NISKANEN CENTER

Public Interest Comment

Comments submitted to the National Highway Traffic Safety Administration in the Matter of:

Proposed Rules Mandating Vehicle-to-Vehicle Communications Technology for Light Vehicles

Ryan Hagemann
Director of Technology Policy
The Niskanen Center

Submitted: April 12, 2017
Docket No. NHTSA-2016-0126

Executive Summary

With each passing day, the world is becoming more interconnected. Digital communications channels have helped connect much of the world, upending traditional means of connectivity. Now, those systems and technologies are poised to begin disrupting the transportation sector. Unfortunately, the government has imperiled a future of connected and autonomous vehicles with its proposed dedicated short-range communications (DSRC) standard for vehicle-to-vehicle (V2V) communications.

Mandating DSRC as the national standard will have numerous unintended consequences for ongoing innovation in connected and autonomous vehicles. Additionally, there remain many outstanding concerns related to cybersecurity, interoperability, spectrum, and other issues. As a result, the Niskanen Center urges the National Highway Traffic Safety Administration to temporarily suspend this rulemaking proceeding until a more thorough assessment of the costs and benefits, as well as an analysis of its impact in light of Executive Order 13711, can be completed.

Introduction

The Niskanen Center wishes to express its concern regarding the National Highway Traffic Safety Administration's (NHTSA) current proposal to mandate dedicated short-range communications (DSRC) as the standard of choice for vehicle-to-vehicle (V2V) communications. What follows is a brief overview of some of those concerns, followed by an alternative recommended course of action for ensuring public safety in an era of connected and automated vehicles.

To begin, however, we wish to very briefly draw the Agency's attention to the interoperability issues associated with DSRC.

We will confine our remarks on this issue by simply noting that interoperability standards do not need to be mandated by federal regulators in order to achieve optimal outcomes. Indeed, one need look no further than the Internet's TCP/IP standard, developed and implemented outside the purview of federal regulators, for an example of a global technological phenomenon in which standards are set by voluntary cooperation and compromise among interested parties in the commercial sector and civil society.[1] We do not wish to belabor this point, however, as other commenters have already discussed this issue in their own comment filings. We direct the Agency's attention to those separate submissions for a more robust discussion of the interoperability issues associated with DSRC.[2]

Another worrisome issue with interoperability standards in particular, and DSRC more broadly, is the potential for incentivizing technological lock-in—that is, disincentivizing continuous and iterative innovation in what constitutes "best" in V2V by mandating one particular, and anachronistic, set of standards.

Technological Lock-in

First generation technological lock-in is a paramount concern with regards to V2V communications standards. Given rapid changes in technology and associated best practices and standards, it is difficult to understand how mandating the deployment of a technological standard that is long outdated will impact future developments in V2V communications. As noted by Ron Adner and Daniel Levinthal:

> *Managerial interest in emerging technologies hinges on the promise these technologies hold for their mature states. However, the path to technological maturity holds great*

[1] *See generally* Milton L. Mueller, "Networks and States: The Global Politics of Internet Governance," The MIT Press (Cambridge, MA), 2010.

[2] In particular, we note the discussion on interoperability concerns laid out in comments from the Competitive Enterprise Institute and Mercatus Center. *See* Marc Scribner, "Comments of the Competitive Enterprise Institute In the Matter of Federal Motor Vehicle Safety Standards; V2V Communications," Competitive Enterprise Institute, Docket No. NHTSA–2016–0126, submitted APril 12, 2017, https://cei.org/sites/default/files/Marc%20Scribner%20-%20Comments%20to%20NHTSA%20on%20V2V%20NPRM.pdf.

> *uncertainty. As a result, a primary challenge in managing technological emergence is how to structure development activities before the full character of the technology and of its market relevance is established.*[3]

NHTSA's DSRC mandate would lock-in V2V communications standards along a path-dependant trajectory that is premised on long-outdated technology—and long before the "full character of the technology and of its market relevance is established." The authors go on to point out that, as in new genetic species, new emerging technologies "undergo periods of evolution and revolution. They involve technological development and the transfer of the technology to new domains of application."[4] Such considerations should be weighed carefully in order to avoid locking innovators into an archaic standard that already has significant competition in the form of advanced sensor technologies and developments in radar, such as LIDAR. While technological lock-in is concerning, the spectrum lock-in issue also warrants a reconsideration of this DSRC mandate.

