WASHINGTON STATE
AUTONOMOUS VEHICLE
WORK GROUP

MEETING SUMMARY

Meeting: System Technology & Data Security Subcommittee
Location: Teleconference
Date: October 21, 2020

Attendees:

Name	Organization
Ginger Armbruster	City of Seattle
Ted Bailey	Washington State Department of Transportation
Jim Blundell	T-Mobile
Dylan Dias	Neal Analytics
Joydeep Hazra	Nokia
Tamara Jones	Washington State Transportation Commission
Steven Maheshwary	Governor's Office, Information & Communication Technology
Daniel Malarkey	Sightline Institute
Leo McCloskey	Echodyne Corp
Tyler Milligan	Milligan Partners
Markell Moffett	WSP USA
Katy Ruckle	Washington Technology Solutions (WaTech)
Kelly Rula	City of Seattle
Michael Schutzler	Washington Technology Industry Association (WTIA)
Ryan Spiller	Alliance for Automotive Innovation
Ian Wesley	Washington Department of Transportation
Joseph Williams	Pacific Northwest National Laboratory

Welcome & Introductions

- Introductions
- Walk through agenda

Current Security Regulations and Potential Gaps

Katy Ruckle & Michael Schutzler

- The European Union (EU) has become the de facto standard for the technology industry through the General Data Protection Regulation[1] (GDPR), a restrictive data protection and security standard enforced across Europe

[1] European Union General Data Protection Regulation (GDPR): https://gdpr-info.eu/

MEETING SUMMARY

- There is an effort among many U.S. States to do something similar to GDPR
    - It is likely the Federal Government will look to do something similar to GDPR in the near future
- 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[2] (CCPA)
    - CCPA looking to get replaced by the California Privacy Rights Act[3] (CPRA)
        - CPRA is more aggressive than CCPA
        - 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, modeling GDPR
    - Serves as a baseline for 12 to 24 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 support from consumer protection groups
    - Legislation needs 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 was supposed to be data privacy
    - In 2019, this subcommittee went down the data privacy path and the resulting recommendations were not endorsed
        - There is a juggling act between technical, legal, corporation, and consumer perspectives on what data privacy in Washington is/should be
        - Data Guiding Principles recommended by this subcommittee were rejected by the AV Executive Committee
- Question to meeting attendees – Is there something useful, specific to autonomous vehicles/technologies and how they use, distribute, or share personally identifiable information (PII) that should be recognized in the Washington Privacy Act[4] being proposed in session? Or presented in its own data privacy bill? Or is autonomous vehicle/technology data privacy no different than any other data privacy?

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

[3] 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

[4] Washington Privacy Act draft legislation: https://sdc.wastateleg.org/carlyle/wp-content/uploads/sites/30/2020/09/WPA-2021-DRAFT-Carlyle.pdf

- If we do not specifically distinguish AVs in the bill, they will be treated as "processors" if they have PII.
    - 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
    - Private vs. fleet/service owned AVs – Privacy managed should be held at the ownership level of the AV
    - The AV itself does not care who is riding
- How is this different from smartphones collecting location data or other data without obtaining express consent from the smartphone owner?
    - AVs are loaded with cameras and sensors, the range of AV privacy goes beyond the inside of the vehicle – pedestrians or others outside the vehicle may be picked up by cameras or sensors
- When is the notification made to a consumer? Does it have to be a permission-based system? How often does it notify consumers of data collection and rights?
    - In a service/fleet-based AV operation, every time a new rider gets in the vehicle, notification needs to occur again
    - Different data require different notification sequences and requirements to be effective getting permission from consumer
- Cellphone companies selling a phone to a consumer is actively selling access to an asset that allows data transfer – active opt-in situation
    - When buying a car, consumers aren't necessarily signing an end user license agreement (EULA), is the consumer actively opting in to the disclosure and use of their data?
    - In a shared use vehicle, consumers sign up for a private service they agreed to participate in and acknowledge the collection and use of data
- With both GDPR and CCPA, a consumer can identify data they want deleted. How would AVs handle the removal of a consumer's experience from the data perspective and its relation to AV improvements or safety responsibilities (such as reporting an incident to law enforcement)?
- Article regarding unusual data vehicles collect today: https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html
- 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

