Comment on the Department of Transportation's *Request for Comments: Vehicle-to-Everything (V2X) Communications*, 83 FR 66338 (proposed Dec. 26, 2018)

Authors: Sam Karson, Esko Brummel

Date: February 25th, 2019

Executive Summary

Department of Transportation (DOT) has requested comments from the public on recent developments in vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) communications sensors, collectively known as vehicle-to-everything (V2X) technologies, and how these developments may impact DOT's role in encouraging the integration of V2X communications into vehicles and transportation infrastructure. V2X communications technology allows vehicles to collect data from drivers, passengers, other vehicles, pedestrians, infrastructure, and the driving environment, and to transmit that data to other vehicles, pedestrians, infrastructure, car manufacturers, and third parties. V2X communications may, in the future, rely on fifth generation (5G) telecommunications technology, which would allow connected vehicles to collect and share data faster and in greater quantities. V2X communications are especially important to the functioning of automated driving features and autonomous vehicles.

This Comment addresses DOT's request for information regarding general issues surrounding V2X communications. First, this Comment provides background on DOT's efforts to encourage integration of V2X communications. Second, this Comment raises concerns about the lack of inter-agency coordination to address privacy issues resulting from the increased collecting and sharing of data through V2X communications. Third, this Comment highlights the

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

need for greater harmonization of cybersecurity standards relevant to V2X communications and the potential for DOT to invest in a more robust cybersecurity workforce. Finally, this Comment identifies areas for technological improvement in V2X communications between vehicles and pedestrians and regarding non-traditional vehicles, such as motorcycles. Ultimately, we conclude that DOT has yet to address several issues relevant to V2X communications with important implications for individual privacy, security, and safety.

Table of Contents

INTRODUCTION

Who We Are:

The Duke Science Regulation Lab (SciReg Lab)[1] is composed of graduate students from a variety of disciplines at Duke University, including science, law, ethics, and policy. The

[1] Michael B. Waitzkin, JD, J. H. Pate Skene, JD, PhD, and Sarah Rispin Sedlak, JD, are the faculty members who lead the SciReg Lab.

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

mission of the Duke SciReg Lab as a part of Duke University's Initiative for Science and Society is to bridge the expertise of scientists and policy-makers in the Federal Rule making process. To accomplish this, participants of the lab combine their experience with on-going research at Duke and beyond to provide unbiased, current, and comprehensive access to key research regarding pending rules and regulation. More information about SciReg Lab and our current projects can be found on our website at scienceandsociety.duke.edu under Engage, Signature Programs.

With the advice and oversight of the SciReg members, this comment was written and prepared by E. Scott Brummel, a researcher with Duke Robotics and Lead Editor for Robotics and AI policy coverage at SciPol.org, and Sam Karson, a JD candidate of Duke University.

B. The Department of Transportation's Request for Comments

On December 26th, 2018. the Department of Transportation (DOT) requested public comments on numerous issues concerning DOT's interest in V2X communications. This request for comments follows several years of inquiry by DOT regarding the emerging field of connected vehicles, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) communications.

In this Comment, we address new concerns brought about by the introduction of telecommunications to transportation. Specifically, the topics we seek to provide comment on are privacy and cybersecurity of connected V2X vehicles and mitigation strategies the DOT can employ. We also bring attention to concerns not recognized in the request for comments regarding issues and challenges for lighter vehicles, such as motorcycles and scooters, and pedestrians.

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

BACKGROUND

As a precursor to the DOT's 2018 request for comments, DOT has engaged in a series of projects related to a new paradigm of connected vehicles. We review these projects first to explain the scope of our review of DOT's work in this area and the trends we seek to address through this Comment.

In 2009, the DOT's Office for Research and Technology, called the Research and Innovative Technology Administration (RITA) at the time, released an annual Intelligent Transportation Systems (ITS) strategic plan[2], which described DOT's initial foray into connected vehicles.

By 2010, the DOT followed up on its strategic plan by releasing its Connected Vehicle Research program's "IntelliDrive" Policy Roadmap.[3] In this roadmap, the DOT outlined future areas of policy research including device and equipment certification, risk allocation and data ownership, cost-benefit analyses in support of deployment, infrastructure for V2V technologies, and governance structures and authorities for a V2X or connected transportation system.

