Nov. 3, 2016).

[125] *Id*.

> that fail to properly secure their technology, resulting in harm to consumers."[126]

The FTC even sponsored a 25,000 prize competition aimed at developing "a tool that can be used against security vulnerabilities in Internet of Things systems."[127] "At its Internet of Things workshop in November 2013, the Commission specifically examined privacy and security issues relating to the different technologies involved with connected cars, including Event Data Recorders ("EDRs") and other vehicle telematics."[128] Based on this 2013

---

[126] *Id.*

[127] Fed. Trade Comm'n, *FTC Announces Internet of Things Challenge to Combat Sec. Vulnerabilities in Home Devices*, FTC (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security. *See also* Patrick Thibodeau, *FTC sets $25,000 prize for automatic IoT patching*, COMPUTER WORLD (Jan. 4, 2017), http://www.computerworld.com/article/3154348/security/ftc-sets-25-000-prize-for-automatic-iot-patching.html.

[128] Fed. Trade Comm'n, Comment Letter In the Matter of Advanced Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle Communications (Oct. 20, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf.

> [P]articipants described three general types of potential privacy and security risks arising from this connectivity. First, participants expressed concern about the ability of connected car technology to track consumers' precise geolocation over time . Such information may divulge personal details about an individual. Did Consumer A visit an AIDS clinic last Tuesday? What place of worship does he attend?...Second, FTC workshop participants expressed a concern that information about driving habits could be used to price insurance premiums or

Workshop[129] the FTC released a staff report "summari[zing] the workshop and provid[ing] staff[] recommendations in this area."[130] One recommendation is to incorporate security by design at the beginning of the product life cycle. The Commission recommends a few steps to achieve this including utilizing privacy and risk assessments, minimizing collection of data, and testing security measures before launch of the IoT product. The Commission also recommends training of employees in security, hiring of outside companies that have the capability to maintain "reasonable security," use of the defense in depth approach to protect identified risks, use of access control mechanisms to prevent unauthorized access, and finally monitoring of the product through its life cycle including the patching of vulnerabilities.[131]

The FTC has already contributed valuable input to NHTSA's ANPRM, including: "three primary concerns relating to V2V communications…The ability of connected car technology to track consumers' precise geolocation over

> set prices for other auto-related products….A third concern relates to the security of connected cars. At the Commission's Internet of Things workshop, one participant discussed his successful efforts to remotely access a car's internal computer network; he reported that he was able to control the vehicle's brakes and other critical functionality by hacking into the telematics unit.
> *Id.*

[129] FTC, THE INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[130] *Id.* at i.
[131] *Id.* at iii.

time; Information about driving habits used to price insurance premiums or set prices…and [t]he security of connected cars, including the ability for third-parties to remotely access a car's internal computer network."[132]

III. JURISDICTIONAL ANALYSIS

A. Radio is the FCC's Jurisdiction

1. Purpose of The FCC

The FCC was created "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio…for the purpose of promoting safety of life and property through the use of wire and radio communications, and for the purpose of securing a more effective execution of this policy by centralizing authority…granted by law to several agencies and by granting additional authority with

---

[132] Kelley Drye & Warren LLP, *FTC supports NHTSA's approach to privacy in V2V rulemaking*, LEXOLOGY (Oct. 27, 2014), http://www.lexology.com/library/detail.aspx?g=ac560f3f-f245-4d9f-a18d-729b3c090b48. The FTC has since acknowledged that NHTSA appropriately addressed these concerns in their current NPRM. *Id.*

> The FTC also noted that…NHTSA designed the proposed V2V system to limit the data collected and stored to that which serves the intended safety purposes, and to ensure that the collected data cannot be used to identify a particular individual or vehicle. Lastly, with respect to the security of the collected data, the FTC supports the NHTSA's decision to help mitigate the potential for unauthorized access to data by keeping the V2V device separate from other onboard computers.
> *Id.*

respect to interstate and foreign commerce in wire and radio communication."[133] The D.C. Circuit Court in *American Broadcasting* explained the reasoning for Congress in creating the FCC was to establish an agency to be able to adapt to the "ever-changing and constantly-increasing problems of a booming industry."[134]

