JANUARY 13, 2020

GOVERNOR'S ADVISORY COUNCIL ON CONNECTED & AUTOMATED VEHICLES

Connectivity and Data Committee

Connectivity, Data, Privacy and Cybersecurity

DESTINATIONCAV

DEPARTMENT OF TRANSPORTATION

WELCOME

Margaret Anderson Kelliher, Co-Chair
Commissioner, MnDOT

Phil Magney, Co-Chair
CEO and Founder, VSI Labs

1

AGENDA

1. Welcome
2. Council mission, vision and values
3. Overview of CAV data opportunities and challengse
4. Connectivity and Data Committee Goals and Priorities
5. Conversation with Council
6. Public Comment
7. Closing

COUNCIL MISSION & VALUES

TARA OLDS, MNDOT CAV-X OFFICE

2

GOVERNOR'S COUNCIL ON CONNECTED AND AUTOMATED VEHICLES CHARTER

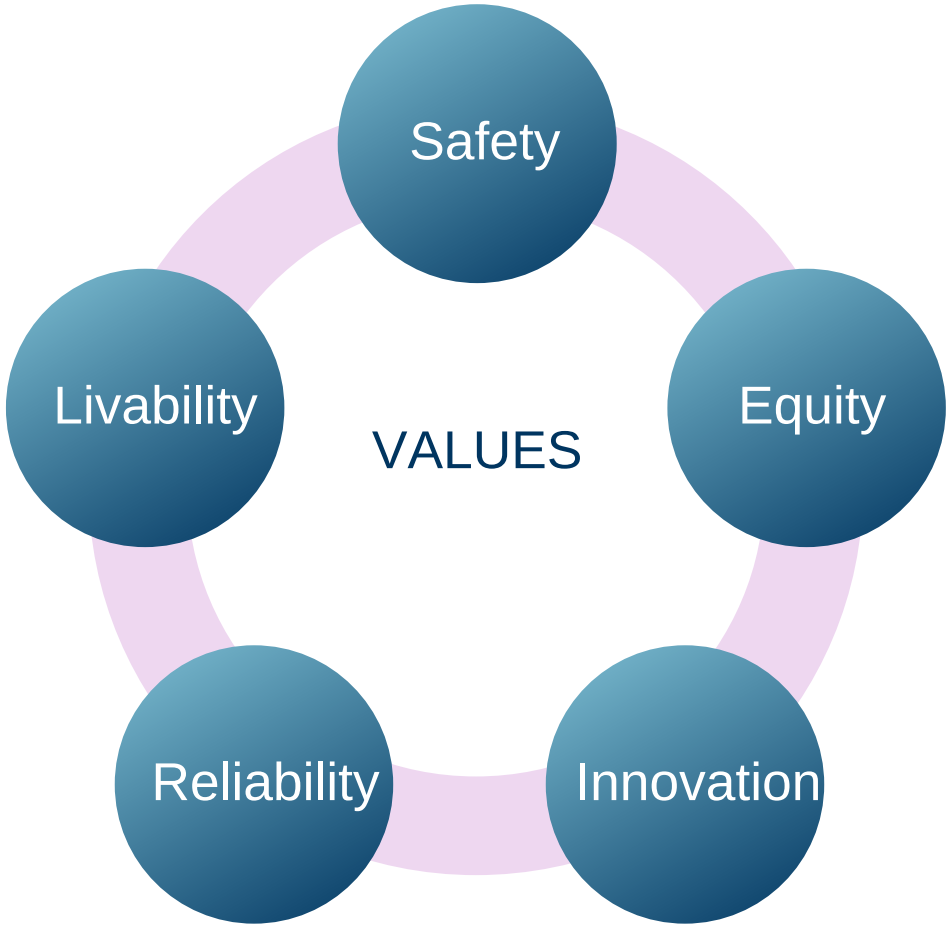
OUTLINING THE COUNCIL'S VISION, MISSION, GOALS, AND SHARED VALUES

VISION

Building a future of transportation system that is safe, equitable, accessible, efficient, healthy, and sustainable

MISSION

The Governor's Council on Connected and Automated Vehicles collaborates with stakeholders, partners with academic institutions and private industry, and engages communities to prepare Minnesota for a future with emerging transportation technologies



ADVISORY COUNCIL GOALS

WHAT IS THE COUNCIL WORKING ON IN THE NEXT 4 YEARS?

