Subcommittee on Cybersecurity, Privacy and Data: Opt-In Options, Fiduciary Duty, Differential Privacy and Data Minimization

A major concern of the Task Force on Autonomous Vehicles is how to balance the protection of individual privacy with the needs of public entities to plan, provide for services, and address historic inequalities in transportation access. Additionally, proprietary information held by industry may also be of use for these same public purposes, but must also be protected from public disclosure.

The Subcommittee on Cybersecurity, Privacy and Data recognizes that privacy is a complex issue in a highly interconnected world. With few exceptions, privacy concerns are not constrained to automated vehicles, but extend to many technologies that are becoming more a part of the lives of Oregonians. The Subcommittee recommends that privacy policies related to automated vehicles align with the work of other groups that are considering policy or regulation to provide Oregonians reasonable privacy protections in a rapidly changing technology landscape.

The Subcommittee recognizes several important privacy tenets. First, data-collecting entities providing a mechanism for individual or corporate “opt-in” for information to be shared, with a specified data use agreement executed by the entity receiving personal or corporate information, would provide the most transparency and highest control of the data by the owner of the information. The Subcommittee recommends that if the end user declines to opt-in to sharing certain information, that it not be a restriction of use, either of the automated vehicle or of public infrastructure the automated vehicle might require.

Second, the Subcommittee recognizes that it is also clear that entities that hold personal information have a fiduciary duty to protect that data. This concept could be applied to any entity that collects sensitive information about a person in connection with use of an automated vehicle. Where a person travels can be highly sensitive, and patterns of travel can reveal to entities that would want to influence behavior. Therefore, some are cautioning against giving away too much personal information without adequate safeguards. ¹ Additionally, considerations in statute or regulation should be made regarding accountability, responsibility, and enforcement in regards to loss or misuse of sensitive personal information, or of proprietary industry information.

Also, for information collected by government agencies, accessing individual personal information for purposes other than those agreed to in user agreements would follow existing due process controls. State, local or tribal governments should use any personal information they hold only for the governmental purposes for which the information was gathered, and have the same fiduciary duty to protect that data as other entities that collect personal information. Governments using information collected from automated vehicles should also be mindful of balancing public records laws with an eye toward protecting privacy.

Fourth, an additional approach to support public policy development is to provide sufficiently depersonalized aggregate information to support public sector planning requirements. This concept of “differential privacy” means that by looking at the output of a dataset, one cannot tell whether any individual’s data was included in the original dataset or not. The goal of differential privacy measures is to ensure that regardless of how eccentric any single individual’s details are, and regardless of the details of anyone else in the database, the guarantee of privacy still holds. Differential privacy is a concept from academic researchers, who are often faced with the challenge of protecting privacy while researching sensitive issues with sensitive personal information. There are approaches that use statistical methods to depersonalize or anonymize information to ensure personal privacy and protect proprietary commercial information, while retaining value of analysis for public planning activities.

The State may wish to require certain elements of information, such as trip origin and destination location, and occupancy of vehicle, to be made available to support public planning efforts. If consumers or industry must provide this information as a condition of use of automated vehicles, the State should specify the data elements desired, the reasons for collection, provide a method for the consumer to access this data, and use and update methods for data anonymization. In an ever-data-saturated world, effective anonymization is an evolving duty. Data-collecting entities should keep in mind the principle of data minimization—that entities should collect only what is necessary. Collecting more than the necessary information can lead to higher costs of data storage, protection, and increased risk of information breach.

While the nature of what and how much is collected will vary with time and needs in the dynamic environment of automated vehicles, the Subcommittee recommends a careful balance amongst protecting proprietary information, preserving individual privacy, and promoting public planning uses.

---