In *American Broadcasting*, the Court was faced with a dispute regarding broadcast frequency allocation. The case dealt with special service authorizations which allowed the FCC to grant a temporary license to broadcasters to transmit on a different frequency then the one they had been licensed to use.[135] The Court found no reason to hold that these licenses were outside the FCC's authority.[136] Instead, the Court wrote that Section 303(r) of the Communications Act of 1934 "contemplates that the Commission will take the lead in exploring the possibilities of radio, and we think unlikely that Congress had in mind a particular method to this end."[137] These "possibilities of radio" are constantly being explored and protected by the FCC.

Several offices within the FCC work to fulfill the FCC's purpose in regards to radio. Specifically, the Wireless Telecommunications Bureau "develops and executes policies and procedures for fast, fair licensing of all wireless services…amateur radio to mobile broadband services."[138]

---

[133] 47 U.S.C. § 151.

[134] *American Broadcasting Co*., *supra* note 118 (reasoning "[t]he purpose of Congress in establishing the Commission was to set up an expert agency capable of coping with the ever-changing and constantly-increasing problems of a booming industry").

[135] *Id.*

[136] *Id.*

[137] *Id*.

[138] *Wireless Telecommunications,* FCC, https://www.fcc.gov/wireless-telecommunications.

The Office of Engineering and Technology "maintains the U.S. Table of Frequency Allocations, manages the Experimental Licensing and Equipment Authorization programs, regulates the operation of unlicensed devices, and conducts engineering and technical studies."[139]

2. Scope of Authority

The Communications Act of 1934 "expresse[d] a desire on the part of Congress to maintain … a grip on the dynamic aspects of radio transmission. Underlying the whole law is recognition of the rapidly fluctuating factors characteristic of the evolution of broadcasting … and of the corresponding requirement that the administrative process possess sufficient flexibility to adjust itself to these factors."[140] "[I]t is clear that Congress meant to confer "broad authority" on the Commission…so as "to maintain, through appropriate administrative control, a grip on the dynamic aspects of radio transmission."[141]

United States Telecom Ass'n v. Fed Commc'n Comm'n dealt with the scope of the FCC's statutory

---

[139] *Engineering & Technology*, FCC, https://www.fcc.gov/engineering-%26-technology. In 2003 in an effort to protect the safety of the American public the FCC "adopted a Report and Order establishing licensing and service rules for the Dedicated Short Range Communications Service in the…5.9 GHz band". The FCC also licenses the DSRC road units which allow vehicle to infrastructure communication. *See Dedicated Short Range Communications (DSRC) Service*, FCC, (last visited Mar. 12, 2007), http://wireless.fcc.gov/services/index.htm?job=service_home&id=dedicated_src.

[140] *FCC v. Pottsville,* 309 U.S. 134, 138 (1940).

[141] *FCC v. Midwest Video Corp.*, 440 US 689, 696 (1979) (explaining the broad scope of authority intended by Congress when creating the FCC in 1934).

authority. In *US Telecom*, the issue presented to the D.C. District Court was whether "broadband internet access service c[ould] be considered a telecommunications service" and therefore under the FCC's jurisdiction specifically in regard to its 2015 Open Internet Order.[142] Telecom argued that the FCC's 2015 Open Internet Order went "beyond the scope of whatever ambiguity [the statute] contains."[143] The Court reasoned "that the proper classification of broadband turns "on the factual particulars of how Internet technology works and how it is provided, questions *Chevron* leaves to the Commission to resolve in the first instance."[144]

DSRC technology falls under Title II regulation by the FCC. Under the Telecommunications Act of 1996,[145] a telecommunications service as opposed to an information service falls under more restrictive Title II regulation. A telecommunications service is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[146] An information service is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[147] Although one might reason that DSRC would be classified as an information service, since there is no fee for DSRC besides that which is added to the