2020 PRIORITIES	2021-2023 PRIORITIES
1. Equity, mobility, accessibility, public health and environment 2. Industry and research partnerships 3. Education, outreach, engagement and demonstrations/pilots to educate communities and decision-makers	4. Infrastructure investment 5. Law for safe testing and deployment 6. Economic and workforce development 7. Data privacy and cyber security 8. Insurance and liability 9. Alignment with other states and federal government and sharing best practices 10. Human factors and impacts of CAV on users

INNOVATION ALLIANCE COMMITTEES

OVERVIEW OFCAV DATA OPPORTUNITIES & CHALLENGES

- *Industry perspective on CAV data, cybersecurity and privacy*
  Phil Magney, VSI Labs
- Industry perspective
  Suzanne Murtha, National Lead for Connected and Automated Technologies, AECOM
- *MnDOT's CAV data pilots and cybersecurity challenges and opportunities*
  Cory Johnson and Brian Kary, MnDOT
- *Government data and privacy issues*
  FrankDouma, University of Minnesota

3

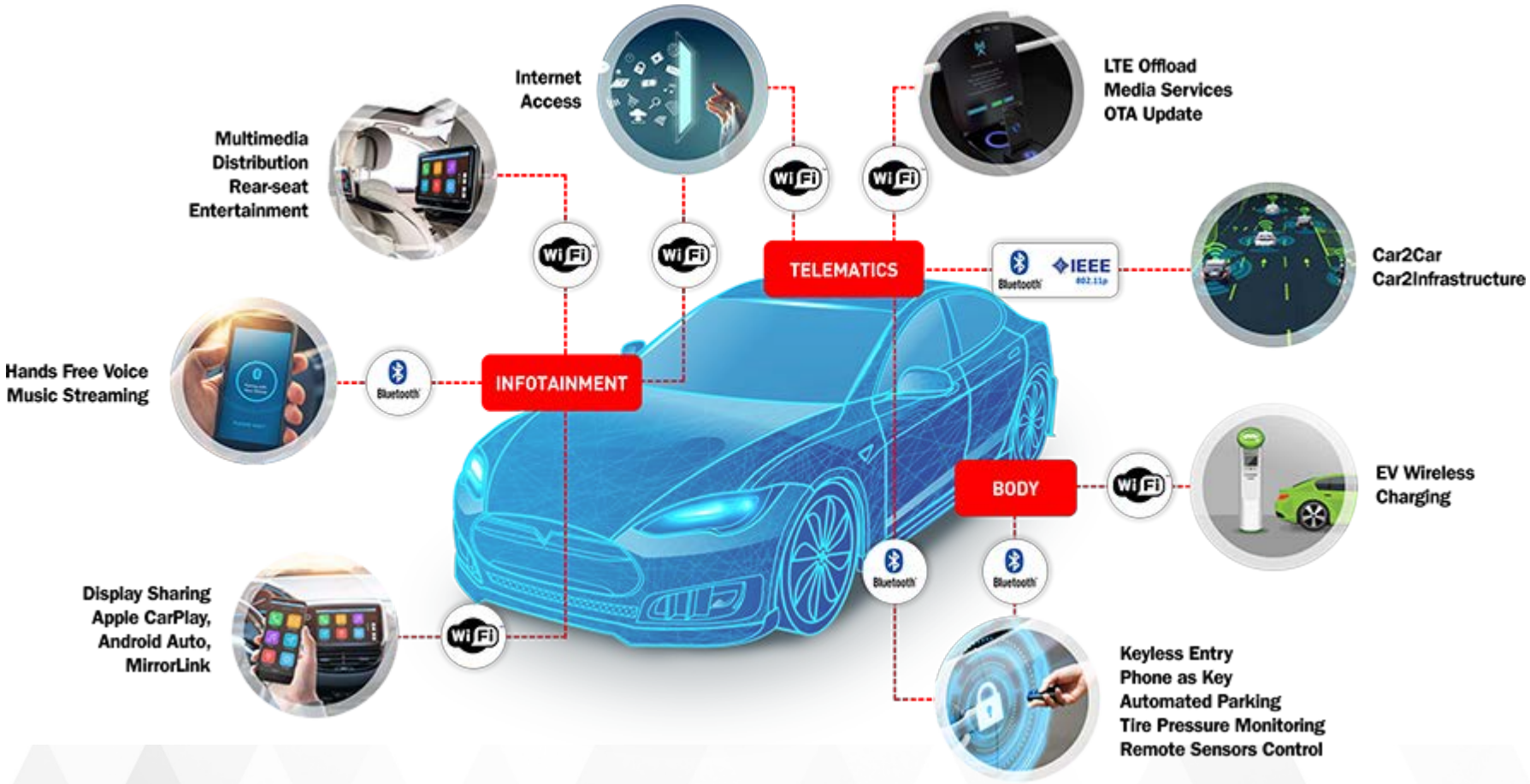
OPPORTUNITIES & CHALLENGES WITH CAV DATA

- Emphasize and reinforce the purpose of the Council
- Working with a valuable commodity: Data
- Future of transportation will run on data, not gasoline. But like gasoline data is vol
  Need to be careful in how we gather, use and share data.
- Can refine data to extract what we need.

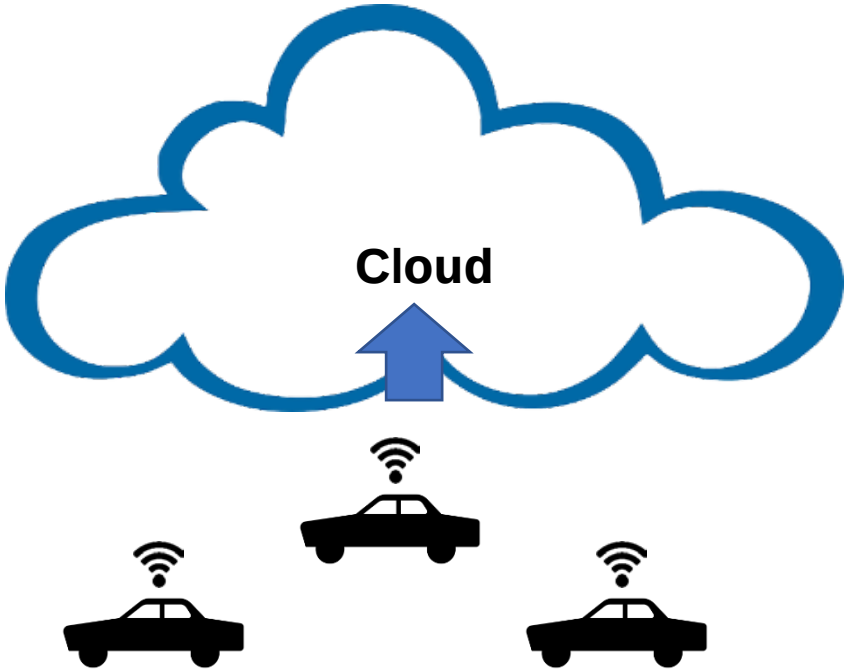
The Current Status of Car Connectivity

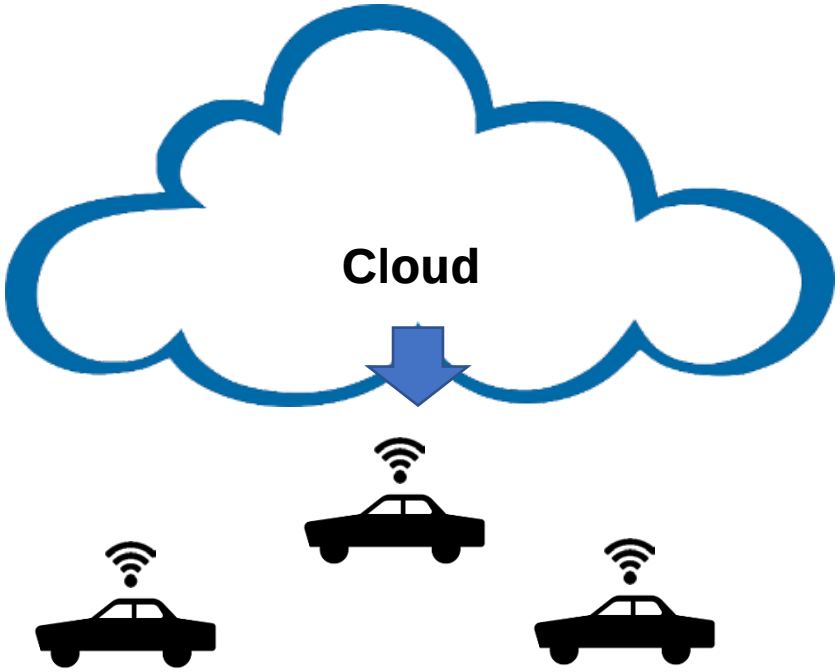
- Nearly half of all cars sold have an embedded cellular modem (telematics)
- Nearly all cars sold have provisions to connect with a smartphone (Bluetooth)
- Very few cars today come with embedded Wi-Fi
- Few cars sold today support any kind of advanced connectivity
  - For OTA (over-the-air) updates

