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

**July 3, 2024**

**Sent via electronic submission**

Timothy Klein
Director, Technology Policy and Outreach
Office of the Assistant Secretary for Research and Technology
Department of Transportation
1200 New Jersey Ave SE,
Washington, DC 20590

**To whom it may concern,**

On behalf of the Future of Privacy Forum (FPF), we are pleased to submit comments in response to the United States Department of Transportation's (DOT) Request for Information on Opportunities and Challenges of Artificial Intelligence (AI) in Transportation.[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices supporting emerging technologies. Of the work that we do, artificial intelligence is an issue area where FPF has years of expertise and experience.

In DOT's work to examine the potential for AI, FPF urges DOT to:

- **Consider existing federal regulations and frameworks for addressing privacy and risk in AI systems;**
- **Center privacy in the evaluation process of AI use cases in transportation; and**
- **Prioritize actions to ensure that the use of AI does not perpetuate or exacerbate harm to marginalized communities.**

## I. DOT should consider existing federal regulations and frameworks for addressing privacy and risk in AI systems.

When considering the opportunities and challenges of AI, DOT should look to existing statutory and regulatory frameworks to inform future action on AI and support alignment across the federal government. Cohesive regulatory structures provide significant benefits, both to impacted organizations, who are able to best operationalize regulatory requirements, as well as to individuals seeking to understand their rights and how to exercise them. An examination of

[1] Opportunities and Challenges of Artificial Intelligence (AI) in Transportation; Request for Information, 89 Fed. Reg. 36848 (2024), https://www.federalregister.gov/d/2024-09645.

existing models will also allow the DOT to build on existing expertise and knowledge.[2] Federal agencies, state law and policy leaders and regulators, and in international jurisdictions, in particular the European Union, have already invested significant effort toward creating regulatory structures governing certain uses of AI. By aligning work with these frameworks, DOT can help build a unified approach to AI governance across sectors.

A central aspect of many of the legal frameworks already introduced or enacted is a risk-based approach to evaluating AI systems. These tiered risk structures provide a model for balancing the importance of responsible AI with the flexibility necessary for further development. Risk management has played a central role in the approach several government agencies have taken to AI.[3] For instance, a risk-based approach is central to the widely-adopted AI Risk Management Framework (AI RMF) produced by the National Institute of Standards and Technology (NIST).[4] NIST's AI RMF acknowledges the potential for harm to people, organizations, and ecosystems while also acknowledging the opportunities for benefits. Use of the AI RMF by federal agencies was encouraged in a memo from the U.S. Office of Management and Budget (OMB) in March 2024.[5] The flexible framework allows agencies, like DOT, to account for a spectrum of risk levels in AI uses. For instance, the potential risks posed by inaccurate or flawed automated driving

---

[2] Pursuant to President Biden's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, the DOT NETT Council was charged with the responsibility to assess the need for information, technical assistance, and guidance regarding the use of AI in transportation. Following the Executive Order, the DOT's Transforming Transportation Advisory Committee (TTAC) was created. As the DOT considers the uses of AI in transportation, we encourage the agency to continue to utilize the knowledge and expertise of TTAC's members–who are experts in various areas of transportation and technology.

[3] *DOE AI Risk Management Playbook*, U.S. Dep't of Energy (Aug. 15, 2022), https://www.energy.gov/ai/doe-ai-risk-management-playbook-airmp; *Fact Sheet: DHS Facilitates the Safe and Responsible Deployment and Use of Artificial Intelligence in Federal Government, Critical Infrastructure, and US Economy*, U.S. Dep't Of Homeland Sec. (Apr. 29, 2024), https://www.dhs.gov/news/2024/04/29/fact-sheet-dhs-facilitates-safe-and-responsible-deployment-and-use-artificial; *Department of Commerce Announces New Actions to Implement President Biden's Executive Order on AI*, U.S. Dep't of Commerce (Apr. 29, 2024), https://www.commerce.gov/news/press-releases/2024/04/department-commerce-announces-new-actions-implement-president-bidens; https://www.hhs.gov/sites/default/files/hhs-ai-strategy.pdf.

[4] Most recently updated in 2024 with a portion to cover generative AI specifically The NIST AI RMF is designed to help organizations identify risks posed by AI and develop risk management strategies that align with their organizational goals. Department of Commerce, National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (Apr. 2024), https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf.

