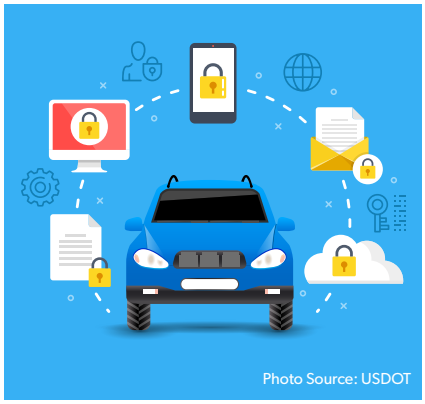
ADVANCING DATA UTILITY WHILE MITIGATING PRIVACY RISK

Transportation safety and mobility applications rely on time-sequenced location data. However, there is a risk of unauthorized parties using such data to discover an individual's travel patterns. To prevent this from happening, organizations often limit data releases. But these limitations often cause unintended consequences, including reducing open sharing of transportation data and the associated benefits, such as improved safety and operational efficiency. Moreover, simply deleting identifiers such as names and addresses from the data does not eliminate the possibility that drivers' identities could be inferred from their travel patterns.



There is a better way.

The U.S. Department of Transportation has developed a method to limit risk of traveler identification using a combination of map data and information theory. The result is context-specific strategies for hiding sensitive location and route information. This approach preserves precise location data characteristics that are necessary for effective safety and mobility applications. However, it removes the risk of the data unintentionally revealing any individual's travel patterns – protecting personal privacy. Moreover, it maintains high-quality data capable of supporting improved transportation operations and planning.