Today's Connected Car



The IoT Stack – The Future of CAV





Data Collection

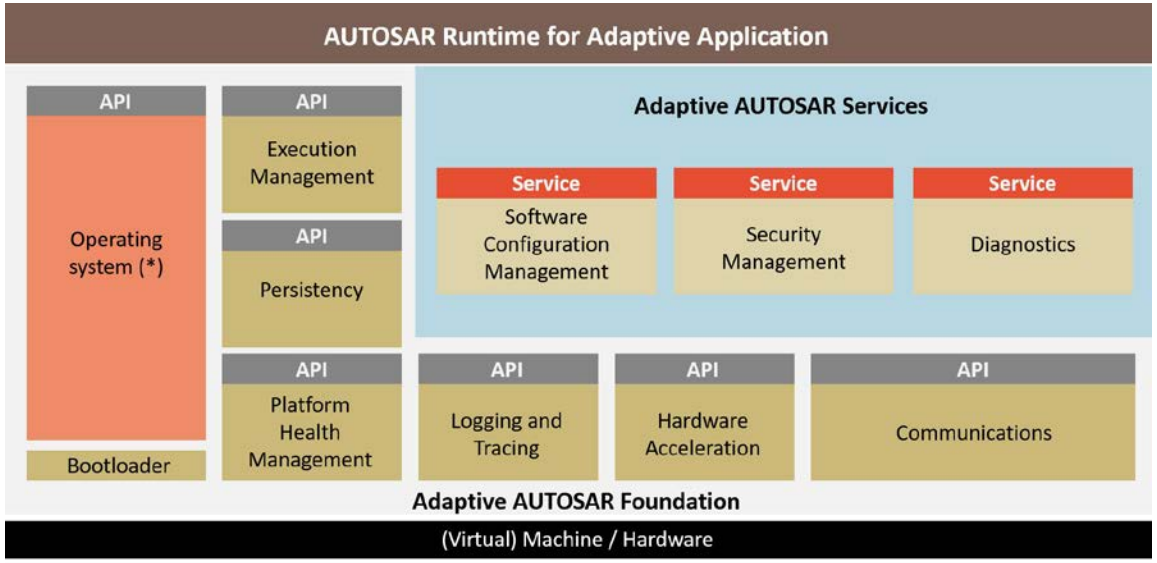
- Sensor data for training AI-based algorithms
- Vehicle performance & diagnostic information
- Record objects for localization assets
- Map change detection
- Road surface condition
- DBUF

Data Distribution

- Software updates – new features
- Firmware updates to distributed ECU systems
- Realtime maps
- Realtime correction data
- Road surface conditions
- Work Zones

Keeping it Secure – Adaptive AUTOSAR

- Vehicle-to-vehicle (V2V), Vehicle-to-everything (V2X), remote diagnostics, and cloud-based analytics are part of the connected vehicle paradigm.
- V2X systems require secure communication with other vehicles and off-board systems.
- Next-gen vehicles will be connected to other vehicles, smartphones, traffic infrastructure, etc. and in-vehicle V2X applications will be required to be updated over the air (OTA).



Adaptive AUTOSAR is both an interface specification and a runtime layer to assure safety at the deepest level!

AECOM Imagine it. Delivered.

