1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

March 4, 2024

Via Electronic Mail

Dan Rabinovitz
U.S. Department of Transportation
Office of the Chief Counsel
1200 New Jersey Avenue SE
West Building Ground Floor
Room W12–140
Washington, DC 20590–0001

To Whom It May Concern,

On behalf of the Future of Privacy Forum (FPF), we are pleased to submit comments in response to the National Highway Traffic Safety Administration (NHTSA) and the U.S. Department of Transportation's (DOT) Advanced Notice of Proposed Rulemaking regarding Advanced Impaired Driving Prevention Technology.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies. FPF has worked on issues around vehicles and privacy since 2014 and has contributed substantial research and analysis to topics in the sector.

In NHTSA's roadmap toward standards for advanced drunk and impaired driving prevention technology, FPF urges the Agency to ensure that driver trust of new vehicle safety standards remains a central tenet to any standards.[2] Accordingly, FPF recommends that NHTSA:

1. Require robust privacy protections in any system that implicates personal data;
2. Provide strict accuracy standards and auditing requirements for any vehicle safety system;
3. Facilitate the creation of cybersecurity resources that protect vehicle safety systems and underlying data; and

---

[1] Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571) https://www.federalregister.gov/documents/2024/01/05/2023-27665/advanced-impaired-driving-prevention-technology (ANPRM)

[2] Throughout the comment, FPF has adopted the term "Vehicle Safety Systems" to refer to all forms of technology discussed in the ANPRM, including Driver monitoring systems, advanced driver assistance systems, and intoxication detection systems, such as DADSS.

4. Actively engage in broad consultations to understand and mitigate the potential for vehicle safety systems to perpetuate bias or increase risks for individuals or communities.

Recommendations

The D.C. Circuit Court of Appeals has noted that public cooperation is necessary for safety systems to "meet the need for motor vehicle safety."[3] Trust is an essential precondition to individuals' acceptance of new technologies.[4] Trust is particularly important in the transportation sector: studies have demonstrated that trust plays a crucial role in an individual's decision to purchase from a specific vehicle manufacturer.[5] FPF's recommendations are designed to facilitate driver trust and the adoption of vehicle safety systems while encouraging strong privacy protections throughout.

1. *NHTSA should require robust privacy protections in any system that implicates personal data.*

As vehicles drive toward the inclusion of more technology, the amount of personal data and information used to make the technology function increases. At the same time, individuals are increasingly worried about the use of their personal data and are in favor of greater privacy protections.[6] To respond to individuals' demands, privacy must be a foundational principle for any mandates regarding vehicle safety systems that use personal information.[7]

NHTSA's ANPRM specifically inquires about privacy protections regarding vehicle safety systems, focusing on the potential need for publishing a privacy impact assessment alongside a regulatory proposal. However, given the potential sensitivity of the data implicated by vehicle safety

---

[3] Pac. Legal Found. v. Dep't of Transp., 593 F.2d 1338, 1345–46 (D.C. Cir. 1979) (citing 15 U.S.C. § 1392(a) (1976))

[4] World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies,* World Economic Forum, (Nov. 15, 2022), https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/

[5] *A new measure of trust: Why it matters for automakers, and how to build it*, Deloitte Digital https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/offerings/offering-20200805-hx-trust-automakers.pdf (last visited Nov. 2, 2023).

[6] Colleen McClain, Michelle Faverio, Monica Anderson and Eugenie Park, *How Americans View Data Privacy,* Pew Research Center, (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/#:~:text=Our%20survey%20finds%20that%20a,how%20companies%20use%20people's%20data

[7] Katie Malone, *Every Car Is a Smart Car, and It's a Privacy Nightmare,* Engadget (Nov. 6, 2023), https://www.engadget.com/every-car-is-a-smart-car-and-its-a-privacy-nightmare-193010478.html.

systems, robust privacy protections are of significant importance and should be considered early in NHTSA's process and throughout the development and deployment of the technologies.[8] In addition to privacy impact assessments, potential protections should include appropriate data minimization standards; limits on data use, transfer, and processing; transparency requirements; and data deletion mechanisms.[9]

2. *NHTSA should provide strict accuracy standards and auditing requirements for any vehicle safety system.*

A mandate to install vehicle safety systems stands a high chance of deteriorating drivers' confidence in new vehicles if the systems are insufficiently accurate. A lack of appropriate accuracy requirements would impede the Agency's goal of detecting and intervening in impaired driving. Accuracy must be considered in context. For instance, vehicle safety systems should respond to a driver's detected impairment status in proportion to the system's proven level of accuracy. For example, a system that responds to a positive trigger by flashing a warning light or emitting a beeping noise may afford a lower threshold than a system that materially limits the vehicle's speed or functionality. To prevent undue harm to drivers, NHTSA must establish clearly defined requirements and standards for consistent deployment and alignment across the industry.