---

[142] *United States Telecom Ass'n v. Fed. Commc'n Comm'n*, 825 F.3d 674, 730 (D.C. Cir. 2016) (upholding broadband internet access as a telecommunications service under FCC regulatory authority).
[143] *Id* at 702.
[144] *Id* at 701.
[145] Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).
[146] 47 U.S.C. §153(53).
[147] 47 U.S.C. §153(24).

cost of the car, there is a third category which was created by Congress. This category is called the telecommunications management exception, which "exempts from information service treatment—and thus treats as a telecommunications service — "any use [of an information service] for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[148] Since DSRC would be utilized "for the management, control, or operation of a telecommunications system"[149] known as V2V communication DSRC falls under this exception and is thus subject to more restrictive common carrier regulation as a telecommunications service. This is important because it allows the FCC to exercise more authority in regulating DSRC.

Likewise, in *US Telecom*, the finding that broadband internet access was a telecommunications service subjected it to more restrictive common carrier regulation.[150] The Court majority upheld the agency's interpretation of broadband internet access services as a form of telecommunications service.[151]

Jurisdiction over wire and radio is expressly granted in the FCC's founding statute.[152] Unlike broadband internet access, regulating DSRC devices does not involve the reclassification of DSRC as radio. Even if it were to involve such reclassification, DSRC devices, like broadband internet access, provide "data to and from … endpoints."[153] Regardless, DSRC devices utilize the 5.9 GHz radio bandwidth which "the FCC is responsible for the entirety

[148] *United States Telecom Ass'n,* 825 F.3d at 691.
[149] *Id*.
[150] *Id* at 739.
[151] *Id* at 700.
[152] 47 U.S.C. § 151.
[153] *United States Telecom Ass'n*, *supra* note 142, at 696.

of"[154] and the rules for this band are the foundation "against which NHTSA's DSRC standards are deployed."[155] The FCC is obligated by its statutorily mandated responsibilities to "allocate the spectrum in a manner that promotes the "safety of life and property."[156] Furthermore, "under *City of Arlington*, the agency is entitled to deference even in matters concerning the scope of its own authority."[157]

3. In the Alternative, FCC has Ancillary Jurisdiction Over DSRC Technology

"The Commission recognized that it may exercise ancillary jurisdiction … when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities."[158] The FCC's "general jurisdiction grant" under Title I covers "wire and radio."[159] Therefore, the FCC's "general jurisdiction grant" covers "the regulated subject" or DSRC devices. The FCC was commissioned "for the purpose of promoting safety of life and property through the use of wire

---

[154] Public Knowledge, *supra* note 109, at 2.
[155] *Id*.
[156] Nat'l Assoc of Broadcasters v. FCC, 740 F.2d 1190, 1213 (D.C. Cir. 1984) (upholding Commission's decision to deregulate DBS systems).
[157] Christopher Wright, *The Scope of the FCC's Ancillary Jurisdiction After the D.C. Circuit Court's Net Neutrality Decisions*, 67 F. Comm's. L. J. 20, 34 (2015).
[158] American Library Assoc. v. FCC, 406 F. 3d 689, 691- 692 (D.C. Cir. 2005). Cited solely for purposes of laying out ancillary jurisdiction analysis. Case actually holds that the FCC exceeded their statutory authority regarding broadcast flag technology.
[159] 47 U.S.C. § 151.

and radio communications."[160] Thus, regulating DSRC devices are within the FCC's "statutorily mandated responsibility."