[5] Memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, (Mar. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

systems are high, including severe injury or death.[6] Conversely, the risks posed by potential harms from an AI powered music or radio system are much lower.[7]

DOT should also consider state level AI legal frameworks, which, once in force, will be binding on a wide range of companies across the transportation sector utilizing AI. In May of 2024, Colorado passed the first United States comprehensive state AI law.[8] The Colorado AI Act (CAIA) uses a risk-based approach to regulate artificial intelligence and "high-risk AI systems."[9] Colorado is not alone in their push to regulate AI; California, Illinois, and Delaware, among others, have bills introduced that would govern the use of AI, and the California Consumer Protection Agency has said that it considers AI within its remit.[10]

International frameworks are also relevant to DOT's work in this area. Organizations in the transportation sector often interact with entities outside of the U.S. and provide solutions, services, or goods across borders.[11] The EU AI Act uses a similar categorical risk framework to that of the CAIA.[12] AI systems are classified by level of risk, and the different risk levels determine different development, deployment, and use requirements.[13] AI systems that are deemed to have

[6] *E.g.* Jacques Bileaud and Anita Snow, *The backup driver in the 1st death by a fully autonomous car pleads guilty to endangerment*, Associated Press (Jul. 28, 2023), https://apnews.com/article/autonomous-vehicle-death-uber-charge-backup-driver-1c711426a9cf020d3662c47c0dd64e35#.

[7] *See, e.g., Spotify debuts a new AI DJ, right in your pocket*, Spotify (Feb. 22, 2023), https://pr-newsroom-wp.appspot.com/2023-02-22/spotify-debuts-a-new-ai-dj-right-in-your-pocket/.

[8] Colo. Rev. Stat. §§ 6-1-1701 — 6-1-1707.

[9] The CAIA defines high-risk AI systems as "Any artificial intelligence system that when deployed, makes, or is a substantial factor in making, a consequential decision," as well as developers of both general-purpose and high risk AI systems, and deployers of high-risk systems. *See* Colo. Rev. Stat. §§ 6-1-1601(9)(a) (2024); *see also* Tatiana Rice, *Colorado AI Act Two-Pager Cheat Sheet*, Future of Privacy Forum (May 17, 2024), https://fpf.org/blog/colorado-enacts-first-comprehensive-u-s-law-governing-artificial-intelligence-systems/.

[10] A.B. 2930, 2023-24 Regular Session (CA 2023).; H.B. 5116, 103rd General Assembly (IL 2023).; H.B. 333, 152nd General Assembly (DE 2023).

[11] *Transportation and the Economy*, U.S. Dep't of Transportation, Volpe Center (Oct. 26, 2022), https://www.volpe.dot.gov/events/transportation-and-economy.

[12] European Parliament legislative resolution of 13 March 2024, on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (2024).

[13] Andrew Folks, *EU AI Act: 101*, International Association of Privacy Professionals (Mar. 2024), https://iapp.org/media/pdf/resource_center/eu-ai-act-101-chart.pdf.

unacceptable levels of risk are prohibited altogether.[14] Under the EU AI Act, certain AI systems used in vehicles and aviation may qualify as high risk.[15] However, because of their categorization under EU product safety legislation and sector-specific legislation, some in-vehicle AI systems are exempted from the EU AI Act.[16]

## II. DOT should center privacy in the evaluation process of AI use cases in transportation.

To build public trust and promote ethical implementation of AI in transportation, DOT should prioritize privacy throughout its evaluation process of AI applications in transportation that utilize personal data. As the transportation sector adopts more advanced technology, including AI, the amount of personal data and information used to make the technology function increases. At the same time, individuals have increasingly raised objections about unexpected uses of their personal data and supported greater privacy protections.[17]

Privacy protections can build trust in our digital economy, and trust is an essential precondition to individuals' acceptance of new technologies.[18] AI systems that rely upon the collection, analysis, and application of personal information create privacy and security risks for those who interact with the system. Understanding the uses of AI and the underlying algorithmic processing is

[14] Unacceptable risk AI includes cognitive behavioral manipulation (especially of vulnerable groups like children), social scoring, and real-time biometric identification systems. The EU allows for some exceptions for law enforcement purposes. EU AI Act: first regulation on artificial intelligence, European Parliament (June 8, 2024), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[15] Nils Lölfing, *Impact of the EU's AI Act on automated and autonomous vehicles*, Bird&Bird (Apr. 12, 2023), https://www.twobirds.com/en/insights/2023/global/impact-of-the-eus-ai-act-proposal-on-automated-and-autonomous-vehicles.