By 2012, the DOT had dropped the "IntelliDrive" moniker. However, it continued its pursuit of researching the technical and regulatory topics previously outlined.[4] To support these efforts, in June of 2012, President Obama signed into law the Moving Ahead for Progress in the 21st Century Act (MAP-21)[5]. As a two-year reauthorization bill for the DOT, MAP-21 specifically strengthened the DOTs work with its inquiry into connected vehicles "by restoring

[2] United States of America. Department of Transportation. Research and Innovative Technology Administration. ITS Strategic Plan. 2009.
[3] United States of America. Department of Transportation. Research and Innovative Technology Administration. IntelliDrive Policy Roadmap. 2010.
[4] United States of America. Department of Transportation. Office for Research and Technology. U.S. Department of Transportation Celebrates 50 Years of Innovation in Intelligent Transportation. 2016.
[5] Congress, U. S. "Moving ahead for progress in the 21 st century act." *Washington, DC* (2012).

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

the … research budget to $100 million per year and establishing a Technology and Innovation Deployment Program for $62.5 million per year".[6]

After these first two years of increased investment in connected vehicles, then-Secretary of DOT Anthony Foxx announced in a February 2014 press release that DOT would finally realize the potential of its investment in connect vehicles through a pending new rule described in the following paragraph.[7] By August of that year, the National Highway Traffic Safety Administration (NHTSA) released an advance notice of proposed rulemaking (ANPRM) and a supporting comprehensive research report on V2V communication technology.[8]

After the ANPRM was released, the DOT and NHTSA released its Federal Motor Vehicle Safety Standard (FMVSS), No. 150.[9] This proposed mandate requires that after 2023 all new light-weight vehicles with four wheels be equipped with V2V communication technology. According to the proposed standard's preliminary regulatory impact analysis, V2V communication capabilities, such as Intersection Movement Assist (IMA), Left Turn Assist (LTA), and Do Not Pass Warnings, could prevent hundreds of thousands of crashes at an acceptable cost to the automotive industry and its consumers.[10]

As an explanation of DOT's emphasis on light-weight vehicles, its analysis indicates that about two out of three police-reported motor vehicle crashes (exactly 62%, or 3.4 million per

---

[6] See note 4.
[7] United States of America. Department of Transportation. National Highway Traffic Safety Administration. Proposed Rule Would Mandate Vehicle-to-vehicle (V2V) Communication on Light Vehicles, Allowing Cars to 'talk' to Each Other to Avoid Crashes. 2016.
[8] National Highway Traffic Safety Administration. "Federal motor vehicle safety standards: vehicle-to-vehicle (V2V) communications." *Federal Register* 79, no. 161 (2014): 49270-49278.
[9] United States of America. Department of Transportation. National Highway Traffic Safety Administration. *Federal Motor Vehicle Safety Standard (FMVSS), No.* 150. 2017.
[10] United States of America. Department of Transportation. National Highway Traffic Safety Administration. *Federal Motor Vehicle Safety Standard (FMVSS) Preliminary Regulatory Impact Analysis, No.* 150. 2017.

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

year) in the United States occur between light-weight vehicles. Assuming full adoption of V2V communication capabilities by the 2023 mandate, the NHTSA predicts that this technology would, on an annual basis:

- Prevent between 439,000 and 615,000 crashes;
- Save 987 to 1,366 lives;
- Reduce 305,000 to 418,000 injuries; and
- Avert damage to 537,000 – 746,000 vehicles.[11]

A major impediment to DOT realizing these benefits, including those resulting from other communication capabilities alluded to in this request for comment as V2X technologies, is the lack of advanced telecommunication infrastructure to support these V2X capabilities.

Existing wireless networks used to communicate via computers and smart phones were not designed with bandwidth to support the massive quantity of data that automotive systems would need to communicate. Instead, as DOT alludes to in this request, a new paradigm of connected cars will require a network with greater data processing capacity. Large quantities of complex data are generated when manufacturers train autonomous driving systems to handle various driving conditions before market entry and when consumers operate autonomous vehicles on the road. There are no universal standards for how information will be shared between manufacturers and users or how systems will be securely linked into a broader network including other vehicles on the road, traffic devices, and pedestrians.