        - Bill writers were not thinking of AVs, they were thinking of websites, phones, etc.
    - **ACTION ITEM**: Any meeting attendees that want more information about engaging with the WTIA on this bill feedback, contact Michael Schutzler
- Geolocation and cameras are two items that seem distinct to AVs not covered in the current bill language
    - In addition to cameras, sensors need to be considered as well
    - For cameras and sensors facing outward, what are the rights of those around the AV?
        - Able to take temperature, biometrics, etc.
        - Another aspect of the 'surveillance society' we are living in
- Notification and consent another point specific to AVs to consider for the bill
    - Note the difference between personally owned and shared AVs
        - Not much personally owned AV testing occurring
        - Tesla's plan for AVs is that if personally owned, when not in use, the AV can subscribe to the fleet and go ferry others until the owner requires the AV again
            - Similar to existing Uber and Lyft concept of personally owned vehicles being used for fleet services
    - We are a consent state, laws are already implicitly broken
- State and cities are advocates for granular trip data for anyone using the right of way for profit, there is a data privacy layer to that
    - Companies want to control their data
    - Vehicle manufacturers, transport, government all want the data
    - Even if the data is deidentified and anonymized for pattern recognition, etc., regulations should still be imposed to guarantee anonymity, data rights, control and ability to delete, etc.

Topic Closed.

Data Security

Katy Ruckle & Michael Schutzler

- At May subcommittee meeting, we discussed the state of technology and regulations across the country respective of security, where are the breach points and hack vulnerabilities of the system

    - Not just about the vehicle, more about the data transport between the vehicle and the data's next step
- Have looked to see if there is any consensus on standards – There is not
    - 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
- Do others have information on how cybersecurity is being tackled at a high level, legislatively?
    - Is this a topic that we should be trying to tackle as a state, or should wait and let other states and/or federal figure it out?
    - Potential recommendation to the Executive Committee that we learn, support, and do what we can with our Federal delegation, but do not try to tackle as a state
    - New standard published, UL4600[5], 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
            - Cybersecurity must be part of the argument
                - How do you know a system is secure?
                - What evidence do you have to back it up?
                - Safety case is the overarching framework, relying on specific standards where it can, otherwise requiring documentation/proof that the AV technology is safe
        - UL4600 being presented at November 12 Executive Committee meeting
            - Will provide advice to the Executive Committee on whether this should take some form of legislation
        - Standard in a revision cycle now
        - Appropriate for this subcommittee to look at UL4600, continue talking through and evaluating whether it should be a standard in Washington

Topic Closed.

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

WASHINGTON STATE
AUTONOMOUS VEHICLE
WORK GROUP

MEETING SUMMARY

Open Discussion and Next Steps
Katy Ruckle & Michael Schutzler

- Looking to get momentum with this subcommittee, suggest meeting monthly
  - Session is coming up, privacy law will be going through committees, can provide monthly updates to this subcommittee
  - Suggestion to meet every 6 to 8 weeks
  - **ACTION ITEM**: Katy Ruckle to figure out meeting cadence and schedule series of subcommittee meetings
- Executive Committee meeting on November 12, 9:00am to 2:30pm
  - **ACTION ITEM**: Any meeting attendees interested in attending, contact Katy Ruckle to get more information
- Interest in seeing more information on the WA AV website, or elsewhere, what the state of play is, how things are changing in this space over time
  - What testing is occurring?
  - What are we hearing from industry?
  - Where is Washington on the roadmap for commercial testing?
  - *Noted the Executive Committee meetings present those types of status updates*
  - **ACTION ITEM**: Katy Ruckle to explore how to get some high-level information to this subcommittee

MEETING ADJOURNED.