[16] *EU AI Act: first regulation on artificial intelligence*, European Parliament (June 8, 2024), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[17] 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

[18] *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/. Neil Richards and Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stanford Technology Law Review 431 (2016), https://law.stanford.edu/wp-content/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf.

necessary for understanding where and how privacy is implicated when these systems are used.[19]

As systems are considered, privacy protections are relevant at every stage in the product life cycle. From the outset, AI models are built upon datasets that can include significant volumes of personal and sensitive information.[20] The increased difficulty in protecting or screening out personal data, deidentifying data within datasets, and the increased possibilities for reidentifying individuals based on comparing data across data sets present privacy challenges when deploying AI. [21] As AI models are trained and used, they may continue to take in individual data and information, which is then processed and used to shape system outputs.[22]

The need for increased collection of personal data driven by many AI systems also raises additional security risks for that information.[23] These massive amounts of data collected and processed raise the risk of security breaches or hacks, potentially exposing sensitive personal information, like location data. Hackers may target AI dependent infrastructure, like electrical vehicle charging networks which can contain sensitive personal data from users.[24] Malicious actors may also exploit vulnerabilities to manipulate these systems by creating safety hazards by tampering with traffic signals or road markings to mislead vehicles.[25] When evaluating AI use,

---

[19] *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning*, Future of Privacy Forum (Oct. 2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

[20] Alice Xiang, *Fairness & Privacy in an Age of Generative AI*, 25 Columbia Science & Technology Law Review 288, 304 (2024), https://journals.library.columbia.edu/index.php/stlr/article/view/12765/6289.

[21] DataFloq, The Re-Identification of Anonymous People with Big Data (February 10, 2011), https://datafloq.com/read/re-identifying-anonymouspeople-with-big-data/228; *see also* Anonymization is not without its own risks to consider. Anonymized data may be less valuable for generative AI systems to learn from. Also, DOT should consider what would qualify as anonymized data, as standards can vary.; Isah Marathe, *With AI Training, Data 'Anonymization' Runs Risk of Becoming a Fig Leaf*, Law.com (Mar. 19, 2024), https://www.law.com/legaltechnews/2024/03/19/with-ai-training-data-anonymization-runs-risk-of-becoming-a-fig-leaf/#:~:text=ANALYSIS-,With%20AI%20Training%2C%20Data%20'Anonymization'%20Runs%20Risk%20of%20Becoming,an%20ambiguous%20or%20inaccurate%20description.

[22] Alice Xiang, *Fairness & Privacy in an Age of Generative AI*, 25 Columbia Science & Technology Law Review 288, 304 (2024), https://journals.library.columbia.edu/index.php/stlr/article/view/12765/6289.

[23] Melinda Rucz and Sam Kloosterboer, *Data Retention Revisited*, Information Law and Policy Lab (Sept. 28, 2020), https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf.

[24] *NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems*, National Institute of Standards and Technology (Jan. 4, 2024), https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems; Jim Motavalli, *As cyberattacks ramp up, electric vehicles are vulnerable*, Autoweek (Feb. 19, 2024), https://www.autoweek.com/news/a46857624/cyberattacks-on-electric-vehicles-and-chargers/.

[25] *NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems*, National Institute of Standards and Technology (Jan. 4, 2024), https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems.

DOT should consider the privacy risks of AI utilization by threat actors, as well as the opportunities AI offers to mitigate those threat actors.

## III. DOT must prioritize actions to ensure that the use of AI does not perpetuate or exacerbate harm to marginalized communities.

DOT must ensure that the use of AI does not perpetuate or exacerbate harm to marginalized communities or disrupt equal access to transportation. While AI offers possibilities to improve the lives of many, there are also great risks, including, for example, privacy risks related both to the data inputs and the potential for AI tools to be used to make sensitive inferences about a person;[26] bias and access risks on how and where AI is deployed and if it is trained on equitable and representative data;[27] and risks to safety and security based, in part, on the transparency and engineering of an AI system and the training and education of impacted communities.[28]

In general, when risks are realized, the harms of AI may be disproportionately borne by marginalized communities who tend to be both less represented in AI training data and more frequently targeted by malicious AI uses.[29] These risks in the transportation space may, for instance, have to do with an individual's location, be it rural or urban. Public transportation options may be abundant to those in a larger city, but at the same time may be inherently difficult to access or create longer commute times for those in rural communities.[30]

---

[26] For a longer discussion of previous risks, refer to section II.

[27] Biased algorithms can produce discriminatory outputs, perpetuating existing social inequalities. Many vehicles use voice-recognition systems for controls, but accuracy of voice recognition varies across different racial and gendered groups. This could impact passenger safety. Chen et al., Exploring racial and gender disparities in voice biometrics, Sci. Rep. (Mar. 8, 2022), 10.1038/s41598-022-06673-y.; Joan Palmiter Bajorek, *Voice Recognition Still Has Significant Race and Gender Biases*, Harvard Business Review (May 10, 2019), https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.