Beyond these technical challenges there remain several matters of public policy regarding V2X technologies which the Duke SciReg Lab seeks to bring to the attention of DOT for consideration and further improvement. Specifically, we are concerned with issues of data privacy and cybersecurity of a connected transportation system. We also identify the need for

[11] *Id.*

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

further research and consideration of how motorcycles and other non-traditional vehicles, as well as pedestrian, will be engaged in the V2X systems. These factors have not been comprehensively considered in DOT's past decade of inquiry into V2X technologies.

Comment Response

a. Data Privacy Concerns Regarding V2X Communications

The United States does not have a comprehensive federal data privacy regime similar to the European Union's General Data Protection Regulation (GDPR). Instead, industries in the United States operate under a patchwork of federal and state privacy laws specific to certain subject matters, such as the federal Health Insurance Portability and Accountability Act (HIPAA), which protects patient health information, and the Family Educational Rights and Privacy Act (FERPA), which protects student educational information. There is no similar federal or state law that specifically covers data generated and collected by vehicles. As vehicles continue to collect and transmit more data about users and the world around them through V2X communications (as well as V2V, V2I and V2P communications) – and as 5G technology allows faster transfers of more data between more devices[12] – it becomes increasingly important to protect individuals' privacy.

i. The Increasing Prevalence of V2X Communications Technology Raises New Data Privacy Concerns

[12] https://www.technologyreview.com/s/612874/the-real-reason-america-is-scared-of-huawei-internet-connected-everything/?utm_medium=tr_social&utm_campaign=site_visitor.unpaid.engagement&utm_source=twitter

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

As cars become increasingly automated, they will gather increasing amounts of sensitive data about individuals inside and outside the cars. V2X-enabeled vehicles may track where the car is driven, record activity within the car through cameras and microphones, collect physical and biometric information about the driver, collect information from third-party devices connected to the car, such as smartphones, and collect information about pedestrians and other vehicles outside the car.[13] All of this information may be sent to the car's manufacturer or a third party through V2X communication technology.[14]

There are increasing incentives for car manufacturers to collect and share data through V2X communications. Car manufacturers are looking to this mass-scale data collection as a new business model. General Motors ran a pilot program in which "90,000 drivers in Chicago and Los Angeles agreed to have their car radio listening habits tracked to assess the potential relationship between what they listen to and what they buy."[15] The CEO of Ford Motor Company recently highlighted the "monetizing opportunity" of its 100 million customers.[16] Monetization of data collected through vehicles may lead to 450 to $750 billion in additional revenue for car manufacturers by 2030.[17] Car manufacturers may generate revenue directly by selling data-dependent products, features, and services to customers and by "[l]everaging car data to push individual offerings to customers."[18] By sending data from cars to their

[13] https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf
[14] https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

[15] https://www.freep.com/story/money/cars/2018/11/13/ford-motor-credit-data-new-revenue/1967077002/
[16] *Id.*
[17] https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/monetizing%20car%20data/monetizing-car-data.ashx
[18] *Id.*

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

manufacturers and third parties, V2X communications technology and 5G technology will allow for the collection and transfer of far more data.

Beyond collecting information on drivers, cars will increasingly collect information on pedestrians (V2P) and vehicles (V2V) outside of the car and may share that information with car manufacturers and third parties through V2X communications. Automated vehicles are increasingly equipped with laser imaging, detection and ranging (LIDAR) sensors, radar, ultrasonic sensors, and cameras.[19] V2P technology will also allow cars to directly connect to pedestrians' mobile devices, including by "pinging" those devices to detect a pedestrian's location.[20] The data gathered by all of these sensing technologies, if stored by the car manufacturer or a third party, would provide a wealth of locational information to businesses, data brokers, and law enforcement. The pedestrians and other drivers captured by these V2P and V2V technologies would have no way to be notified of or meaningfully consent to the collection of their information, nor would they have a say in how that information would be used by automakers or third parties. For instance, will a pedestrians' walking on the street with their phone be regarded as implied consent? These and other privacy questions have been left unanswered.

ii. DOT Can Take the Lead in Coordinating Efforts to Ensure Data Privacy in V2X Communications

