epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Office of the Secretary, Department of Transportation

on

Non-Traditional and Emerging Transportation Technology (NETT) Council; Request for Comment

87 Fed. Reg. 13368, Docket No. DOT-OST-2022-0016

April 8, 2022

---

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Office of the Secretary's (OST) Request for Comment in connection with the Non-Traditional and Emerging Transportation Technology (NETT) Council, published March 9, 2022. OST requests "public comment on projects, issues, or topics that DOT should consider" through the NETT Council.[1]

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights issues, and to protect civil liberties, the First Amendment, and constitutional values.[2] EPIC is a leading advocate for privacy and privacy-enhancing techniques for emerging technology, which includes connected cars and automated

[1] 87 Fed. Reg. 13,368.
[2] *About Us*, EPIC, https://epic.org/about/.

devices comprising the "Internet of Things."[3] EPIC has testified before Congress and submitted comments to various agencies, including the Federal Trade Commission and the National Highway Traffic Safety Administration (NHTSA), concerning the privacy and safety risks of automated vehicles.[4]

EPIC urges the Council to investigate the privacy impacts of emerging transportation technologies, promulgate guidelines for privacy in transit systems, and standing up a working group to study the issue of privacy in transit.

## I. Developments in transportation technologies should not increase surveillance.

As a baseline rule, new transportation technologies should prioritize privacy and should not expose the public to increased surveillance, collect unnecessary data on users, or transfer data to third parties. This section highlights several examples of developments in technology around transportation that harm privacy. Although these examples may not be within the NETT Council's jurisdiction, they illustrate the types of problems that the Council should be looking for.

---

[3] *See, e.g.*, *Consumer Privacy Project*, EPIC (2022), https://epic.org/issues/consumer-privacy/; *Big Data and the Future of Privacy*, EPIC (2022), https://epic.org/issues/consumer-privacy/big-data/; *Internet of Things (IoT)*, EPIC (2020), https://archive.epic.org/privacy/internet/iot/.

[4] *See, e.g.*, EPIC Comments to the DOT, Notice of Request for Comments: Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0) (Dec. 8, 2018), https://archive.epic.org/apa/comments/EPIC-DoT-AV-Comments.pdf; EPIC Comments to the FTC and NHTSA, Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles (May 1, 2017), https://epic.org/apa/comments/EPIC-ConnectedCar-Workshop-Comments.pdf; EPIC Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf; EPIC Statement to the House Committee Subcommittee on Communications and technology, Feb. 2, 2017, https://epic.org/testimony/congress/EPIC-Statement-NTIA-02-02-2017.pdf; EPIC Comments to the NTIA, On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (Jun. 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; EPIC Comments to NHTSA, Federal Motor Vehicle Safety Standards; Event Data Recorders (Feb. 11, 2013), https://epic.org/apa/comments/EPIC-Coalition-NHTSA-EDR-comments-FINAL-1.pdf; EPIC Comments to NHTSA, Request for Comment on 'Federal Automated Vehicles Policy (Nov. 22, 2016), https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf; EPIC Comments to NHTSA, Federal Motor Vehicle Safety Standards; V2V Communications (Apr. 12, 2017), https://epic.org/apa/comments/EPIC-NHTSA-V2V-Communications.pdf.

*a. Public transit systems should use anonymous credential verification systems to prevent location tracking.*

Public transit systems in the U.S. now commonly rely on swipe cards like Washington, DC's SmarTrip Card and other payment methods tied to personal balance accounts. Contactless payment systems built into cell phones are a rapidly spreading next step in public transit payment. But these systems come with a significant downside for privacy: electronic payment systems create an easily accessible record of an individual's movements over time. And the expansion to phone-based Near Field Communication (NFC) payments is enabling broader location tracking.

Traditional swipe card or tap card systems often create a record of every transaction a rider makes on a public transit system, typically when the rider enters and exits the system. Police can often access those records without obtaining a warrant, creating the potential for abuse. For example, EPIC recently submitted an amicus brief to the Massachusetts Supreme Judicial Court arguing that police searching Boston's Charlie Card system needed to obtain a warrant.[5] The court ruled that two days of transit data showing a suspect's movements around the city were not enough to constitute a search requiring a warrant under the Fourth Amendment.[6] This type of location tracking erodes privacy in public and can have especially serious implications for civil liberties if used to monitor protesters, activists, or other groups vulnerable to harassment.

