CENTER FOR DEMOCRACY & TECHNOLOGY

March 5, 2024

VIA ELECTRONIC TRANSMISSION

National Highway Traffic Safety Administration,
U.S. Department of Transportation,
1200 New Jersey Avenue SE, West Building Ground Floor, Room W12–140,
Washington, DC 20590–0001

Re: RIN 2127–AM50
Docket No. NHTSA–2022–0079 - Advanced Impaired Driving Prevention Technology

Introduction

The Center for Democracy & Technology (CDT) files these comments in response to the National Highway Traffic Safety Administration (NHTSA) Advance Notice of Proposed Rulemaking (ANPR) on Advanced Impaired Driving Prevention Technology.[1] CDT is a nonprofit public interest organization fighting to advance civil liberties and civil rights in the digital age. CDT champions policies, laws, and technical designs that empower people to use technology for good while protecting against invasive, discriminatory, and exploitative uses. CDT consistently seeks to protect and promote user privacy and calls for online platforms to be transparent and accountable, and to respect human rights.

CDT commends NHTSA for its ongoing efforts to further reduce drunk and impaired driving crashes and fatalities, and appreciates that the agency has included privacy considerations in its pursuit of reducing impaired driving. Nevertheless, CDT urges NHTSA to include robust privacy protections in its rules for impaired driving prevention technology. In particular NHTSA should impose strict limits on data collection and use to prevent widespread and government-approved privacy invasions.

Advanced Impaired Driving Prevention Technologies Will Add to the Vast Amounts of Personal Data Modern Cars are Capable of Collecting

Modern cars collect extraordinary and growing amounts of data. Cars have the power to watch, listen, and collect information through sensors including microphones and cameras, such as where people go in their cars, what drivers and passengers do and say, and also what is happening outside of and around those cars.[2] Cars also connect to a host of online services,

[1] Advanced Impaired Driving Prevention Technology, 89 FR 830 (Jan. 05, 2024), https://www.federalregister.gov/documents/2024/01/05/2023-27665/advanced-impaired-driving-prevention-technology (https://perma.cc/PW6T-S646).
[2] *See* Jen Caltrider, Misha Rykov & Zoë MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, Mozilla (Sept. 6, 2023),

whether from the original car manufacturer or third parties like Spotify or OnStar, that all collect and store data about the vehicle and its occupants.[3] As a result, cars are now able to create, maintain, and share a record of essentially every interaction drivers and passengers have with those cars.[4]

A recent Mozilla report found that every car brand examined was found to collect more personal data than necessary and use that information for reasons other than to operate the vehicle and manage manufacturers' relationship with consumers.[5] The data that cars can collect, include but are not limited to, health diagnosis data, facial geometric features, physiological characteristics, fingerprints, faceprints, photographs, user-generated content and other materials that users may submit, precise location, audio recordings of vehicle occupants, and voice recordings.[6] Further, new cars share and/or sell personal data with service providers, data brokers, and other businesses that consumers do not have relationships with or know little or nothing about.[7]

The proposed advanced impaired driving prevention technologies contemplated within the ANPR would add to the ever-growing list of data-collecting components within modern passenger vehicles. For example, the technologies under consideration can use cameras to collect data about a driver's eye movements, facial measurements, and other touch sensors to detect alcohol levels in the blood.[8] The data that would be collected by these technologies has

---

https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[3] A recent Mozilla report notes, "There's probably no other product that can collect as much information about what you do, where you go, what you say, and even how you move your body ("gestures") than your car." Jen Caltrider, Misha Rykov & Zoë MacDonald, *What Data Does My Car Collect About Me and Where Does It Go?,* Mozilla (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/; *see also* Geoffrey A. Fowler, *What does your car know about you? We hacked a Chevy to find out*, Wash. Post (Dec. 17, 2019), https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/ (https://perma.cc/KG7G-E369); Gopal Ratnam, *Your car is watching you. Who owns the data?*, Roll Call (Apr. 9, 2019), https://rollcall.com/2019/04/09/your-car-is-watching-you-who-owns-the-data/ (https://perma.cc/63JG-8DQR).