Accuracy standards must also include transparency requirements to ensure that a driver or other vehicle occupant understands the parameters of any vehicle safety system and can identify when a technology is working as intended. It is imperative that the understanding includes details on how technology reacts to any specific trigger and what options are available if the vehicle's response inhibits the vehicle from starting or moving. For instance, in an emergency where a driver is inaccurately flagged by the vehicle as being "impaired," the driver must know what options are available to seek medical attention, particularly if the vehicle either won't turn on or only allows limited functionality.

Finally, protections for privacy and accuracy standards are closely related and should be considered together. Stringent accuracy standards may provide increased personal autonomy

---

[8] *Privacy Impact Assessments,* U.S. Department of Transportation, https://www.transportation.gov/individuals/privacy/privacy-impact-assessments (last visited Mar. 4, 2024); see also *Safe and Effective Systems,* The White House Office of Science and Technology Policy, https://www.whitehouse.gov/ostp/ai-bill-of-rights/safe-and-effective-systems-3/ (last visited Mar. 4, 2024)

[9] *Fair Information Practice Principles (FIPPS),* Federal Privacy Council, https://www.fpc.gov/resources/fipps/ (last visited Mar. 4, 2024); *see also* Shelby Brennan et al., *The Brave New World of Third Party Location Data*, 16 J. of Strategic Security 81, 83 (2023); *see also* D. Sladović et al., Investigating Modern Cars, 2019 42nd Int'l Convention on Info. and Commc'n Tech., Elec. and Microelectronics (MIPRO) (2019), doi: 10.23919/MIPRO.2019.8756732.

and control, for instance, in preventing a driver from being labeled with an incorrect impairment condition (drowsiness, intoxication, etc.) or keeping one car occupant from being categorized by data related to another occupant. On the other hand, increased accuracy may require increased data volume or data specificity of personal information, increasing privacy risks. Increased privacy risks may also relate to a vehicle safety system's ability to detect or process information related to health status. Medical conditions may cause vehicle safety systems to return false positives for driver impairment unless properly accounted for. For example, NHTSA flags myokymia–eye twitching–as a condition that could potentially confuse driver assistance systems.[10] However, the collection of health data is likely to trigger state and federal privacy laws, such as Washington State's "My Health, My Data" Act, which provides individual rights and mandatory protections.

3. *NHTSA should facilitate the creation of cybersecurity resources that protect vehicle safety systems and underlying data.*

The evolution of connected vehicles has seen a corresponding growth in cybersecurity risks. On average, a connected vehicle takes 100 million lines of code to operate, implicating fuel injection, air conditioning, GPS/navigation, and other systems.[11] However, the more code that goes into a car, the more likely that car could contain vulnerabilities. In addition, after-market devices (e.g., insurance dongles, smartphones, and other third-party connected devices via telematics or cloud systems) directly connect to vehicle systems. If compromised, those devices can leave entire systems vulnerable to backdoors. Other (post-production) concerns include, among other things, firmware updates, cloud server access, malware, and global supply chain management.

NHTSA must consider the intricate and overlapping challenges between technical development and security considerations in a way that adapts to evolving threats specific to vehicles. In 2022, NHTSA updated its non-binding Cybersecurity Best Practices for Modern Vehicles (NHTSA Best Practices) in response to some of the cybersecurity risks of vehicles, advocating for a layered cybersecurity approach derived from leading government and private sector standards.[12] In addition to the NHTSA Best Practices, rulemaking should follow other federal guidelines, such as

