AV Data Privacy and Security Subcommittee

Initial Recommendations

I. Purpose

This document sets forth recommendations in the form of broad principles to enable the safe and secure adoption of Autonomous Vehicles in the State of Washington. We have divided the scope into two phases: Testing and Deployment. We hope that these guidelines inform future work for our committee and other committees tasked with identifying issues and solutions pursuant to our implementing statute.

II. Scope

The following are in scope for these principles:

1. Vehicles with Conditional Automation
2. Vehicles with Full Automation
3. On-Demand Fleets of Automated Vehicles
4. Automated Regional Public Transit (Early Deployment Opportunity: Automated Low-Speed Passenger Shuttles)
5. Automated Interregional Transit
6. Automated Local Delivery Vehicles
7. Automated Medium- and Long-Haul Freight Trucks
8. Automated Heavy Equipment Vehicles

The following are out of scope for these principles, but are worthy of future study

1. Farm equipment operated on private land
2. Vessels and watercraft
3. Aircraft, including UAS

III. Objective:

It is the intent of the State of Washington to enable the safe testing and deployment of autonomous vehicles in a manner that protects the security and privacy of our residents. To that end, we have established the following Autonomous Vehicle Privacy Principles for the testing and development phase:

IV. Privacy and Data Protection Principles:

Transparency

Testing and deployment of autonomous vehicles should be conducted in a transparent manner to the extent reasonably consistent with protection of intellectual property. Any test conducted in Washington State should be required to provide at least the following information to state and local agencies responsible for licensing within 90 days of the start of the test:

a. Number of vehicles involved
b. Approximate mileage travelled
c. General location of test operations
d. Number of trips
e. Types of engine or propulsion
f. Basic navigation system technology utilized
g. Basic security system technology utilized
h. Biometric and personal data collected or processed during the test (if any)
i. National, international or industry standards for privacy and data protection to which the test will conform

Consent and Use

To the extent consumer data containing personally identifiable information is collected, it should be done with informed consent and only used only for the purpose indicated at the time of collection. Entities considering or conducting tests are advised to thoughtfully consider state laws on biometric identifiers and data breach.

Collection

Data should be collected in formats to allow for utilization and portability across different platforms and systems. For example, data could be written to confirm to NIST or other widely accepted national standards.

Sharing

We encourage data sharing between various participants in this nascent industry. Data containing personal information should be shared in an anonymized fashion.

Retention and Disposal

Data should only be retained for time periods reasonably related to the purpose of processing and analysis. Contractual permitting agreements should include data retention and disposal policies that conform with legal requirements.

Access

AV service providers should limit access to data and information to those with a need to know and in accordance with the provider's Privacy Statement and Terms of Use. Personal information collected should be exempt from public records disclosure due to security concerns during the testing phase.

People involved in the testing should be afforded at least the following rights of access to data concerning themselves and their families:

a. the right to access the data relating to their AV usage if it is personalized (PII)
b. the right to delete their AV usage data, provided, however, that a testing entity should have the right to aggregate and anonymize group data for future use
c. the right to approve or reject the sale or rental of their PII by any entity controlling or processing data connected with the test

Security

Vehicles and systems should be testified and certified to prevent cyber hacking, specifically with respect to data theft and vehicle take-over and/or control. New technologies capturing audio and video of participants inside vehicles should be held to the highest privacy protection standards.

The Autonomous Vehicle Work Group should maintain a list of acceptable cyber security standards believed to be in use by testing entities, such as the following:

- Service Organization Control (SOC) 2 Type II examination (AICPA or CPA)
- General Data Protection Regulation (GDPR) of the European Union
- National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).
- Auto-ISAC best practices (https://www.automotiveisac.com/best-practices/)

Enforcement

Monitoring and reporting requirements should be established to ensure that service providers comply with contractual obligations regarding the safe operation and secure data practices established for operation.

Harmonization

As law and practice evolve in this area among cities, states and provinces, Washington should seek to promote harmonization of regulation.