[4] *See* Caltrider et. al., *supra* n. 3.

[5] *See* Caltrider et. al., *supra* n. 2.

[6] *See* Caltrider et. al., *supra* n. 3.

[7] *See* Caltrider et. al., *supra* n. 2.

[8] The ANPR discusses a series of impaired driving detection systems developed by auto manufactures and details how these systems use a litany of sensors to determine if a driver is impaired and/or distracted. These include the following:

- Camera-based detection measures (i.e., eye gaze, eyelid/eye closure, and facial/emotional measures), as well as lane monitoring and steering input,
- Touch and breath sensors detect high levels of alcohol.
- Facial monitoring system built to monitor signs of drowsiness or distraction,
- Infrared cameras to capture driver facial and eye movements to determine if the driver keeps eyes forward, changes blinking patterns, or exhibits other signs of drowsiness.

long been considered sensitive and private data that warrants greater privacy protections.[9] Indeed, data that cars collect, including the types of data collected by advanced impaired driving prevention technologies, are the same types and categories of sensitive data that have been subject to greater privacy regulations and federal agency enforcement actions.[10] For example, the state of Illinois has long had a biometric law in place that has been enforced against several technology companies.[11] NHTSA should keep pace with current privacy protections and practices to protect against the significant overcollection of car data by ensuring robust privacy protections are in place for data collected and used by advanced impaired driving prevention technologies.

Over-collection of Data by Cars, and Its Subsequent Sharing and Use, Harms Individuals

Overcollection and overuse of data is harmful.[12] Privacy-based harms occur when companies collect, maintain, share, and use personal data for purposes unrelated to the product or service being provided.[13] Collecting and retaining more data than necessary to provide a product or

---

See Department of Transportation, National Highway Traffic Safety Administration, *supra* n. 1, at 849-851.

[9] Sensitive data includes various types of data such as health and financial data, content of communications, identification numbers, biometric information, location, and demographic information. *See e.g.*, § 2(28)(a) of the "American Data Privacy and Protection Act", H.R. 8152, 117th Cong. (2022).

[10] *See. e.g.*, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security#citation-24-p51290 (https://perma.cc/EBL9-58LL); HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (Apr. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html (https://perma.cc/JR29-BVB7); Federal Communications Commission, *FCC Chairwoman Calls on Agency to Help Stop Abusers from Using Connected Cars to Harass and Intimidate Their Partners*, (Feb. 28, 2024),https://docs.fcc.gov/public/attachments/DOC-400812A1.pdf (https://perma.cc/T5LG-WE7M).

[11] *See e.g.*, Michael Gennaro, *Privacy Class Action Over Unauthorized Voiceprint Collection to Proceed Against Meta*, Courthouse News Service (Feb. 28, 2024), https://www.courthousenews.com/privacy-class-action-over-unauthorized-voiceprint-collection-to-proceed-against-meta/; Stephen Joyce & Skye Witley, *BNSF Settles Illinois Biometric Privacy Case for $75 Million*, Bloomberg Law (Feb. 27, 2024), https://news.bloomberglaw.com/privacy-and-data-security/bnsf-settles-illinois-biometric-privacy-case-for-75-million (https://perma.cc/5UB7-CQRV); Stephen Joyce & Skye Witley, *Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling*, Bloomberg Law (May 2, 2023), https://news.bloomberglaw.com/privacy-and-data-security/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling (https://perma.cc/EY72-PLGM).

[12] *See* Lydia X. Z. Brown, Andrew Crawford, Nick Doty, et. al., *CDT Comments to FTC Regarding Prevalent Commercial Surveillance Practices that Harm Consumers*, Center for Democracy & Technology (Nov. 21, 2022), https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf (https://perma.cc/RA99-7WTM).

[13] *See e.g.*, Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 Boston U. L. Rev. 793, 831-45 (2021),

service results in large databases that can become the target of hackers or unauthorized access. Moreover, when personal data is subject to data breaches, further downstream harms like identity theft can occur. That danger is particularly acute with biometric data that reflect unchangeable characteristics such as facial measurements.