[19] https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf
[20] https://www.its.dot.gov/press/2015/v2p_tech.htm

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

While DOT, through the NHTSA, asserts that it "takes consumer privacy seriously,"[21] NHTSA has nonetheless taken the position that the Federal Trade Commission (FTC) "is the primary Federal agency responsible for protecting consumer privacy."[22] DOT, however, is still the lead federal agency addressing automated vehicle activities,[23] of which V2X communications are an integral part.[24] Yet, the Government Accountability Office has reported that "NHTSA has not clearly defined its roles and responsibilities as they relate to the privacy of vehicle data," and has recommended that NHTSA do so.[25] DOT, as the agency leading policy efforts behind automated vehicles and V2X communications, should accordingly take the lead in coordinating with relevant federal agencies to ensure data privacy in V2X communications and clearly communicate that role to the automated vehicle and V2X communities.

In June, 2017, the FTC and NHTSA held a workshop on "Privacy and Security Issues Associated with Current and Future Motor Vehicles."[26] The workshop brought together stakeholders from the automated vehicle community to discuss data privacy and cyber security concerns regarding V2X communications.[27] Following the workshop, the FTC produced a summary of "Key Takeaways," highlighting concerns about the collection of "sensitive personal data" and the "secondary, unexpected uses of such data."[28] Neither the FTC nor DOT, however,

[21] https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy
[22] *Id.* Notably, NHTSA omitted data privacy from its revised federal guidance on automated vehicles. *Compare* https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, *with* https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.
[23] https://www.transportation.gov/AV
[24] https://www.transportation.gov/v2x
[25] https://www.gao.gov/products/GAO-17-656
[26] https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf
[27] https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf
[28] https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

has acted to address these concerns. A search of the FTC's website reveals that the FTC has not published any guidance regarding V2X communications, while DOT's website directs data privacy inquiries to the FTC's website.[29] This gap in data privacy guidance on V2X communications demonstrates a need for the federal government to establish a coordinated response from the relevant federal agencies.

In addition to the federal government's role in establishing a coordinated multi-agency response to data privacy concerns in V2X communications, the private sector is an important stakeholder in establishing an effective structure. For example, the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers have Consumer Privacy Protection Principles for Vehicle Technologies and Services, which do not yet effectively address the privacy issues raised by V2X.[30] In this document, which was submitted to the FTC in 2014, major automakers in the U.S. market committed to a framework of principles meant to protect "personal information collected through in-car technologies."[31] These principles include

[29] https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy
[30] https://autoalliance.org/wp-content/uploads/2017/01/Auto_Alliance_Global_Automakers_Letter_to_FTCRE_Privacy.pdf
[31] *Id.*

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

transparency,[32] choice,[33] respect for context,[34] data minimization,[35] data security,[36] integrity & access,[37] and accountability.[38]

While the automakers' adoption of these principles is a laudable effort to protect individuals' data privacy in V2X communications, the principles are deficient in several ways. First, the principles only apply to data collected from the owner or "registered user" of a car.[39] The principles thus do not protect information collected about passengers in the car, vehicles outside of the car, or pedestrians outside of the car. Under current policies, none of these individuals will be notified of or meaningfully consent to the collection of their information, nor do they have a say in how that information is used by automakers or third parties. Furthermore, only automakers have committed to these principles.[40] The principles thus do not apply to technology companies or other third parties that collect data through V2X communications or

[32] "Participating Members commit to providing Owners and Registered Users with ready access to clear, meaningful notices about the Participating member's collection, use, and sharing of Covered Information." *Id.*
[33] "Participating members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information." *Id.*
[34] "Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information." *Id.*
[35] "Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes." *Id.*
[36] "Participating Members commit to implementing reasonable measures to protect Covered Information against unauthorized access or use." *Id.*
[37] "Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to offering Owners and Registered Users reasonable means to review and correct Personal Subscription Information that they provide during the subscription or registration process for Vehicle Technologies and services." *Id.*
[38] "Participating Members commit to taking reasonable steps to ensure they and other entities that receive Covered Information adhere to the Principles." *Id.*
[39] A registered user is "[a]n individual other than an Owner who registers with, and provides Personal Subscription Information to, a Participating Member in order to receive Vehicle Technology and Services that use Covered Information." *Id.*
[40] *Id.*

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

receive information collected thereby. Finally, adherence to these principles is voluntary[41] and the principles are subject to change.

