# Subcommittee on Cyber Security and Data Privacy

Damien Riehl| Joshua Root

DEPARTMENT OF TRANSPORTATION

# Considerations

1. **DEFINITIONS** – The terms currently used in industry, statute, or rule may not align with how people or the law will interpret CAVs' newly revised "driving" experience.
   A. Driver vs. Operator
   B. Private Data

2. **CLASSIFICATION** – The Minnesota Data Practices Act's data-classification scheme will impact which CAV data is shared, how it could be shared, and with whom.
   A. Aggregate data vs. Specific data
   B. Commercial value vs. Obligation

3. **UNIFORMITY** – Will specific industry, federal, or early adopting states use a shared framework?
   A. Minnesota vs. the World (or at least North America)

# Considerations

4. **SECURITY** – The sooner security protocols are determined, the cheaper they will be.
   A. Standards (SOC vs. ISO vs. NIST vs. IEEE)
   B. Trust / Authenticate
   C. Score
   D. Immutability / Integrity

5. **PARTNERSHIPS** – This is an exciting area with a few early players. There is great knowledge, but be careful not to isolate new ideas. There can be more than one buggy whip.
   A. Winners vs. Losers

# Considerations

6. **REGULATORY** – In CAV, the government's role can help foster new development, while protecting the public from bad actors.
   - *A. Breach*
   - *B. MN vs. CA vs. NY vs. EU vs. CAN*
   - *C. Regulatory response vs. Private right of action*
   - *D. Opt In (Collection / Use / Sale)*
   - *E. Consumer Information*
   - *F. Disclose what data is being collected*
   - *G. Opt In (Collection / Use / Sale)*

7. **INEVITABLE CONSEQUENCE** – Start the process now: determine what data to collect, where it will be retained, and how it will be disseminated.
   - *A. Storage*
   - *B. Distribution*

# Recommendation 1: DEFINITIONS

The terms currently used in industry, statute, or rule may not align with how people or the law will interpret CAVs' newly revised "driving" experience.

A. *"Driver" vs. "Operator"*

B. *Private Data*

Our group thinks that with the advent of CAVs, the legislature should clarify two terms: "Driver" and "Private" data.

**Driver.** Currently, the term "driver" is a sliding-scale element that routinely means the person controlling the steering wheel. If the role of control is changing — from human to machine — then that term might be ripe for re-definition.

# Recommendation 1: DEFINITIONS

The terms currently used in industry, statute, or rule may not align with how people or the law will interpret CAVs' newly revised "driving" experience.

A. *"Driver" vs. "Operator"*

B. *Private Data*

**Private Data 1.** Control relates to another key term: "private." Our group had considerable conversations about how that term exists in statute, business, and common perception.

Regarding PII (personally identifiable information), we concluding that connected "talking" vehicles could share more personal information than the public is likely going to be comfortable with. Specifically, the group considered two privacy aspects:

(1) what information about a human is being shared and

(2) with whom.

# Recommendation 1: DEFINITIONS

The terms currently used in industry, statute, or rule may not align with how people or the law will interpret CAVs' newly revised "driving" experience.

A. *"Driver" vs. "Operator"*

B. *Private Data*

**Private Data 2.** People frequently share their PII with private companies, in exchange for services (e.g., Google), but that dynamic changes when that PII is shared with governmental entities.

As a first step, the legislature might consider expanding the definition of Private Data as it relates to data the government collects about humans who travel in vehicles. The public might not be comfortable with governmental sharing of sensitive data (e.g., pinpoint geolocation, driving habits) that CAVs may collect and communicate.

# Recommendation 2: CLASSIFICATION

The Minnesota Data Practices Act's data-classification scheme will impact which CAV data is shared, how it could be shared, and with whom.

1. *Aggregate data vs. Specific data*
2. *Commercial value vs. Obligation*

**Collection.** Carrying forward the theme of "What is private data?" — we also evaluated what data types governmental authorities will likely collect, create, store, or maintain. We also considered how both governmental entities and industry might use that data. We came to two general consensus elements:

(1) This data should be **anonymized** and **aggregated**, reducing attributability to a particular person, and

(2) The data likely has **value**.

# Recommendation 2: CLASSIFICATION

The Minnesota Data Practices Act's data-classification scheme will impact which CAV data is shared, how it could be shared, and with whom.

1. *Aggregate data vs. Specific data*
2. *Commercial value vs. Obligation*

Government may have a partnership opportunity with specific industry sectors regarding government-collected CAV data. But the data's potential commercial value could also complicate the governmental role.

Clarifying or setting policies around the data would help create both a uniform roadway user experience and data simplification.

# Recommendation 3: UNIFORMITY

Will specific industry, federal, or early adopting states use a shared framework?

1. *Minnesota vs. the World (or at least North America)*

Many states — Arizona, California, Michigan, and Minnesota (among others) — are currently considering how to integrate these new technologies into:

(1) the driver's experience,

(2) regulatory framework, and

(3) future planning.