An opposing argument might point to the leading case *Comcast* where the Court found the FCC did not have ancillary jurisdiction.[161] However, that case was centered around the regulation of network management practices.[162] The Comcast Court explains "Courts have come to call the Commission's section 4(i) power its "ancillary" authority."[163] Section 4(i) provides that the Commission is authorized to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[164] The *Comcast* Court notes that rejection of ancillary authority in all "three [leading Supreme Court] cases dealt with Commission jurisdiction over early cable systems at a time when the Communications Act gave the Commission no express authority to regulate such systems." [165] Contrary to these cases, Congress gave express authority over radio to the FCC.[166]

---

[160] *Id*.
[161] *Compare* Comcast Corp v. F.C.C., 600 F.3d 642, 644 (D.C. Cir. 2010) *with*, 47 U.S.C. § 151 (distinguishing from present issue where authority is explicitly provided for by Congress).
[162] *Comcast Corp*., 600 F.3d at 644.
[163] *Id* at 646.
[164] 47 U.S.C. § 154(i).
[165] *Comcast* at 646; citing United States v. Southwestern Cable Co., 392 U.S. 157, 88 S.Ct. 1994, 20 L.Ed.2d 1001 (1968), United States v. Midwest Video Corp., 406 U.S. 649, 92 S.Ct. 1860, 32 L.Ed.2d 390 (1972) (Midwest Video I), and FCC v. Midwest Video Corp., 440 U.S. 689, 99 S.Ct. 1435, 59 L.Ed.2d 692 (1979) (Midwest Video II).
[166] 47 U.S.C. § 151.

4. The FCC's Interpretation of its Statutory Authority is Entitled to Chevron Deference

Chevron provides a two-step analysis for assessing whether an agency is afforded deference as to statutory interpretation. "First…is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter…[I]f the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute."[167]

Congress expressly provided that the FCC have jurisdiction over radio in the Communications Act of 1934. Assuming arguendo that such an intent is ambiguous as to DSRC, the FCC already regulates the bandwidth. Therefore, whether such an interpretation of its statutory authority is permissible has already been decided by previous regulation. As to the regulation of radio including Dedicated Short Range Communications the FCC is entitled to *Chevron* deference. Furthermore, "[u]nder *Chevron*…the FCC is entitled to substantial deference in its interpretation of the Communications Act, [and]…under *City of Arlington,* the agency is entitled to deference even in matters concerning the scope of its authority."[168]

---

[167] Chevron v. Natural Resources Defense Council, 467 U.S. 837, 842-43 (1984) (providing *Chevron* deference analysis).

[168] Wright, *supra* note 157, at 34. *See also* City of Arlington Tex, v. F.C.C., 133 S. Ct. 1863, 1866 (2013) ("We consider whether an agency's interpretation of a statutory ambiguity that concerns the scope of its regulatory authority (that is, its jurisdiction) is entitled to deference under Chevron. . .").

B. FTC Jurisdiction in Support of Privacy of Individuals

The Federal Trade Commission's authority over data security arises from "Section 5(a) of the Federal Trade Commission Act."[169] The Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[170] This authority was affirmed in *Fed. Trade Comm'n v. Wyndham Worldwide Corp*.[171] The FTC alleged that Wyndham, a hospitality company, stored credit card information in unencrypted text, permitted use of simple passwords, and did not use firewalls

> "It suffices to decide this case that the preconditions to deference under Chevron are satisfied because Congress has unambiguously vested the FCC with general authority to administer the Communications Act through rulemaking and adjudication, and the agency interpretation at issue was promulgated in the exercise of that authority. . . . Where Congress has established a clear line, the agency cannot go beyond it; and where Congress has established an ambiguous line, the agency can go no further than the ambiguity will fairly allow. But in rigorously applying the latter rule, a court need not pause to puzzle over whether the interpretive question presented is "jurisdictional." If "the agency's answer is based on a permissible construction of the statute," that is the end of the matter."
> *Id*. at 1872.