[10] ANPRM at 72-73.
[11] Marius Mihailovici, *When Software Writes Software,* Porsche Newsroom, (Aug. 8, 2021) https://newsroom.porsche.com/en_US/2021/technology/porsche-engineering-when-software-writes-software-25367.html
[12] Standards include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, industry standards from the International Standard of Organization and the Society of Automotive Engineers (ISO/SAE 21434), and best practices from the Automotive Information Sharing and Analysis Center (Auto-ISAC), *Cybersecurity Best Practices for the Safety of Modern Vehicles,* National Highway Safety Traffic Administration, (2022) https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf; https://www.nist.gov/cyberframework; http://www.iso.org/standard/70918.html; https://automotiveisac.com/best-practices

the Cybersecurity and Infrastructure Security Agency's (CISA) secure-by-design principles and zero trust maturity model, which provide practical roadmaps and best practices to ensure consumer trust and secure systems.[13] The development of resources connecting federal guidelines and industry best practices with respect to the unique needs of the mobility sector can provide consistency, strong governance, and a data-centric approach to mitigating unique and fast-developing cybersecurity threats relevant to vehicle systems and the data that they process.

4. *NHTSA should actively engage in broad consultations to understand and mitigate the potential for vehicle safety systems to perpetuate bias or increase risks for individuals or communities*

There is no way to predict with certainty what could result from the deployment and use of any particular technology. However, broad technology mandates without testing and evaluation to understand how they could impact specific communities, including individuals in specific geographic regions–such as a rural community or a metropolis–can raise the specter of significant harm.[14] In establishing standards for vehicle safety systems, NHTSA must take affirmative steps to ensure a broad and inclusive consultative process that includes individuals and communities from various backgrounds and cultures.

Transportation as a concept and vehicles have a range of meanings that may change based on culture, gender, geography, socioeconomic background, or physical security, to name only a few examples. For instance, a vehicle may be a luxury in an urban environment with many transit options. At the same time, it may be the only way for an individual in a rural community to get to work, home, medical appointments, or any other location. In another show of contrast, a victim of a car accident may see vehicles as primarily an instrument of violence, whereas for an individual escaping an abusive relationship, a vehicle may be the person's only lifeline to safety.[15] In one

---

[13] *Secure-by-Design*, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/resources-tools/resources/secure-by-design (last visited Mar. 4, 2024); see also *Zero Trust Maturity Model,* Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/zero-trust-maturity-model (last visited Mar. 4, 2024)

[14] Becky Chao, Eric Null, Brandi Collins-Dexter, and Claire Park, *Centering Civil Rights in the Privacy Debate,* (Aug. 2019), https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/for-marginalized-communities-the-stakes-are-high/; see also Nicol Turner-Lee, Paul Resnick, and Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms,**May 22, 2019), https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[15] Brenda Baddam, *Technology and Its Danger to Domestic Violence Victims: How Did He Find Me?*, 28 Alb. L.J. Sci. 73, 78 (2017); *see also, e.g.*, Kashmir Hill, Y*our Car Is Tracking You. Abusive Partners May Be, Too.,* New York Times (Dec. 31, 2023), https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html (describing how a woman's

more example, people from certain privileged communities may see traffic and law enforcement officers who intervene with vehicle use as a societal imperative. In contrast, for people from black communities who are overpoliced and for whom police interventions have a significantly disproportionate chance of ending in violence, the connection of law enforcement to vehicle use may represent a significant threat. NHTSA should ensure that each perspective is considered, weighted, and accounted for in any vehicle safety system mandates.

Conclusion

The Future of Privacy Forum appreciates this opportunity to comment on these issues and NHTSA's and U.S. DOT's efforts to ensure vehicle safety and consider the implications for privacy and security in line with the additional questions.

We welcome any further opportunity to provide resources or information to assist in this vital effort. If you have any questions regarding these comments and recommendations, please contact Adonne Washington at awashington@fpf.org (cc:info@fpf.org).

Sincerely,

Adonne Washington, *Policy Counsel Mobility, Location, & Data*
Beth Do, *Christopher Wolf Diversity Law Fellow*
Niharika Vattikonda, *Health and Wellness Research Assistant*
Angela Guo, *Legal Intern*

The Future of Privacy Forum
https://fpf.org/

abusive husband used the Mercedes Mbrace app to track her location); Kristina Cooke & Dan Levine, *An Abused Wife Took on Tesla Over Tracking Tech. She Lost.*, Reuters (Dec. 19, 2023 10:48 AM EST), https://www.reuters.com/technology/an-abused-wife-took-tesla-over-tracking-tech-she-lost-2023-12-19/ (reporting how a San Francisco woman unsuccessfully sued Tesla for continuing to provide her ex-husband access to her car's technology despite a restraining order against him).