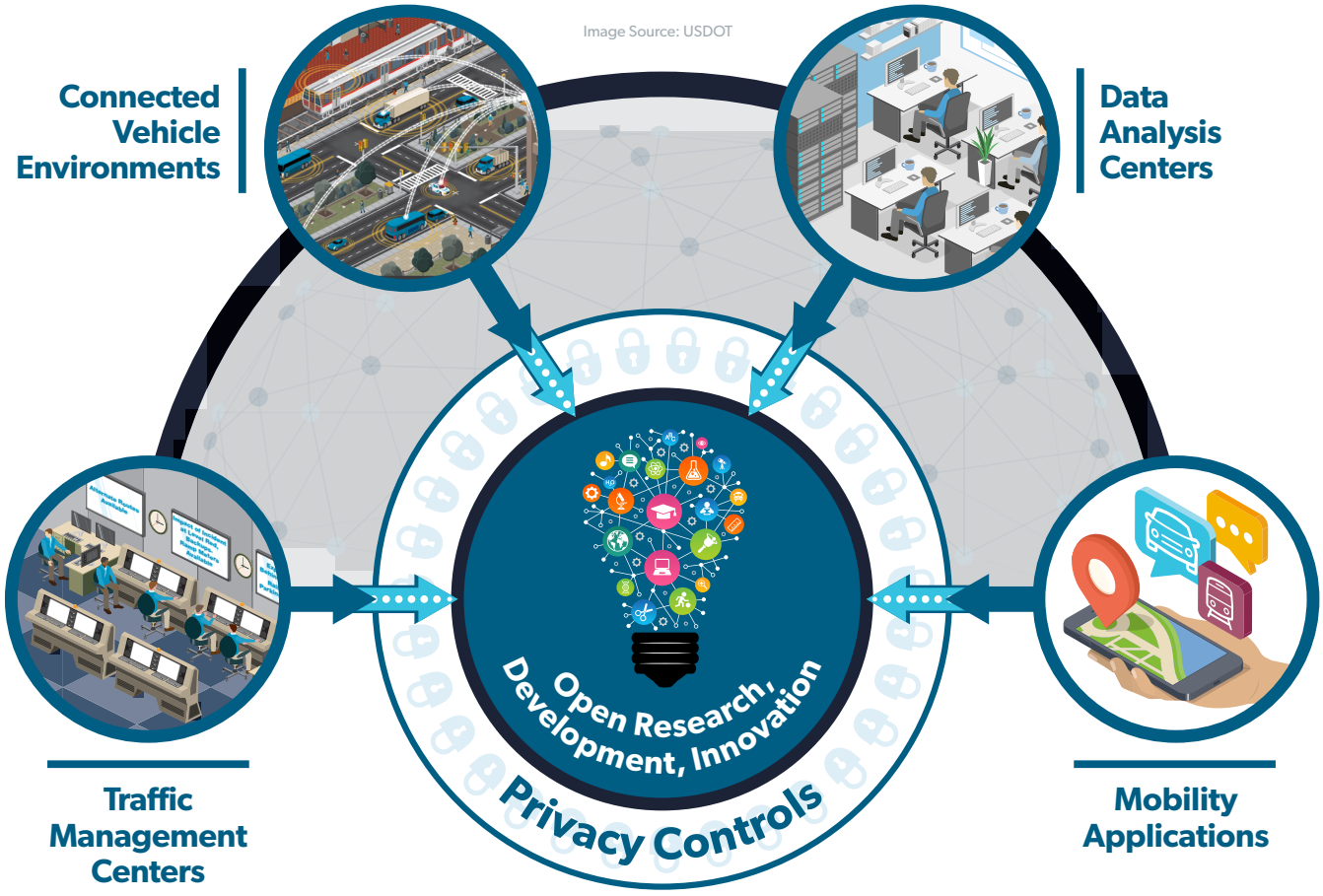
Vision

We are developing tools and practices that manage privacy risk while maintaining the utility of time-sequenced location data that can be used for the research and development of innovative applications to improve safety, mobility, and environmental protection.

Project Objectives

- **Improve public understanding** of existing and proposed privacy-protection designs.
- Define a **common, privacy-focused language** for time-sequenced location data and technologies.
- **Proactively identify and develop solutions to address potential weaknesses** that could create privacy risk in safety and mobility data specifications, and data transport and storage systems.
- **Collaborate with transportation deployers** to build privacy-protection technologies that **increase consumer confidence** in data-oriented services that rely on location data.
- **Develop a Privacy Assessment Framework** for transportation data architectures and systems. This includes developing consistent measures of privacy effectiveness across organizations, identifying data elements that could compromise privacy if linked to currently-protected data, and evaluating whether privacy designs are effective.

U.S. Department of Transportation



This image shows how data from a variety of sources can be processed to limit risk of traveler identification and made available to the public for open research, development, and innovation.

Existing Capabilities

This project has developed computational tools to manage privacy risk while supporting transportation analysis, services, and research.

The **Privacy Protection Module (PPM)** processes real-time data from vehicles and infrastructure devices, routed through the Operational Data Environment (ODE). This technology retains data within a pre-determined geographic boundary – a process known as *geofencing* – while suppressing data from outside the boundary. The PPM can apply other constraints as needed and is capable of rapidly processing large-volume data streams. To download the code, visit: https://github.com/usdot-jpo-ode/jpo-cvdp.

The **Privacy Protection Application (PPA)** prevents inferences of drivers' identities from large collections of connected vehicle geo-location data. The PPA uses road networks, map-matching, and vehicle dynamics to identify and hide potentially sensitive locations based on information theory. Times and locations in retained records are not modified, so analysis for safety application development remains possible. An independent party evaluated the tool and found that it effectively mitigates certain risks. Visit: https://github.com/usdot-its-jpo-data-portal/privacy-protection-application.

Work in Progress

- We are researching relationships between applications and privacy controls, potential effects on data utility, and how to mitigate such effects to preserve data usefulness.
- We have developed a proof-of-concept privacy sensitivity model that uses modeling and simulation in concert with time-sequenced location data to measure the effectiveness of privacy controls when deployed over a large geographic area.

Get Involved – It's a Win-Win Situation

Want to learn how these privacy-enhancing technologies can support your advanced transportation deployments? Have an ITS data privacy challenge you'd like to solve in collaboration with our team? We're looking for your input to inform our product roadmap. Open a Github Issue or contact us at: data.itsjpo@dot.gov.

To access other code and data available through ITS JPO research, visit:

https://its.dot.gov/data/

https://its.dot.gov/code/

For more information about this initiative, please contact:

Ariel Gold, Data Program Manager, ITS Joint Program Office
USDOT Office of the Secretary of Transportation, Federal Highway Administration
(202) 366-4374 | ariel.gold@dot.gov | www.its.dot.gov

FHWA-JPO-18-630