The need for flexible-use spectrum hasn't been given a detailed considered treatment in the promulgation of these standards. Spectrum allocated in 1999 has been reserved for the development of DSRC, with the effect of crowding out potentially innovative uses. The rise of 5G networks and LTE as alternative means of V2V communications raises concerns that the dedicated spectrum band set aside for DSRC use is not being leveraged to its highest valued use. While it is understandable that the Clinton-era Federal Communications Commission led it to make an educated guess that the 75 MHz in the 5.9 GHz band was appropriate for DSRC at the time, delayed implementation has resulted in spectrum that has gone unused and unavailable for potentially innovative, commercially valuable uses.[5]

Cybersecurity and Safety

We live in an age of ubiquitous connectivity, where the Internet of Things is starting to connect the digital data flows of cyberspace to the analog world. Security and privacy are of paramount concerns. In a future world of interconnected autonomous transportation networks, hacking a vehicle that individuals have no personal control over is a scary thought. It's scarier still that the DSRC standard that NHTSA is mandating fails to plug those security gaps.

For instance, as cybersecurity expert Alex Kreilein noted in a recent report on the technical issues with DSRC, "the addition of DSRC exposes a *new additional* attack surface to vehicles which may already be vulnerable through different means. Moreover, the security and privacy vectors that are specific to DSRC

---

[3] Ron Adner and Daniel A. Levinthal, "The Emergence of Emerging Technologies," *California Management Review*, October 2002, p. 23-24, https://www.researchgate.net/publication/228393183_The_Emergence_of_Emerging_Technologies.

[4] Ibid.

[5] Flexible-use spectrum holds the possibility of contributing to immense consumer benefits, and the more that is hoarded by government agencies (or in the case of DSRC, earmarked for outdated and unleveraged technologies), the less that is available for other uses. *See generally* Brent Skorup, "The Importance of SPectrum Access to the Future of Innovation," Mercatus Center, December 2016, https://www.mercatus.org/system/files/skorup-spectrum-access-future-innovation-mop-v2.pdf.

increase the vulnerabilities of vehicles."[6] He identifies numerous technical security gaps in the standard's architecture, from its failure to compartmentalize basic safety messages in separately masked channels to its vulnerability to spoofing, jamming, and distributed denial of service (DDoS) attacks. In short, Kreilein's report concludes:

> *Empirical security research already shows the general lack of security in vehicles. DSRC, as presently conceived, would make matters worse. It presents a new attack surface with special considerations, given its integration into critical control systems. The absence of security frameworks or a compliance regime risks life and safety. ... Without a framework, the ills of the broader IT market will be realized in vehicles, privacy and security will be risked, and the costs to security will not be easily controlled, disproportionately harming those with the least amount of economic agency.*[7]

The Department of Transportation's own analysis doesn't fare much better for DSRC. In its 2015 report on the Safety Pilot Program, the Department concluded that its program was, overall, "a major success" and recommended moving forward with recommendations requiring V2V communications standards for light vehicles.[8] However, if one reads through the report carefully, it is difficult to ascertain how the Department reached such a conclusion. It cites numerous cost overruns, timeline delays, and technical failures throughout the rudimentary pilot deployment of the technology. For a report that purports to assess the readiness of DSRC-equipped connected vehicle safety applications for national deployment, the ultimate conclusion appears to be at odds with the evidence of what actually transpired.

In addition, a 2014 NHTSA report on V2V communications noted the necessary baselines for what would constitute a successful V2V system, arguing:

> *the basis of a relevant V2V security system is "trust"—a requirement that thousands of data messages will be authenticated, in real-time, as coming from a trusted (if unknown) source. It is also a critical element in achieving interoperability—that vehicles of different make/model/year will be able to exchange trusted data without pre-existing agreements or altering the actual vehicle designs.*[9]

On both the interoperability and security front, in conjunction with the results (but not conclusion) of the Safety Pilot Program report, DSRC fails the basic test of what constitutes a "relevant" and reliable V2V system. The standard cannot communicate with non-DSRC-equipped vehicles and adds layers of insecurity that creates additional distrust in the cybersecurity

---

[6] Alex Kreilein, "Security Considerations for Connected Vehicles and Dedicated Short Range Communications," SecureSet report, March 2017, p. 2, https://securesetaccelerator.com/vehicle-security.
[7] Ibid., p. 14.
[8] "Safety Pilot Model Deployment: Lessons Learned and Recommendations for Future Connected Vehicle Activities," FHWA-JPO-16-363, September 2015, https://ntl.bts.gov/lib/59000/59300/59361/FHWA-JPO-16-363.pdf.
[9] "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," National Highway Traffic Safety Administration, Report No. DOT HS 812 014, August 2014, p. 158, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf.

ecosystem. For these reasons, the cybersecurity failings of DSRC makes it a less-than-ideal standard for V2V communications.