We strongly urge Minnesota to not "go it alone." Rather, we should collaborate to help frame the future vision. As the ground solidifies about how machines, infrastructure, and humans are integrating this technology, Minnesota should adopt as much of that practice as practicable (considering our state-specific needs).

Rather than re-creating the wheel, we should identify where "the way it is" could work for us.

# Recommendation 4: SECURITY

The sooner security protocols are determined, the cheaper they will be.

1. *Standards (SOC vs. ISO vs. NIST vs. IEEE)*
2. *Trust / Authenticate*
3. *Score*
4. *Immutability / Integrity*

The single most important element of CAV vehicles is their security protocols. If the security is implemented poorly, no other element will have its anticipated effect.

Security is best “baked in” which means developers and policymakers need to emphasize “security by design.”

Much like the previous aspect (Uniformity), security standard-making provides an opportunity for Minnesota to pair with early adopters to pick a technology. We need to avoid the Betamax vs. VHS wars; rather than market fragmentation, we should help the industry consolidate around common security standards

# Recommendation 4: SECURITY

The sooner security protocols are determined, the cheaper they will be.

1. *Standards (SOC vs. ISO vs. NIST vs. IEEE)*
2. *Trust / Authenticate*
3. *Score*
4. *Immutability / Integrity*

We suggest that beyond the basic security backbone, Minnesota should also invest in systems that permit building relationships with changing technology.

Like human relationships, identifying/building relationships with technology can increase its credibility — and infrastructure's ability to rely on that relationship.

# Recommendation 5: PARTNERSHIPS

This is an exciting area with a few early players. There is great knowledge, but be careful not to isolate new ideas. There can be more than one buggy whip.

1. *Public-private partnerships*
2. *Maps / Mapping*

**Partnerships.** In the CAV space, private industry is seeing great competition and investment — at a level that government is unlikely to match. Large-scale investment leads to increased innovation.

As such, Minnesota may want to consider partnering with private industry to both:

(1) increase the availability of CAVs' benefits, as well as

(2) further and enforce Minnesota's obligations to maintain safety standards.

The state's policies should incentivize public/private cooperation through partnerships.

# Recommendation 5: PARTNERSHIPS

This is an exciting area with a few early players. There is great knowledge, but be careful not to isolate new ideas. There can be more than one buggy whip.

1. *Public-private partnerships*
2. *Maps / Mapping*

**Maps.** The group also discussed private-industry partnerships for maps/mapping.

The State has a role in reporting what is being done on roads (e.g., construction, detours), which could impact CAVs' performance.

Certain roads may have higher or lower "trust" levels and CAV-capability.

Similarly, map attributes (e.g., streets, lanes, potholes) might have a variety of sources (e.g., government, industry, individuals).

The state should consider staffing and funding a system that assesses the reliability of map data and its sources. And additional research and partnering is required to define the state's role.

# Recommendation 6: REGULATORY

With CAV, the government's role can help foster new development, while protecting the public from bad actors.

1. *Breach*
2. *MN vs. CA vs. NY vs. EU vs. CAN*
3. *Regulatory response vs. Private right of action*

**Breach.** Where there is data (information), there will be a breach.

**Multi-jurisdiction.** Minnesota has one of several successful data classification and breach systems that have developed, in addition to California, New York, the EU, and Canada. We believe that Minnesota's requirements are fair, even with changing technology. But some enhancements may provide increased certainty for business sectors.

**Regulatory response vs. Private right of action.** We believe that given the known issues, legislators and regulators should consider explicit guidance, rather than requiring people and industry to rely upon policy being made through costly and uncertain litigation.

# Recommendation 6: REGULATORY

With CAV, the government's role can help foster new development, while protecting the public from bad actors.

1. *Breach*
2. *MN vs. CA vs. NY vs. EU vs. CAN*
3. *Regulatory response vs. Private right of action*

**Consumer information.** We see great room for improvement on consumer notice and protection.

**Disclosure.** Data collectors (governmental and private) must disclose what data the CAV is collecting about people. And the data-collection purpose should be clear (e.g., traffic flow, road conditions, safety, emissions).

**Opt-in** language can help consumers chose what data they are willing to share, and with whom. Specifically, we discussed three areas where opt-in is preferred:

(1) collection (likely by OEMs),

(2) use (likely both OEMs and trusted suppliers), and

(3) sale (controlling who may buy data about people).

# Recommendation 7: INEVITABLE CONSEQUENCE

Start the process now: determine what data to collect, where it will be retained, and how it will be disseminated.

1. *Collection*
2. *Storage*
3. *Distribution*

**Collection.** Because CAVs are able to generate enormous amounts of sensitive data, government should first identify:

1. what data government needs
2. for how long, and
3. what triggers destruction.

**Storage, format, and necessity.** After that, government should identify:

1. how to store it,
2. where to store it, and
3. whether to collect/store it at all.

**Distribution.** Who has access?

The best way to prevent data from being improperly being accessed: don't have the data at all.

# Questions?

# Thank you again!