[169] 15 U.S.C § 45(a) (2012).
[170] *Id.*
[171] Skelton Crystal, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, COMPETITION J. 302, 303 (Spring 2016), http://www.kelleydrye.com/publications/articles/2079/_res/id=Files/index=0/Competition%20Journal%20Article%20by%20Crystal%20Skelton.pdf (citing Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015)).

to segregate its corporate and hotel property management networks from the internet contrary to the company's stated policy.[172] The Court held that the "company's alleged failure to maintain reasonable and appropriate data security…could constitute an unfair method of competition in commerce."[173]

"The FTC is the most active government enforcer with respect to business compliance with data security obligations."[174] Companies, such as auto manufacturers for example, "that accept consumers' personal data without reasonable and appropriate data security procedures to protect the data are considered by the Federal Trade Commission…to be engaging in unfair, and potentially deceptive, trade practices, in violation of 15 U.S.C. §§ 45(a) and (n) ("Section 45")."[175] Furthermore, if third party vendors do not use reasonable security measures the FTC may find the contracting company liable for the vendor's own lack of security measures [176] "In several cases, the FTC has alleged that the defendant was responsible for the security deficiencies of its third-party clients or end-users of its products or services."[177] An example of such third-party vendors in the context of the connected vehicle technology mandate would include the certificate authorities on which the system depends. The data created by connected vehicle technology in general could eventually be subject to the same standards as other personal consumer data. The FTC's collaborative input and expertise is likely to ensure that auto

[172] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d Cir. 2015).
[173] *Id.* at 236.
[174] *Skelton*, *supra* note 171, at 303.
[175] Gerber, *supra* note 119.
[176] Cho & Caplan, *supra* note 120.
[177] *Id.*

manufacturers have a clear yet affective standard to which they can adhere.

It is important to note that while the FTC has enforcement authority for unfair and deceptive trade practices their rulemaking authority is more limited. The FTC's rulemaking authority extends to the "use [of] trade regulation rules to remedy unfair or deceptive practices that occur on an industry-wide basis."[178] "Under Section 18 of the FTC Act, 15 U.S.C. Sec. 57a, the Commission is authorized to prescribe "rules which define with specificity acts or practices which are unfair or deceptive."" [179] However, "before commencing a rulemaking proceeding the Commission must have reason to believe that the practices to be addressed by the rulemaking are "prevalent"."[180] In order to engage in rulemaking related to the V2V mandate the FTC would have to do so by specifying unfair or deceptive acts and practices related to DSRC. Furthermore, such rulemaking would have to address unfair or deceptive practices which are prevalent. However, throughout V2V rulemaking the FTC's comments have proven helpful and continued collaboration through an Inter-Agency Working Group is likely to yield similar results despite the FTC's admittedly limited authority regarding V2V rulemaking. With regard to enforcement for deceptive acts and practices involving data security the FTC's enforcement authority is well established.

---

[178] FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* FCC (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[179] *Id.*
[180] *Id.* (citing 15 U.S.C. § 57a(b)(3)).

1. Deceptive Practices

"Early FTC data security cases relied almost exclusively on allegations of deceptive trade practices based on security practices inconsistent with representations companies made in their privacy policies or elsewhere."[181] Generally, "[t]he FTC will consider an act or practice to be deceptive "if there is a representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[182] "In the data security context, the FTC generally finds an act deceptive if an entity makes materially misleading statements…or deceptive omissions of material facts concerning its security measures and how it would handle, protect, or otherwise treat personal information that is inconsistent with the entity's actions."[183]

The amount of the FTC's consent decrees regarding misrepresentation and the misleading of consumers about the security or quality of their products speaks further to their competence and experience in data security.[184] As

---

[181] *FTC Data Security Standards and Enforcement*, Practical Law Intellectual Property & Technology, Resource ID 8-617-7036.

[182] Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html.

[183] *Id. See also* 15 U.S.C. § 45(a) (2012); letter from Chairman Miller III, *FTC Policy Statement on Deception*, 1-2 (Oct. 14, 1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[184] In the Matter of ASUSTeK Computer, Inc., No. 142 3156, 2016 WL 807981, 37-44 (F.T.C. Feb. 22, 2016) (providing 4 counts for misrepresentations); In the Matter of Oracle Corp., No. 132 3115, 2016 WL 1360808, 3 (F.T.C. Mar 28, 2016) (explaining "Oracle represented, directly or indirectly, expressly or by implication, that by updating Java

aforementioned the Markey report discovered the majority of auto manufacturers offered technology features that gathered and sent data to a data center, sometimes run by a third party and explained further that "[c]ustomers [we]re often not explicitly made aware of data collection."[185] Such an omission in the context of connected vehicle technology could be considered deceptive practices in or affecting commerce. Although the FTC does not typically bring enforcement actions in the transportation sector[186] a review of *DOT Litigation News* reveals that NHTSA has not brought any enforcement actions in regards to data security practices by automakers.[187] The FTC may also pursue data security cases as unfair practices.