Recommendation: Focus on Autonomous Vehicle Deployment, Not V2V Mandates

Advocating for the implementation of the DSRC mandate is a poor use of NHTSA's limited time, energy, and resources. Those resources should be directed towards higher leveraged uses—especially in the wake of the current Administration's executive orders on regulatory review. The Niskanen Center concurred with the Competitive Enterprise Institute and others in a joint letter to the Department of Transportation on this point, arguing that the language of Executive Order 13771 necessitates a temporary suspension of these regulatory proceedings.

> *Executive Order 13771 directs that "for every one new regulation issued, at least two prior regulations be identified for elimination," and that the total incremental costs for all new regulations to be finalized this year "shall be no greater than zero." A temporary suspension of the proceeding would allow NHTSA to consider how it might offset the substantial costs of this controversial proposal. NHTSA estimates that mandating DSRC will cost $5 billion annually, with total costs in the year 2060 of $108 billion.*[10]

Moreover, the previously mentioned cybersecurity flaws inherent in DSRC suggest its effect on public safety will be far less pronounced than originally suggested—and possibly even deleterious to that end. Instead of focusing on this mandate, we suggest the Agency focus on its attention on the ongoing development of autonomous vehicles standards and policies. This technology, unlike DSRC, has already proven itself capable of reducing roadway fatalities at even non-fully autonomous levels.

For example, in pursuing an investigation into last year's roadway death associated with Tesla's autosteer technology, NHTSA's Office of Defects Investigation not only cleared the technology's complicity in the accident, but noted that the adoption of Tesla autosteer technology actually reduced accidents in the Model S by 40 percent.[11] Even in its relatively early stages, autonomous vehicle technology is showing strong empirical evidence that it actually helps reduce accidents and saves lives. DSRC, as discussed, has barely passed the muster of early-stage pilot deployment, and still leaves much to be desired.

Instead, we urge the Agency to focus its time and attention on continuing the multistakeholder process aimed at expediting the safe and effective deployment of autonomous vehicles on American roadways.

---

[10] Letter to Secretary Elaine Chao, Department of Transportation, April 3, 2017, https://cei.org/sites/default/files/Letter%20to%20USDOT%20on%20V2V%20April032017.pdf.

[11] National Highway Traffic Safety Administration, Office of Defects Investigation, Investigation PE 16-007, closed January 19, 2017, https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF.

That will have a far greater positive impact on public safety than the time spent implementing the costly, technologically-outdated, and already delayed implementation of the DSRC mandate.[12]

Conclusion

For the reasons discussed above, the Niskanen Center respectfully submits that NHTSA should temporarily suspend the rulemaking process for implementing the DSRC mandate. Until such time as the Agency can assess how its proposed mandate comports to the demands of Executive Order 13771, no further action towards implementation should be taken. Additionally, the many concerns associated with privacy and cybersecurity, potential technological lock-in, and interoperability and other technical difficulties still need to be addressed. Rather than pursue this mandate, NHTSA should focus the bulk of its attention and resources on finalizing its policies on autonomous vehicles to expedite their safe and expeditious deployment, which will have a far greater benefit to public safety and health than the DSRC rules.

We thank the Agency for the opportunity to submit these comments and look forward to a productive and ongoing dialogue on these matters.

[12] On the issue of autonomous vehicles, we would direct the Agency to the Niskanen Center's previous comments on this issue. *See* Ryan Hagemann, "Comments Submitted to the National Highway Traffic Safety Administration in the Matter of Federal Automated Vehicle Policy," Niskanen Center, NHTSA-2016-0090, submitted November 21, 2016, https://niskanencenter.org/wp-content/uploads/2016/11/CommentsAutonomousVehicleStandardsNHTSA.pdf.