[28] Tan Yigitcanlar et al., Contributions and Risks of Artificial Intelligence (AI) in Building Smarter Cities: Insights from a Systematic Review of the Literature, Energies (March 2020), https://doi.org/10.3390/en13061473; Olga Akselrod, *How Artificial Intelligence Can Deepen Racial and Economic Inequities*, American Civil Liberties Union (July 13, 2021), *https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities*.

[29] Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023).

[30] *The Critical Role of Rural Communities in the U.S. Transportation System*, U.S. Dep't Of Transportation (Nov. 20, 2023), https://www.transportation.gov/rural/grant-toolkit/critical-role-rural-communities.

In another example, AI-powered video surveillance technologies, while useful to detect fare evasion, have been shown to evince racial disparities when deployed.[31] The harms of AI systems may also be exacerbated based on whether an AI system is designed to catalyze a specific action and what action that is.[32] For instance, in the above example, an AI system that disproportionately and inaccurately flags people with darker skin for fare evasion could cause an increase in investigations and lead to racial profiling of individuals from those communities. However, the same system that is designed to alert armed police officers or to sound alarms could lead to violent interactions that cause physical harm or death, particularly when considering that statistics show that police are more likely to act aggressively toward people from these same communities.[33] DOT should ensure that it is considering all potential harms from AI systems and carefully evaluate the implementation of such programs to ensure that the tools do not disproportionately exacerbate existing risk.[34]

It is important to ensure the promotion of equitable, lawful uses of AI that the DOT addresses how AI in transportation can perpetuate harm to marginalized communities and ensures that it is addressed in any DOT action to support or promote AI development or deployment as well as in any direct deployment of AI systems by the DOT. Proactive equity assessments as part of the evaluation process may help to ensure equity and accessibility for the systems as they develop.[35]

---

[31] Jess Weatherbed, *The NYC subway is using automated scanning software to spot fare evaders,* The Verge (Jul. 21, 2023), https://www.theverge.com/2023/7/21/23802912/mta-nyc-subway-ai-scanning-software-fare-evasion; *see also* Thaddeus L. Johnson et al., *Facial* recognition *systems in policing and racial disparities in arrests, Government Information Quarterly 39* (Oct. 2022), https://doi.org/10.1016/j.giq.2022.101753.

[32] Nina Dewi Toft Djanegara et al., Exploring the Impact of AI on Black Americans, Stanford University and Black in AI (Mar. 1, 2024), https://hai.stanford.edu/sites/default/files/2024-02/Exploring-Impact-AI-Black-Americans.pdf. Consider also, NHTSA flags myokymia–eye twitching–as a condition that could potentially confuse advanced driver assistance systems (ADAS). *See*, Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571), *available at* https://www.federalregister.gov/documents/2024/01/05/2023-27665/advanced-impaired-driving-prevention-technology/. If ADAS responds to myokymia by disabling or limiting functionality of a vehicle, the driver could be severely limited in their daily movements.

[33] Susannah N. Tapp and Elizabeth J. Davis, Contacts Between Police and Public, U.S. Dep't of Justice, Bureau of Justice Statistics (Nov. 2022), https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/cbpp20.pdf.

[34] Laura Wagner, *Here are the fare-evasion enforcement data the NYPD fought to keep secret*, Vice (Jan. 29, 2020), https://www.vice.com/en/article/y3mww7/here-are-the-fare-evasion-enforcement-data-the-nypd-fought-to-keep-secret?callback=in&code=YTIWOGI5MJKTNWQ5MC0ZYWI2LTG3NWYTYZLHZJZKZDCYMGQ2&state=53a4440c9e37447cba2a37e3213eb06f; *see also* Marin Cogan, *How Cars Fuel Racial Inequality,* Vox (June 13, 2023), *https://www.vox.com/23735896/racism-car-ownershipdriving-violence-traffic-violations*.

[35] *Blueprint for an AI Bill of Rights*, The White House (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

Equity assessments might include algorithmic impact assessments, disclosure of training data (representative), protections for demographic features, and assessments of accessibility.[36]

## IV. Conclusion

FPF appreciates this opportunity to comment on these issues and the Department of Transportation's efforts. We welcome any further opportunity to provide resources or information to assist 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

Madison Fleischaker, *Legal Intern*

[36] *Id.*