Federal efforts to address data privacy concerns in other emerging technologies provide several models for DOT in coordinating multi-agency efforts to address data privacy concerns in V2X communications. First, the National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, issued the "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" as part of a multi-stakeholder effort to address privacy concerns surrounding unmanned aircraft systems (UAS).[42] Second, National Institute of Standards and Technology (NIST), another part of the Department of Commerce, has designed a cross-enterprise "Privacy Framework", which might be suitable to address V2X communications.[43]

In a related field, President Trump's recent Executive Order regarding the development of artificial intelligence emphasizes the importance of federal agencies' commitment to protecting data privacy.[44]

b. V2X Cybersecurity Concerns

As the DOT's Notice of Request for Comment suggests, the future of V2X technologies will require upgraded and/or new communications infrastructure, such as the 5G spectrum which promises to increase connectivity speeds anywhere from 10 to 100 times as fast as current

[41] *Id.*
[42] https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf
[43] https://www.nist.gov/sites/default/files/documents/2018/09/04/privacyframeworkfactsheet-sept2018.pdf
[44] https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

cellular technology[45], to enable the transfer of data among connected devices. While this increased connectivity promises an evolution in transportation, there has also been an increased concern about an evolution in cybersecurity threats and an increase in our transportation system's vulnerabilities .[46] For instance, the increased connectivity and speed from 5G technologies could also be used by compromised devices (which could include V2X devices as well all other connected devices) to perform Distributed Denial of Service Attacks directed to cripple business or infrastructure devices.[47] In other instances, transportation cyber security threats have also resulted in severe economic and violent consequences. For example, in 2009, vulnerabilities in a single computer being used to control traffic signals in Maryland resulted in gridlocks causing commuters, emergency services, and critical consumer supply-chains in the area massive delays.[48]

As evidence of DOT's consideration of these threats, in 2014, DOT requested information[49] regarding Security Credential Management Systems and, in 2016 published of cybersecurity best practices[50] as a means of standardizing cyber security protections for a

---

[45] "Everything You Need to Know About 5G." IEEE Spectrum: Technology, Engineering, and Science News. January 27, 2017. Accessed February 25, 2019. https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g.

[46] "5G Security Concerns Persist with New Research Pointing to Critical Flaw." IT PRO. February 01, 1970. Accessed February 25, 2019. https://www.itpro.co.uk/mobile/32893/5g-security-concerns-persist-with-new-research-pointing-to-critical-flaw.

[47] Mantas, Georgios, Nikos Komninos, J. Rodriuez, Evariste Logota, and Hugo Marques. "Security for 5G communications." (2015): 207-220.

[48] Halsey, A. Traffic Signals Disrupted, Creating Chaos in Montgomery. The Washington Post, November 5, 2009.

[49] *See* NHTSA, *Vehicle-to-Vehicle Security Credential Management System*, Request for Information, 79 Fed. Reg. 61927 at 61929 (2014).

50 United States of America. Department of Transportation. National Highway Traffic Safety Administration. Cybersecurity for Modern Vehicles. 2016.

connected transportation system. What is lacking from these earlier efforts is the need to harmonize and coordinate DOT's efforts to fend off cybersecurity threats with those of other Federal agencies. Similarly, there is currently no system to coordinate with other agencies to stay up to date in its cyber security efforts or to ensure that DOT and other Federal agencies can maintain the critical cyber security workforce to ensure the Nation's security as new cybersecurity threats emerge and evolve.

i. Harmonizing DOT Cybersecurity Efforts Across the Government

In December 2015, then-President Obama signed the nation's first comprehensive cybersecurity coordination bill for the Federal government, the Cybersecurity Information Sharing Act (CISA) of 2015. This law coordinated efforts of both the private and public sectors to share cyber threat information and defense strategies as well as designated seven federal agencies to lead these efforts and define best practices and standards for participating entities to follow.[51] These seven agencies were the Departments of Homeland Security (DHS), Justice (DOJ), Defense (DOD), Commerce (DOC), Energy (DOE), and the Treasury, and the Office of the Director of National Intelligence (ODNI). Significantly, DOT was not designated as part of this effort.