Secondary uses of data by the company itself can harm people because they have no way of knowing or understanding the implications of the use. Thus, additional harms can occur with subsequent use of data that is unknown or secretive, such as developing detailed individual profiles of people and selling the data to third parties for use in a variety of circumstances, such as targeted advertisements or training an algorithm.[14]

The over-collection and -use of biometric data in particular can be harmful and has faced legal scrutiny. For example, biometric data can trigger evictions or arrests, further criminalizing people who are already disproportionately surveilled, and for whom facial analysis has been shown to produce unreliable matches.[15] Biometric data such as facial expressions, eye contact, voice intonation, and inflection, has also harmed people when used in employment and hiring software.[16] Biometric data can also prove harmful when it is not secure. For example ID.me, a facial recognition identity verification company, allowed employees to bring home devices that carried U.S. citizens' identity data and retained biometric data longer than necessary.[17] Such practices increase the chances of data being leaked onto the internet and later used for identity theft or other harmful activities.

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222 (https://perma.cc/L5KM-NXF9); Saumya Kalia, *What is a Constant Lack of Digital Privacy Doing to Our Mental Health?*, The Swaddle (Jan. 26, 2022), https://theswaddle.com/what-is-a-constant-lack-of-digital-privacy-doing-to-our-mental-health/ (https://perma.cc/NB3P-T5RR).

[14] *See* Solove & Keats Citron, *supra* n. 13.

[15] *See e.g.* Sophia Maalsen, Peta Wolifson, Dallas Rogers, Jacqueline Nelson, & Caitlin Buckle, *Understanding Discrimination Effects in Private Rental Housing*, AHURI (Sept. 4, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916655 (https://perma.cc/2VZR-KF9J); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings Of Machine Learning Research (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (https://perma.cc/XFB4-9UMB).

[16] *Federal Judge Allows Lawsuit Against CVS to Proceed Over Alleged Lie Detector Use*, New England Biz Law Update (Feb. 23, 2024), https://newenglandbizlawupdate.com/2024/02/23/federal-judge-allows-lawsuit-against-cvs-to-proceed-over-alleged-lie-detector-use/ (https://perma.cc/FJ39-BQ2R).

[17] Caroline Haskins, *Inside ID.me's Torrid Pandemic Growth Spurt, Which Led to Frantic Hiring, Ill-Equipped Staff, and Data-Security Lapses as Tte Company Closed Lucrative Deals With Unemployment Agencies and the IRS*, Bus. Insider (Jun. 7, 2022), https://www.businessinsider.com/id-me-customer-service-workers-hiring-secuirty-privacy-stress-data-2022-6 (https://perma.cc/9UFN-LGJX); Jessy Edwards, *ID.me Lawsuit Claims Company Violates Data Storage Requirements*, Top Class Actions (Aug. 22, 2022), https://topclassactions.com/lawsuit-settlements/privacy/bipa/id-me-lawsuit-claims-company-violates-data-storage-requirements/ (https://perma.cc/E3XR-3ACH).

The advanced impaired driving prevention technologies contemplated in the ANPR are invasive. They have the capabilities of continually collecting and using data that is very personal - such as the alcohol levels in peoples' blood and sweat, eye movements, and facial expressions. The same data that informs advanced impaired driving prevention technologies can also reveal private and sensitive information about drivers and passengers.

Highly-privacy invasive cars are also unlikely to garner consumer acceptance. Many Americans do not want to be tracked and have their data collected and stored, especially when the tracking includes data about their bodies, their conversations and communications with others. A 2020 survey showed that almost 80% of people in North America expressed concern over sharing personal information with online businesses.[18] In 2019, a significant majority of Pew survey respondents were concerned about how much data about them is collected by businesses, and similar numbers believed the risks to such data collection outweighed the benefits.[19] When it comes to cars, a recent Kaspersky survey found that "71% of drivers said they would consider buying an older car or one with less technology, in order to protect their privacy and security."[20] The same survey also found that "72% of drivers are uncomfortable with the idea of an automaker sharing their data with third parties."[21]

Therefore, it is imperative for NHTSA to consider, identify, and evaluate potential privacy risks and possible harms when deciding whether to impose impaired driving technology in new cars, especially given these technologies are known to collect very sensitive data about individuals. Moreover, any rulemaking should impose robust privacy protections and mitigations to ensure that advanced impaired driving technology does not over collect or use consumer data in harmful ways.