The Department of Transportation (DOT) has identified contactless electronic fare payments as a rapidly growing trend in public transit.[7] The agency identified potential drawbacks to these systems, including equity and access issues for low-income and unbanked individuals and

[5] *See Commonwealth v. Zachery*, EPIC.org, https://epic.org/documents/commonwealth-v-zachery/.
[6] Commonwealth v. Henley, 488 Mass. 95 (2021) (this opinion consolidated the case in which EPIC submitted an amicus brief, Commonwealth v. Zachary).
[7] Intelligent Transportation Systems Joint Program Office, Advancements in Electronic Fare Payment Contactless and Open Loop Technologies, DOT (Jan. 25, 2022), https://www.itskrs.its.dot.gov/sites/default/files/doc/04_Electronic%20Fare%20Payment_Final%20508_01_25_22_v2.pdf.

implementation problems when the private companies providing payment systems change ownership.[8] There are also substantial privacy concerns, including police access to the data, the risk of data breach, and the potential for sale of rider data to data brokers.

Anonymous credentials provide a possible technical solution to allow electronic verification systems without compromising privacy. Anonymous credentials would allow a rider with an unlimited use pass to verify that they can access the system without disclosing the rider's identity, removing the possibility of location tracking.[9] An anonymous credentialing system could be compatible with radio-frequency identification (RFID) tap-cards or cell-phones. Of course, a lower-tech solution would be to simply make mass transit free to use, resolving privacy and equity issues at once.

*b. Transportation systems should not sell or license user data.*

Both public and private transportation systems create and collect massive amounts of data tied to individuals. Data brokers, intermediary companies that collect or buy up large volumes of data and resell that data to third parties, are an increasing threat to privacy. The DOT should recommend privacy safeguards banning the sale or transfer of user data from public or private transit systems. The NETT Council should consider the potential for the collection and dissemination of user data early in evaluating new projects.

Data brokers scoop up information, package it, and sell that information to third parties, often including the federal government and law enforcement. In 2019, the data broker industry was worth

[8] *Id*. at 4-7.
[9] *See*, *e.g.*, Anna Lysyanskya, *Signature schemes and applications to cryptographic protocol design* (2002), https://dspace.mit.edu/handle/1721.1/29271; Melissa Chase, *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications* (May 2008), http://static.cs.brown.edu/research/pubs/theses/phd/2008/chase.pdf; Fonteini Baldimtsi, *Efficient Cryptography for Information Privacy* (May 2014), https://cs.brown.edu/research/pubs/theses/phd/2014/baldimtsi.pdf; Endre Bangerter, Jan Camenisch, & Anna Lysyanskaya, *A Cryptographic Framework for the Controlled Release of Certified Data*, 3957 LNCS 20-42 (2006), https://link.springer.com/chapter/10.1007%2F11861386_4.

roughly $230 billion worldwide, and it is expected to grow to nearly $350 billion by 2026.[10] Sales of historical location data are particularly harmful. In recent years, companies have amassed large databases of location information, mostly from cell-phone apps quietly sending location data.[11] This data is often sold to law enforcement and the U.S. military, providing an end-run around Fourth Amendment protections that would require a warrant to track someone's phone.[12] Cars, mass transit, and new transit technologies like the hyperloop or personal transport drones can also create granular records of an individual's movements. Setting up rules to ban the sale, or transfer, or unnecessary use of transit data can protect privacy and prevent wrongful surveillance by either the government or private actors.

## II. The NETT Council should prioritize protecting privacy in emerging technologies, investigate the privacy implications of Council projects, and adopt guidelines to encourage privacy considerations in development of new transportation technologies.