As the designated head of this consortium of agencies, DHS and DOJ lead in these efforts. CISA also requires that DHS and DOJ coordinate with DOD and ODNI to develop policies for sharing information about cyber threats and defensive strategies for federal, public, and private entities alike. Further, the act required these four agencies to coordinate the

[51] Cybersecurity Act of 2015 §§ 101–407, 6 U.S.C. §§ 1501–33 (2015)

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

development of these strategies with DOC, DOE and the Treasury while also consulting with the remaining agencies to devise guidelines to protect privacy and civil liberties.

Despite DOT's clear interest and experience in establishing best practices for preserving cybersecurity in a connected transportation system, it has not been included in this Act. We do recognize that as recent as May of 2018, DOT's Volpe National Transportation Systems Center has coordinated with DHS' Science and Technology Directorate to create a cyber security primer for connected vehicle fleet managers across the federal government.[52] However, as a matter of efficiency and public transparency, we believe that these partnerships, such as between the DOT's Volpe Center and DHS, should be codified and held to the same standards of upholding civil liberties, such as rights to privacy indicated in the section above, as those originally outlined by CISA.

DOT's cybersecurity guidance documents have not been updated to follow the advice of the National Cooperative Highway Research Program and Transit Cooperative Research Program of the National Academies transportation cyber security primer.[53] Specifically, DOT does not currently provide instruction to public and private connected transportation system stakeholders direction on creating documents such as business continuity plans, crisis communication plans, and disaster recovery plans in the unfortunate event that our current cybersecurity measures fail.[54]

52 "Snapshot: DHS, DOT Partner on Government Vehicle Telematics." Department of Homeland Security. May 15, 2018. Accessed February 25, 2019. https://www.dhs.gov/science-and-technology/news/2018/05/15/snapshot-dhs-dot-partner-government-vehicle-telematics.

53 National Research Council. National Cooperative Highway Research Program and Transit Cooperative Research Program. Protection of Transportation Infrastructure from Cyber Attacks: A Primer. 2016.

54 *Id.*

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

ii. **Government Wide Shortage of Cybersecurity Officials**

Undergirding these considerations is the critical scarcity of cybersecurity specialists available to the government. In 2013, the National Academies set out to assess the Nation's challenges and prospects for ensuring a strong cybersecurity workforce. At the time of the Academies' consideration, before the prospect of a nationally connected and vulnerable transportation system, there were approximately as few as one cybersecurity professional for every twenty government and business entities with cybersecurity vulnerabilities.[55] Beyond this impending connected transportation paradigm, the emergence of connected devices beyond transportation, or the "Internet of Things", indicates that the need for ensuring a cybersecurity will continue to be of national security and economic interest.

As such, we believe that there is a need for the DOT to coordinate and prioritize its efforts to ensure an adequate workforce is available to provide cybersecurity specialists for a nationally connected transportation system. Beyond budgeting to provide competitive cybersecurity wages to incentivize the cybersecurity job market, the DOT can also be heavily invested in the development of cybersecurity workers and researchers within professional organizations and academia. For example, as the National Academies' report suggests, DOT could help fund certification or formal education programs with candidate institutions in a similar manner as Congress' proposed Transportation Workforce Modernization[56] and Unmanned Aircraft Systems Collegiate Training Initiative Program[57] Acts.

[55] National Research Council. *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. National Academies Press, 2013.
[56] https://www.govinfo.gov/app/details/BILLS-115hr6200ih
[57] https://www.govinfo.gov/content/pkg/BILLS-115hr7044ih/pdf/BILLS-115hr7044ih.pdf

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

By coordinating with Congress and other agencies with vested interests in the future of the nation's cybersecurity workforce, DOT can develop similar initiatives to ensure the safety and integrity of a national connected transportation system by investing in the country's greatest assets its people.

c. Connected Vehicles and People

Despite the DOT's prediction of a connected transportation system drastically reducing the number of vehicle to vehicle fatalities, a comprehensive consideration of how these changes may affect pedestrian safety has largely been absent. Just as motorcycles were neglected in its analysis, DOT's preliminary regulatory impact analysis of its Federal Motor Vehicle Safety Standard, No. 150, does not include predictions of pedestrian safety.[58] This lack of consideration is particularly striking as 2018 marked the second year in a row in which pedestrian fatalities were at a 25-year high according to the Governors Highway Safety Association.[59]