Connected and Automated Vehicles Data and Privacy

Suzanne Murtha

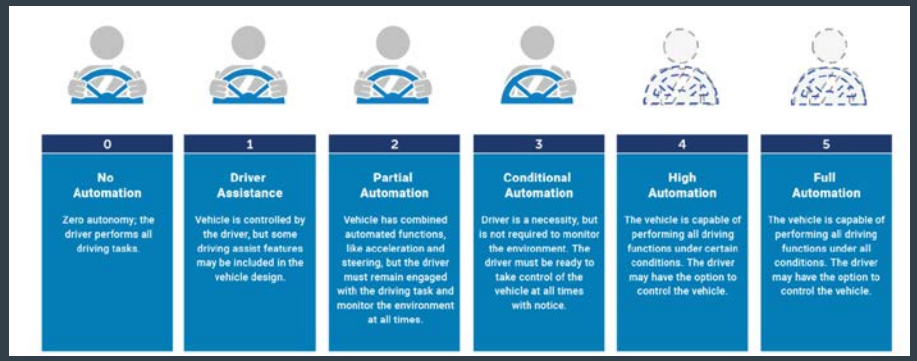
What are Connected or Automated Vehicles?

Connected Vehicles

Where a vehicle communicates with something outside itself

- Another vehicle
- Pedestrians
- Infrastructure (signals)
- Buildings
- Parking
- Toll systems

Automated Vehicles



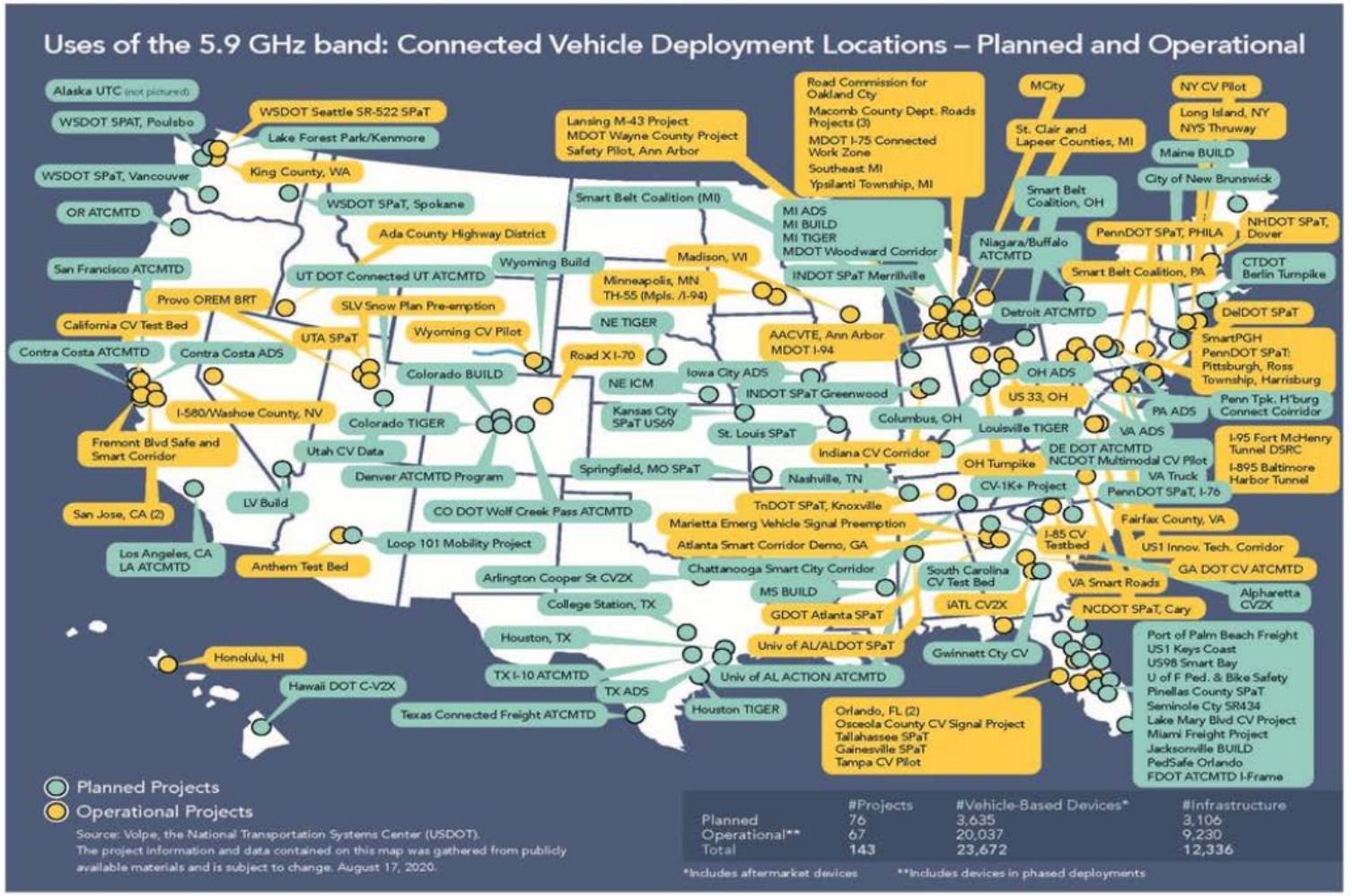
Where some or all driving task is done by a machine

