WASHINGTON STATE AUTONOMOUS VEHICLE WORK GROUP

Washington State Autonomous Vehicle Work Group Subcommittee Discussion Form

Subcommittee	System Technology and Data Security Subcommittee
Date of Meeting	October 21, 2020

This form is to be used for all subcommittee discussions that do not have specific recommendations.

1) NOTEWORTHY TOPICS OF DISCUSSION, SUMMARY OF DISCUSSION, AND OUTCOME OF DISCUSSION

- There is an effort among many U.S. States to do model privacy on GDPR
  - It is possible the Federal Government will look to do something similar to GDPR in the near future. If several states have passed privacy laws, the Feds will use that as a baseline.
- California has become the 'tip of the spear' in the U.S. for creating data protection and privacy standards
  - California recently implemented the California Consumer Privacy Act[1] (CCPA)
  - CCPA has been modified by the California Privacy Rights Act[2] (CPRA)
    - CPRA is more aggressive than CCPA on controls and penalties
    - CPRA is an ACLU-forward form of consumer protections on data privacy that goes beyond those in GDPR
- In Washington State, an effort has been underway for about 4 years to take a legislative approach to data protection, modeled on GDPR
  - Serves as a baseline for more than a dozen other states that are looking to Washington for leadership on this topic
  - 2020 legislative session came close to approving legislation
  - Senator Carlyle bringing new version this session, with slightly more support from some consumer protection groups
  - Legislation hopes to instill confidence among consumers that their data is retained well, managed well, is something they can delete/edit/change, and something they can have control over (if not outright ownership of)
- A component of this subcommittee includes data privacy
  - In 2019, this subcommittee made some modest recommendations; those recommendations were not endorsed by the Executive Committee
  - If we do not specifically distinguish AVs in the Carlyle bill, they will very likely be treated as "processors" if they collect, store, or transmit PII.
  - There are some specific considerations unique to AV; required notifications must be safe and clear; some data collected is not related to the individual(s) in

[1] California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa

[2] Consumer Privacy Rights Act (CPRA) draft language: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

1) NOTEWORTHY TOPICS OF DISCUSSION, SUMMARY OF DISCUSSION, AND OUTCOME OF DISCUSSION

the vehicle but rather about other vehicles and people within range of cameras and other sensors.

- A component of this subcommittee includes cybersecurity.
    - The subcommittee has met with technology experts and has begun collection of data regarding federal and other state regulations related to system vulnerabilities.
    - More analysis is required. At the moment it appears that cyber-risk is a standards matter more suited for federal agencies to address as it spans far beyond the vehicle into a wide array of government transportation, private transportation, telco, and other systems that connect to the vehicle as it moves from place to place.
- Consumers will have rights to access, correction, deletion, and opt out of targeted sales, advertisements, and profiling
- AVs themselves should have no distinction – the service operators that own the vehicle will be the one to contain information on riders
- Washington Technology Industry Association (WTIA) will be weighing in on the Washington Privacy Act during session
    - WTIA wants to make sure the language is useful, but that it also does not inadvertently create barriers for AVs
- New standard published, UL4600[3], a systemwide safety assessment for AVs
    - Attempt to have an approach to answering the question of how do we know if an AV is safe enough to put in public?
    - Incorporates prescriptive standards where applicable, but focuses on a safety case approach instead – Companies must have a structured argument on why an AV technology is safe

2) NEXT STEPS AND PLANS FOR SUBCOMMITTEE

- Next meeting scheduled for December 2, 2020 – Subcommittee members specifically requested more information about who is testing and status of commercial testing in Washington. Subcommittee will also focus on security standards to determine if there is any consensus on standards
    - Looking at ISO standards, which are specific to coding
    - Evaluating National Highway Traffic Safety Administration (NHTSA) vs. National Institute of Standards and Technology (NIST) cybersecurity frameworks
    - UL4600 standards recently published regarding a system wide safety assessment for AVs

[3] Underwriters Laboratories (UL) 4600 Standard for Safety for the Evaluation of Autonomous Products: https://ul.org/UL4600