As we will review in the following paragraphs, the research of Amir Rasouli and John K. Tsotsos provides a comprehensive survey of research on pedestrian and intelligent vehicle interactions and demonstrates the likely correlation between this uptick in pedestrian fatalities and with connected vehicles equipped with autonomous control and communication systems.[60]

A major concern addressed in the research is the growing "social interaction void", as drivers, and their attention, are being replaced by imperfect automated systems. Due to the myriad of factors that influence road users (culture, weather, sobriety, etc.), the safe and efficient

[58] United States of America. Department of Transportation. National Highway Traffic Safety Administration. Federal Motor Vehicle Safety Standard (FMVSS) Preliminary Regulatory Impact Analysis, No. 150. 2017.
[59] https://www.ghsa.org/sites/default/files/2018-02/pedestrians18.pdf
[60] *See* Rasouli, Amir, and John K. Tsotsos. "Autonomous vehicles that interact with pedestrians: A survey of theory and practice." *arXiv preprint arXiv:1805.11773* (2018).

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

operation of vehicles currently requires human attention to monitor the autonomous systems that are incapable of accounting for the complexities and ambiguities faced on the road.[61] For instance, pedestrians wanting to cross the road where designated crosswalks and signals are not available often rely on visual and physical communication with drivers to know when it is safe to cross.[62] As these scholars note, studies of autonomous vehicles have shown that the vehicles' lack of programed social understanding often exacerbate the ambiguity of such scenarios, drastically increasing risk to pedestrians and passengers alike.[63]

To avoid such ambiguities and to ensure the safety of our nation's roadways for all its users, there is a need for the DOT to consider Amir Rasouli and John K. Tsotsos' Autonomous Vehicles that Interact with Pedestrians: A Survey of Theory and Practice"[64] as the seed of a comprehensive research agenda for better understanding and ensuring the safety of pedestrians in a connected transportation system. Specifically, we see that the DOT could consider and support the work of behavior psychologists who study what factors influence road use including

---

[61] A. Rasouli, I. Kotseruba, and J. K. Tsotsos, "Understanding pedestrian behavior in complex traffic scenes," *IEEE Transactions on Intelligent Vehicles*, vol. 3, no. 1, pp. 61–70, 2018.
[62] I. Wolf, "The interaction between humans and autonomous agents," in *Autonomous Driving*, 2016, pp. 103–124.
[63] S. E. Anthony, "The trollable self-driving car," On- line, 2017-05-30. [Online]. Available: http : / / www.slate.com / articles/technology/future tense/2016/03/google self driving cars lack a human s intuition for what other drivers.html and M. Richtel, "Google's driverless cars run into problem: Cars with drivers," Online, 2017-05-30. [Online]. Available: https : //www.nytimes.com/2015/09/02/technology/personaltech/google- says- its-not-the-driverless-cars-fault-its-other-drivers.html? r=2

[64] Rasouli, Amir, and John K. Tsotsos. "Autonomous vehicles that interact with pedestrians: A survey of theory and practice." *arXiv preprint arXiv:1805.11773* (2018).

pedestrians' demographics[65], road conditions[66], social factor[67], and traffic characteristics[68]. In addition to supporting and considering research in these areas, we also advise DOT to invest in strategies to ensure this research informs how intelligent and connect vehicle systems are developed. Further, DOT can also invest in the research and development of vehicle-to-pedestrian (V2P)[69], Vehicle-to-infrastructure (V2I) and Infrastructure-to-pedestrian (I2P) technologies such as vehicular visual intent displays such as LED lights[70] or projectors[71]. Additionally, just as DOT can consider and research how pedestrians respond to automated systems in vehicles, we also see that the DOT can fund research directed towards better understanding how pedestrians interact with automated V2P and I2P systems that may also be influenced by culture, demographics, road conditions, etc.