SE, Java users would ensure that Java SE on their computers had the latest security improvements. Oracle failed to disclose…in numerous instances, updating Java SE would not delete or replace all older iterations of Java SE…and as a result, a consumer's computer could still have iterations of Java SE installed that are vulnerable to security risks. This fact would be material to consumers' decision whether to take further action after "updating" Java SE to protect their computers."); In the Matter of Microsoft Corp., 134 F.T.C. 709, 2002 WL 34463137, 715 (F.T.C. Dec. 20, 2002) ("Passport did collect personally identifiable information other than that described in its privacy policy….the representation set forth in paragraph 15 was false or misleading.")

[185] *Supra* note 35.

[186] *FTC Data Security*, *supra* note 181.

[187] Office of General Counsel, *DOT Litigation News*, Department of Transportation https://www.transportation.gov/administrations/office-general-counsel/litigation-news, (last updated May, 6 2016) (reviewing March 2010 to March 2016).

2. Unfair Practices

The FTC has jurisdiction over "unfair…acts or practices in or affecting commerce."[188] "[T]he following three factors govern[] unfairness determinations: (1) whether the practice,… offends public policy…whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen)." As noted by the Court in *Wyndham* "the Supreme Court implicitly approved these factors…acknowledging their applicability to contexts other than cigarette advertising and labeling."[189] "The Court also held that, under the policy statement, the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied."[190]

As to substantial injury to the consumer "[T}he FTC will deem an act or practice to be "unfair" if it (1) causes or is likely to cause substantial consumer injury (2) which is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers and password maintenance to data collection and storage practices."[191] "The FTC's evaluation for an unfairness claim

---

[188] 15 U.S.C. §45(a)(1) (2012).
[189] *FTC v. Wyndham*, *supra* note 172, at 240.
[190] *Id.* at 243 ("§ 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.")
[191] *Id.*

will generally focus on whether the practices at issue were "reasonable" under the circumstances and in light of industry standards, the cost and ease of having various security controls in place, and the known vulnerabilities of not having such controls."[192]

When considering data created by connected vehicle technology consumers have little control over how that data is used. Consumer injury resulting from the theft or manipulation of connected vehicle data would be "likely to cause substantial consumer injury", could not be "reasonably avoided by consumers themselves", and considering the availability of software to manage access to data such limited costs cannot "outweigh the countervailing benefits" to such consumers. As Senator Markey noted, "[c]ustomers [we]re often not explicitly made aware of data collection and, when they [we]re, they often cannot opt out without disabling valuable features, such as navigation."[193] Data on vehicle location and travel patterns could cause substantial consumer injury whether this data is used for more direct criminal purposes such as stalking, the targeting of homes for purposes of burglary,[194] or simply resale on the dark web to be used in identity theft.[195]

---

[192] *Id.*

[193] Markey, *supra* note 35.

[194] Beyoud, *supra* note 44.

[195] *See generally* Vindu Goel & Nicole Perlroth, *Hacked Yahoo Data Is for Sale on Dark Web*, N.Y. TIMES, Dec. 15, 2016, https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0; James Connington, *How to check if your financial data is for sale on the dark web*, TELEGRAPH, Feb. 19, 2016, http://www.telegraph.co.uk/money/consumer-affairs/how-to-check-if-your-financial-data-is-for-sale-on-the-dark-web/; Arjun Kharpal, *Hackers are selling your data on the dark web…for only $1*, CNBC, Sept. 23, 2015, http://www.cnbc.com/2015/09/23/hackers-are-selling-your-data-on-the-dark-web-for-1.html.