The NETT Council is tasked with "engaging with new technologies to address legitimate concerns about safety, security, and privacy without hampering innovation."[13] To date, the Council has not significantly incorporated privacy protections in its reports or stood up a working group to consider the privacy implications of emerging technologies. But the Council has the authority to do

[10] Knowledge Sourcing Intelligence, *Global Data Broker Market Size, Share, Opportunities, COVID-19 Impact, And Trends By Data Type (Consumer Data, Business Data), By End-User Industry (BFSI, Retail, Automotive, Construction, Others), And By Geography - Forecasts From 2021 To 2026* (Jun. 2021), https://www.knowledge-sourcing.com/report/global-data-broker-market.
[11] *See Location Tracking*, EPIC, https://epic.org/issues/data-protection/location-tracking/; Charles Levinson, *Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones*, Protocol (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data.
[12] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Bryan Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.
[13] Office of the Secretary of Transportation, Pathways to the Future of Transportation: A Non-Traditional and Emerging Transportation Technology (NETT) Council Guidance Document (Jul. 2020), https://www.transportation.gov/sites/dot.gov/files/2020-08/NETT%20Council%20Report%20Digital_Jul2020_508.pdf.

so. Prioritizing privacy can provide a competitive advantage for American companies and positively shape the development of transportation technologies.

The Council's main work product to date, a review of standards and regulations that might apply to hyperloop systems, summarized information security standards but did not address privacy standards.[14] Privacy protections, like information security protocols, are not the central issue in evaluating the potential for an early-stage technology like the hyperloop. However, the Council can ensure that privacy is built into proposed future transportation systems like the hyperloop by identifying it as an issue from the outset. Hyperloops, like any form of mass transit system, would present an opportunity for location-tracking and camera surveillance. The Council should take the opportunity to get ahead of the curve by identifying privacy as an issue for possible hyperloop systems and ensuring it is addressed early in development.

Prioritizing privacy can have substantial benefits for both innovation and competition. Too often, legal safeguards on the collection and use of personal information are assumed to be at odds with innovation and economic growth. But this view of privacy as merely a regulatory burden ignores the ways in which data protection will benefit consumers, strengthen market competition, and lead to the development of better and more popular products and services. Time and again, studies have found that the American public cares strongly about protecting personal data from commercial exploitation and will opt for credible privacy-protective alternatives when they are

[14] NETT Council, *Hyperloop Standards Desk Review* (Jan. 2021), https://www.transportation.gov/sites/dot.gov/files/2021-01/NETT%20Council%20Hyperloop%20Standards%20Desk%20Review_14Jan2021_final.pdf.

available.[15] For example, when Apple recently gave iOS users the power to easily block advertisers from tracking them across multiple apps, 96% of users opted out of such tracking.[16]

Prioritizing privacy can position American firms to compete well in privacy-conscious markets like Europe. For example, as the Council considers development of drones for personal transport, drone privacy rules like Europe's 2019 comprehensive drone regulations[17] will be highly relevant. With prompting from regulators like the agencies comprising the NETT Council, American firms can take a leading position in privacy-forward transportation development worldwide.

To provide that push, the Council should (1) consider privacy implications early and often in all its projects and (2) stand up a specific privacy working group to promulgate guidelines for applying privacy to emerging transportation technologies. To better understand how to implement privacy protections, the Council should solicit information from privacy experts outside of industry and consult the general public on their transportation privacy concerns. Getting the jump on privacy issues will be good for the NETT Council, good for industry, and good for the public.

---

[15] *See, e.g.*, Cisco Secure, *Building Consumer Confidence Through Transparency and Control* (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (finding that 86% of respondents "care about data privacy" and "want more control," while 79% are "willing to spend time and money to protect data" and "pay more"); Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data*, Morning Consult (Apr. 27, 2021), https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/ (finding that 83% of voters believe Congress should enact privacy legislation); Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (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/ (finding that 75% of respondents believe there should be new regulations of what companies may do with personal data).

[16] Samuel Axon, *96% of US Users Opt Out of App Tracking in iOS 14.5, Analytics Find*, Ars Technica (May 7, 2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/.

[17] Commission Delegated Regulation (EU) 2019/945, on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (Mar. 12, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN.

## III. Conclusion

EPIC applauds the NETT Council's early involvement with emerging transportation technologies. EPIC urges the Council to prioritize privacy by investigating the privacy implications of transit systems early in their development, promulgating guidelines for privacy in transit systems, and standing up a working group to study the issue of privacy in transit. For further information, please contact EPIC Fellow Jake Wiener at wiener@epic.org.

Respectfully Submitted,

*Jake Wiener*
Jake Wiener
EPIC Law Fellow
*Calli Schroeder*
Calli Schroeder
EPIC Global Privacy Counsel