---

[65] J. Cohen, E. Dearnaley, and C. Hansel, "The risk taken in crossing a road," *Journal of the Operational Research Society*, vol. 6, no. 3, pp. 120–128, 1955.
[66] W. A. Harrell, "Factors influencing pedestrian cautiousness in crossing streets," *The Journal of Social Psychology*, vol. 131, no. 3, pp. 367– 372, 1991.
[67] A. Willis, N. Gjersoe, C. Havard, J. Kerridge, and R. Kukla, "Human movement behaviour in urban spaces: Implications for the design and modelling of effective pedestrian environments," *Environment and Planning B: Planning and Design*, vol. 31, no. 6, pp. 805–828, 2004.
[68] G. Jacobs and D. G. Wilson, "A study of pedestrian risk in crossing busy roads in four towns," *Rrl Reports, Road Research Lab/UK/*, 1967.
[69] A. Hussein, F. Garc´ıa, J. M. Armingol, and C. Olaverri-Monreal, "P2V and V2P communication for pedestrian warning on the basis of autonomous vehicles," in *ITSC*, 2016, pp. 2034–2039.
[70] T. Lagstrom and V. M. Lundgren, "AVIP-autonomous vehicles in- teraction with pedestrians," Master's thesis, Chalmers University of Technology, Gothenborg, Sweden, 2015.
[71] "Overview: Mercedes-Benz F 015 luxury in motion," Online, 2017-06-30. [Online]. Available: http://media.daimler.com/ marsMediaSite / en / instance / ko / Overview - Mercedes - Benz - F - 015 - Luxury- in- Motion.xhtml?oid=9904624

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

d. V2X Considerations for Non-traditional Light Vehicles

Like the lack of consideration of the impact on pedestrians, motorcycles and other non-traditional vehicles are not fully considered in the DOT's original V2X inquiry. In addition to pedestrians not being considered in DOT's preliminary regulatory impact analysis of its Federal Motor Vehicle Safety Standard, No. 150, neither were motorcycles nor other non-traditional lightweight vehicles.

Over the past several decades, DOT's and other roadway safety institutions have recognized the safety threats faced by motorcyclists. Even with drivers fully in control of their vehicles, motorcyclists face disproportionately high rates of traffic safety risks than others on the road.[72] With the added concerns highlighted in the previous section of the increasing "social interaction void" in an automated and connect transportation system, the need for research and regulatory consideration of these new risks for motorcyclists and operators of non-traditional vehicles has never been greater.

Though there is a lack of comprehensive research supporting whether motorcycles and similar vehicles face increased risks in a connected transportation system, preliminary studies depict a grim picture. Research conducted by Dynamic Research, a consultant testing the fidelity of connected and autonomous driving components has compared the rates at which its test vehicles can detect motorcycles compared to a standard sedan-sized vehicle. While the test vehicles could successfully detect and provide warning of other four-wheeled vehicles in more than 95% of trials, over 40% of trials with a standard motorcycle resulted in either a late alert or no alert at all on the connected vehicle.[73] These findings suggest that even though connected

[72] https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812353
[73] https://www.cycleworld.com/can-autonomous-cars-detect-motorcycles

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU

vehicles may limit the amount of car-on-car crashes, the opposite could be true for motorcyclists and the like.

To ensure that a new paradigm of connected vehicles is an improvement for all travelers, the DOT could reconsider its mandate of connected vehicles until it has fully considered the implications to all drivers and incorporated motorcycles in its V2X testing and standard-setting. Further, we see that the DOT could coordinate these efforts with private and public stakeholders, such as the Connected Motorcycles Consortium, American Motorcycle Association, and the European Association of Motorcycle Manufactures.

Conclusion

As vehicles become increasingly connected to other vehicles, pedestrians, and infrastructure through V2X communications, new issues arise implicating individual privacy, security, and safety. This Comment has raised several of such issues for which DOT has yet to issue guidance and which may benefit from inter-agency regulatory efforts. While perhaps less visible now, these issues may have significant consequences for individual privacy, security, and safety if left unaddressed and if not considered in the design of V2X communications regulations. DOT and its sister agencies may therefore be able to mitigate these issues by addressing them before V2X communications technologies become more even prevalent in vehicles and transportation infrastructure in the United States.

304 RESEARCH DRIVE • BOX 90222 • DURHAM, NC 27708-0222 • (919) 668-0790 • SCIENCEANDSOCIETY.DUKE.EDU