Privacy-Protective Recommendations for NHTSA Rulemaking

NHTSA should ensure that new advanced impaired driving prevention technologies do not simply allow business as usual with invasive privacy practices such as over-collection and over-sharing of data. To decrease the likelihood of privacy harms and increasing consumer acceptance, NHTSA should require robust data collection and use limitations associated with advanced impaired driving prevention technologies.

---

[18] *Global Crisis In Trust Over Personal Data*, Worldwide Independent Network for Market Research (July 20, 2020), https://winmr.com/global-crisis-in-trust-over-personal-data (https://perma.cc/MK4L-WU57).
[19] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information (https://perma.cc/YU5V-3UPZ).
[20] Kurt Baumgartner, *Is My Car Spying on Me?*, Kaspersky Lab (2023), https://media.kasperskydaily.com/wp-content/uploads/sites/85/2024/01/10103616/13195_Driver_Survey_Report_WEB-2.pdf (https://perma.cc/F2AQ-3DXN).
[21] *Id*.

CENTER FOR DEMOCRACY & TECHNOLOGY

I. NHTSA has the Authority to Included Strong Data Privacy Protections and Limit Data Collection via Advanced Impaired Driving Prevention Technology

Robust data privacy protections are essential to any rule regulating advanced impaired driving prevention technology. The inclusion of data privacy protections will ensure that NHTSA satisfies the legal requirements of the National Traffic and Motor Vehicle Safety Act. The Act requires that standards regulating motor vehicle safety problems be "practicable."[22] To demonstrate that a proposed standard is "practicable," NHTSA must consider several factors, including technological and economic feasibility and consumer acceptance.[23] Including privacy protections will bolster consumer acceptance. A core element of consumer acceptance is trust.[24] When consumers do not trust products' and services' data practices, they are less likely to use those products and services.[25] Thus, strong data privacy protections will help NHTSA satisfy the Safety Act's requirements and the agency has authority to impose such protections.

II. NHTSA should conduct a Privacy Threshold Analysis and publish a Privacy Impact Assessment.

As an initial matter, the ANPR notes that NHTSA intends to conduct a privacy threshold analysis (PTA) to determine whether the agency should publish a draft Privacy Impact Assessment (PIA) concurrent with its issuance of a regulatory proposal that would establish performance requirements for advanced impaired driving technology.[26] CDT applauds NHTSA's intention to conduct a PTA and strongly recommends the publication of a PIA. NHTSA has issued numerous PIA's in response to other initiatives and should do so again here to demonstrate the agency's commitment to driver and passenger privacy and bolstering driver and passenger trust and acceptance of advanced impaired driving prevention technologies.[27]

Within that PIA, NHTSA should explicitly consider whether this technology is too privacy invasive, and whether alternative technologies that are less privacy-invasive would accomplish similar goals. The privacy reviews should evaluate data practices around minimization, security, and encryption like those contemplated in NHTSA's V2V Communications PIA.[28]

---

[22] 49 U.S.C. 30111(a).
[23] Department of Transportation, National Highway Traffic Safety Administration *supra* n. 1, at 837.
[24] Worldwide Independent Network for Market Research *supra* n. 18.
[25] *Id*.
[26] Department of Transportation, National Highway Traffic Safety Administration *supra* n. 1, at 855.
[27] *NHTSA Privacy Impact Assessments*, Department of Transportation, https://www.transportation.gov/individuals/privacy/privacy-impact-assessments/NHTSA (https://perma.cc/59R9-AVSC).
[28] Ryan Posten & Claire W. Barrett, *Privacy Impact Assessment, National Highway Traffic Safety Administration, Notice of Proposed Rulemaking (NPRM) on V2V Communications*, U.S. Dept. of Transportation (Dec. 29, 2016),

CENTER FOR DEMOCRACY & TECHNOLOGY

III. NHTSA should include robust driver and passenger privacy limitations related to collection, use, and retention of data by alcohol and impairment detection systems.