The value of connected car data alone is valued around "$1.5 trillion by the year 2030 and it might even become a key focus area for the automotive industry."[196] This will draw attention from adversaries and lead to eventual breaches and subsequent theft of the data. As the mantra goes "it's not if, but when."[197] Therefore, it is paramount that auto companies are assured that their technologies including those mandated by NHTSA meet the data security standards provided not only by NHTSA but also those of the FTC. Consumers will not be the only ones who reap the benefits of a V2V Communications Inter-Agency Working Group.

IV. CONCLUSION

The Supreme Court in *FCC v. Fox Television* held that "agency action is not subject to a heightened or more searching standard of review simply because it represents a change in administrative policy…[and] not every agency action representing a change in policy need be justified by reasons more substantial than those required to adopt a policy in the first instance."[198] Thus, if the FCC grants the

---

[196] Tim Clark, *Fasten Your Seat Belt, Connected Car Data Worth $1.5 Trillion*, FORBES, Sept. 7 2016, http://www.forbes.com/sites/sap/2016/09/07/fasten-your-seat-belt-connected-car-data-worth-1-5-trillion/#226876455a2b.

[197] *See generally*, BAE Systems, CyberSecurity Breaches: It's not if, but when, available at*https://www.baesystems.com/en/cybersecurity/cyber-security-breaches-its-not-if-but-when*

[198] F.C.C. v. Fox Television Stations, Inc., 556 U.S. 502, 513 (2009) (explaining that "our opinion in *State Farm* neither held nor implied that every agency action representing a policy change must be justified by reasons more substantial than those required to adopt a policy in the first instance. That case, which involved the rescission of a prior

petition for Emergency Stay and undertakes Rulemaking, their decision to act requires only the same reasons that would be necessary to "adopt a policy" of regulating radio "in the first instance."[199] Applying the same reasoning the FTC could also argue for jurisdiction over V2V and other autonomous technologies. As the District Court of New Jersey noted in *F.T.C. v. Wyndham Worldwide Corp.*, "even accepting that the FTC shifted its stance on data security, this cannot limit its authority without more."[200]

Some but not all of the issues a V2V Inter-Agency Working Group should address are; the introduction of aftermarket devices into the network,[201] monitoring the accuracy of warnings including new warnings/features as they are added to the V2V system, further restrict access to data by encrypting the Basic Safety Messages transmitted through the network, actively monitor the addition and removal of devices from the Secure Certificate Management System, utilize defensive coding practices in the formulation

---

regulation, said only that such action requires "a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance.").

[199] *Id*. *See also Id.* at 502-03 (Scalia explaining "[t]here is, however, no basis…for a requirement that all agency change be subjected to more searching review. Although an agency must ordinarily display awareness that it is changing position…and may sometimes need to account for prior fact finding or certain reliance interests created by a prior policy, it need not demonstrate to a court's satisfaction that the reasons for the new policy are better than the reasons for the old one. It suffices that the new policy is permissible under the statute, that there are good reasons for it, and that the agency believes it to be better, which the conscious change adequately indicates.").

[200] F.T.C. v. Wyndham Worldwide Corp., 10 F.Supp 3d 602, 615 (D.N.J. 2014).

[201] FBI *supra note* 13, (explaining "[t]hird party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.").

of basic safety messages, and not allow access by private companies, including use of third party applications, to the DSRC 5.9GHz bandwidth. The Working Group should also consider logging all basic safety messages for auditing purposes.

The DSRC mandate presents an opportunity to begin interagency collaboration in the present rather than suffer through an inevitable jurisdictional tug of war that would result in duplicative, confusing regulations. However, the security and privacy of the public is paramount. If collaboration through an Inter-Agency Working Group is deemed unfeasible then the FCC must put consumer privacy and safety first and act alone to regulate DSRC devices. It is their statutorily mandated responsibility and they must begin now before the cars on America's highways are once again "*Unsafe at Any Speed*."[202]

[202] Nader, *supra* note 23.