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

Department of Transportation

on

Request for Information: Enhancing the Safety of Vulnerable Road Users at Intersections

87 Fed. Reg. 57,019

November 15, 2022

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Department of Transportation (DoT)'s September 16, 2022 Request for Information on Enhancing the Safety of Vulnerable Road Users at Intersections. The DoT requests input on the "possibility of adapting existing and emerging automation technologies to accelerate the development of real-time roadway intersection safety and warning systems for both drivers and VRUs in a cost-effective manner that will facilitate deployment at scale."[1] DoT's proposed system would use a variety of sensors including fixed cameras, LiDAR, and radar to detect vulnerable road users like pedestrians and bikers and communicate that information to driver/autonomous warning systems installed in cars.

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,

[1] 87 Fed. Reg. 57,021.

the First Amendment, and constitutional values.[2] EPIC is a leading advocate for privacy and privacy-enhancing techniques for emerging technology, such as connected cars and automated devices comprising the "Internet of Things."[3] EPIC testified before Congress and submitted comments to various agencies, including the Department of Technology, the Federal Trade Commission and the National Highway Traffic Safety Administration ("NHTSA"), concerning the privacy and safety risks of automated vehicles.[4] EPIC regularly advocates to preserve and expand privacy in public.[5]

EPIC urges the Department of Transportation to prioritize privacy from the outset of any vehicle warning system project. A privacy-preserving warning system would by design minimize data collected and transmitted, avoid recording and storing video, and would not require or collect any cellular or NFC data.

---

[2] EPIC, *About Us*, https://epic.org/about/.

[3] *See, e.g.*, EPIC, *Consumer Privacy*, https://epic.org/privacy/consumer/; EPIC, *Internet of Things (IoT)*, https://epic.org/privacy/internet/iot/.

[4] *See, e.g.*, EPIC Comments to the DOT, Non-Traditional and Emerging Transportation Technology (NETT) Council; Request for Comments (Apr. 8, 2022), https://epic.org/documents/epic-comments-non-traditional-and-emerging-transportation-technologies/; 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.

[5] *Privacy in Public*, EPIC, https://epic.org/issues/surveillance-oversight/privacy-in-public/.

I. Privacy is a vital element of any public system capable of conducting surveillance.

The DoT's plan for a VRU and Vehicle Warning System is a thoughtful first step towards improving pedestrian safety, especially as assisted-driving cars become more common and fully autonomous cars are considered. Although the RFI identifies privacy as a concern in several discrete areas, it does not prioritize privacy as one of the main design concerns when developing a public-facing sensor system. To properly weigh privacy concerns, the DoT should regularly evaluate what privacy risks the planned system may pose and whether the system as designed outweighs those risks. The DoT should recognize that there are privacy-preserving means to enhance traffic safety and select for the most privacy-protective option when choosing between systems.

Any system that deploys cameras and other sensors in public with the potential to record and store individuals' movements can become a system of surveillance instead of safety. The proposed system would include cameras, as well as a variety of other potential sensors that could record the location, movements, and activities of both pedestrians/VRUs and cars. Such a system runs the risk of creating a record of people's movements and expanding video camera surveillance. Privacy in a person's location history is important for personal safety and autonomy because location data can reveal intimate details of a person's life.[6] In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Supreme Court recognized that warrantless tracking of a person's location over time can constitute an unlawful search under the Fourth Amendment of the Constitution.[7] As such, the DoT should prioritize privacy in a vehicle warning system to ensure that pedestrian safety is not a justification for expanding surveillance, possibly in violation of the Constitution.

Data brokers are a particular concern when setting up a system capable of monitoring the public. Data brokers scoop up information, package it, and sell that information to third parties, often

[6] *See* EPIC, *Location Tracking*, https://epic.org/issues/data-protection/location-tracking/.
[7] *See* EPIC, *Carpenter v. United States*, https://epic.org/documents/carpenter-v-united-states-2/.

including the federal government and law enforcement. In 2019, the data broker industry was worth roughly $230 billion worldwide, and it is expected to grow to nearly $350 billion by 2026.[8] Selling historical location data is both profitable and particularly harmful. In recent years, companies have amassed large databases of location information, mostly from cell phone apps quietly sending location data to third parties.[9] 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.[10] The DoT should be careful in designing a system to avoid exposing personal information to companies that could turn around and sell that information.

Deploying more cameras to intersections that focus specifically on pedestrians also runs the risk of expanding camera surveillance, creating a record of every interaction at an intersection. If intersection camera footage is stored, police could have warrantless access to the details of a person's movements, who that person regularly associates with, and the patterns of that person's life. Many intersections are in heavily trafficked public areas; therefore a poorly designed VRU warning system runs the risk of recording far more than just the flow of pedestrian and vehicle traffic. The best way to address the threat of expanded public surveillance is data minimization by design.