NHTSA is proposing to require cars to have a system in place that would involve a significant increase in the collection and use of sensitive and personal information about millions of American drivers and their passengers. NHTSA should impose strict limits on data collection and use to prevent widespread and government-approved privacy invasions from abuses of that system.

First, NHTSA should allow data collection by these systems only to the extent necessary to make a determination as to whether the driver is impaired. Allowing the collection of superfluous data about other people in the car, unrelated data about the driver, or any other data that cars are capable of collecting for any other purpose would allow car companies to abuse this new system and violate people's privacy for the company's own gain.

Second, NHTSA should require that the data collected be used only for determining whether the driver is impaired. Companies should not be allowed to use this personal, sensitive data for secondary purposes. The data also should not be sold or otherwise transferred to any third parties such as data brokers, insurance companies, or (absent a legal requirement) law enforcement.

Third, once data has been successfully used to determine whether a driver is impaired or not, that data should then be promptly deleted, unless there exists another legal duty or requirement to retain the data for longer. The determinations made by advanced impaired driving prevention technologies are temporal. They are a yes/no determination at a specific instance in time - is this specific individual attempting to operate a vehicle while intoxicated? This type of determination does not require any historical data from past operations nor does it require the creation of stored data moving forward.

Next, where practical, data used by advanced impaired driving prevention technologies should only be processed on the vehicle and, when necessary to retain such data, be retained only on the vehicle. Local data storage and processing decreases opportunities for data to be used or shared for unrelated purposes. Additionally, local data storage decreases the chance that such data will be accessed and used by individuals who do not have a need to see or have approval to see such data. Provisions like these also add to driver and passenger data privacy and trust since they know their data is not being shared with third parties and/or potentially being used for unknown and unrelated purposes.

---

https://www.transportation.gov/sites/dot.gov/files/docs/Privacy%20-%20NHTSA%20-%20V2V%20NPRM%20-%20PIA%20-%20Approved%20-%20122016.pdf (https://perma.cc/7K9Q-V2VJ).

These privacy protections will help ensure consumers accept NHTSA's proposed detection system. If people know data collection will be minimized and that data will not be retained and potentially used in unknown or unwanted ways, like to create profiles for specific drivers that could later be shared with insurance companies and/or law enforcement, they are more likely to accept detection systems.

IV. Transparency is critical for individuals to understand and trust new technologies.

NHTSA should establish effective mechanisms and requirements that inform drivers and passengers about how advanced impaired driving prevention technologies operate and how their data will be kept private. Drivers and passengers should know what data about them is being collected, why collection is necessary for the intended purpose of the detection system, how that data will be used, how long it will be retained, and how and with whom their data will be shared (though, as noted above, it should not be shared absent a legal requirement to do so).

Importantly, transparency should not be conflated with a notice and consent regime: companies should be subject to the data minimization rules set forth above and not be permitted to evade them through providing "notice" in privacy policies and the fiction that drivers and passengers have consented to whatever practices those policies contain.

Such disclosures should be conveyed in multiple ways. First, the rules should require a short, easy-to-understand disclosure. This short-from disclosure should contain enough detail to enable drivers and passengers to understand how and why their data will be collected, retained, used, and shared. Short-from disclosures should be made available to drivers and passengers in the vehicle prior to any data collection. For example, this data could be displayed on the car's infotainment system and provide top-level information and options for drivers and passengers to learn more via additional menus and windows.

In addition to the shorter and more digestible information provided to drivers and passengers in-vehicle, a second and more thorough disclosure detailing how advanced impaired driving prevention technologies collect, retain, use, and share driver and passenger data should also be required and publicly available on manufacturers' websites. That more detailed information also will enable advocates and government regulators to evaluate and ensure that advanced impaired driving prevention technologies are complying with data minimization requirements.

Conclusion

NHTSA should incorporate strong privacy protections in its Advanced Impaired Driving Prevention Technologies in any final rule. Those protections should include meaningful limits on data collection, retention, sharing, and use. We look forward to continuing to work with you to advance data privacy rules that protect drivers and passengers.