[8] 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.

[9] *See* EPIC, *Location Tracking*, 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.

[10] 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 & 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.

II. Data minimization by design is necessary to preserve privacy.

If the DoT opts to develop a VRU detection and warning system, the Department should mandate that the system minimize the data it collects to what is strictly necessary and should adopt privacy-by-design principles.[11] The system should *by design* collect only the information necessary to make it effective and should not retain that information any longer than is necessary to provide the service. Privacy by design extends to choosing more privacy protective technologies over more invasive surveillance technologies.

The most privacy protective version of a vehicle warning system would use only technologies are incapable of collecting data on pedestrians and other VRUs. The DoT should consider prioritizing systems using radar or LiDAR over systems using cameras because those technologies inherently collect less personal information. Radar or LiDAR cannot detect and store a person's face or other physical details, so any

Even if the DoT opts for a system relying on cameras, requiring data minimization by design would ensure that a VRU warning system is effective without compromising privacy. A VRU warning system that meaningfully embraces data minimization would likely function on the following principles:

- Sensing and transmitting only the presence or absence of a pedestrian or other VRU in the intersection.
    - Although the RFI proposes using artificial intelligence to estimate the progress of pedestrians through intersections, a system that only detects and reports presence would be more likely to preserve privacy and less prone to potentially fatal errors.
- Using cameras only for real-time sensing. No video recordings are stored at all.

[11] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner of Canada* (Jan. 2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

- No identifying information collected. Pedestrians, drivers, and other VRUs should not have to expose any identifying information including facial images for a warning system to work.

- Strict data retention limits for any information that is collected. Data should be retained only for long enough to make the system effective.

III. A VRU detection system should not require or collect any data broadcast by pedestrians.

Several recent proposals for pedestrian detections systems have suggested using Bluetooth™ signals from cellphones or tile devices to alert cars to the presence of pedestrians. The DoT should not endorse any system that requires or even collects data from cell phones because such a system creates unacceptable risks to location privacy and privileges the safety of pedestrians with phones over those without.[12]

The Ford Motor Company recently announced it was developing an app to alert drivers to the presence of pedestrians by collecting Bluetooth Low Energy signals from pedestrians.[13] Ford has also filed a patent for a system allowing autonomous cars to communicate directly to pedestrians and alert pedestrians to the presence of vehicles, through some form of augmented reality system.[14] The latter system is particularly dangerous because it would place the onus on pedestrians to avoid cars instead of providing cars with the necessary information to avoid pedestrians and bicyclists.

Using phone data in a vehicle warning system also risks creating another source of location data which car companies could sell to data brokers or make available to law enforcement. Cars are

[12] For more on the harms of location tracking, *see* EPIC, *Location Tracking*, https://epic.org/issues/data-protection/location-tracking/.
[13] Ford Media Center, *Ford Explores Smartphone-Based Tech that Could Help Alert Drivers of Hard-to-See Pedestrians, Bicyclists and More* (Sept. 19, 2022), https://media.ford.com/content/fordmedia/fna/us/en/news/2022/09/19/ford-research-tech-for-vulnerable-road-users.html.
[14] Erin Marquis, *Ford Patents App to Tell Pedestrians When Autonomous Vehicles Won't Stop for Them*, Jalopnik (Aug. 9, 2022), https://jalopnik.com/ford-patents-app-to-tell-pedestrians-when-autonomous-ve-1849366457.

equipped with a variety of sensing systems such as GPS that, combined with a unique device ID from a cellular device, could establish an individuals' location. Cars are already a source of significant surveillance directed against their drivers and passengers, and police are often granted access to data from car sensors.[15] Equipping cars to identify and log cell phones could potentially expose pedestrians to hundreds of car-phone interactions per day, building a detailed record of individuals' movements.

Collecting cell phone data through Bluetooth exposes pedestrians' data and forces pedestrians to either carry a phone or travel in a technological blind spot. A system relying on cell phone data will be less effective at protecting children, the elderly, and other groups unlikely to carry phones.

Conclusion

EPIC urges the DoT to prioritize privacy in the development of a warning system for Vulnerable Road Users. Ensuring that any system implements data minimization by design and does not collect any data broadcast by pedestrians will help ensure that the warning system does not become a surveillance system as well. For further questions, please contact EPIC Counsel Jake Wiener at wiener@epic.org.

Respectfully Submitted,

John Davisson
John Davisson
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Counsel

[15] *See* Evan Enzer et al., *Wiretaps on Wheels*, Surveillance Technology Oversight Project (Nov. 1, 2022), https://www.stopspying.org/wiretaps-on-wheels.