- Braking
- Steering
- Speed changes

AECOM

Connected Vehicle Deployments in the US

The Safety Band at Work: Current Deployments



Pending Applications to the FCC for Use of the Safety Band (by State)*

State	Applications
CA	4
CO	25
FL	499
GA	123
MD	17
MI	149
NE	9
NV	8
NY	50
OH	29
PA	2
TN	1
Total	**916**

*As of July 17, 2020

Cybersecurity

Pre-2021

SCMS, other security concerns

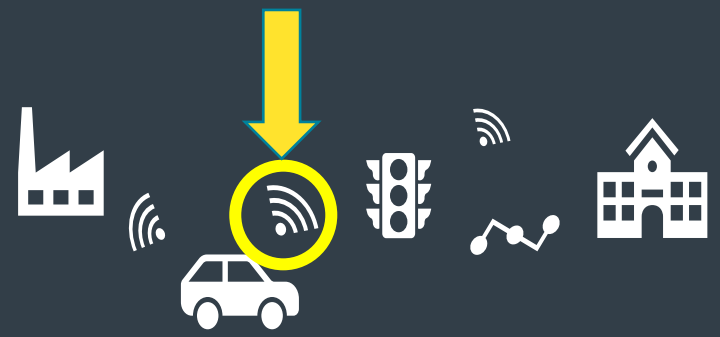
No formal national cyber standards/best practices for ITS or CV/AV deployments

Now

- Data may now largely bypass infrastructure and shift to OEM to IOO**, potentially lessening cyber security risk to governments**
- Think physical security, locking cabinets are biggest risk

AECOM

Privacy Concerns



V2I

- No publicly identifiable information (PII) except opt-in (tolling)
- Small bandwidth
- SCMS
- Low risk of privacy violations

Telematics

- Vehicle owners agree to share data when they buy the vehicle
- Data transaction between vehicle and OEM, not government
- No risk of privacy violations to government

CV/AV Transit

First/Last Mile

www.automatedbusconsortium.com

eVTOL

AECOM

Thank you

Suzanne Murtha
National Lead CV/AV Tech
AECOM
Suzanne.murtha@aecom.com

AECOM

Imagine it.
Delivered.

Government Data and Privacy Issues

Frank Douma, State and Local Policy Program

HUMPHREY SCHOOL
OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

DATA PRIVACY, SAFETY AND SECURITY

Data Privacy v. Security

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

- Related, but not the same

- Security
  - Protect collected data from unauthorized use

- Privacy
  - Whether data collection is appropriate
  - Once collected, whether data used for appropriate purposes
  - Appropriateness can be set by law or contract

Why Does Privacy Matter?

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

Public policy &/or public opinion can restrain data use and collection because of privacy concerns.

Privacy concerns may limit the deployment of otherwise socially beneficial technologies.

Lessons From History

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

- **With privacy, public perception matters as much as legal reality**
- Increased safety or efficiency rationales only go so far to offset privacy concerns
- Tackling privacy issues at the outset of technology development can reduce privacy related deployment risks

“Right to Privacy”

- No single legal source
  - Arises piecemeal from narrow laws and interpretation of constitution by courts
  - No fixed meaning, evolves as society and technology changes.
- Federal constitution and laws set baseline
- States can (and do) increase protections

Transportation Data Privacy

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

- There is no comprehensive statutory privacy regime

- *Katz* Test (1967)
  - There is a protected privacy right when:
    1) An individual has an expectation of privacy; and
    2) Society recognizes that expectation as reasonable

- *U.S. v. Knotts (1983)*
  - A person traveling in an automobile on public thoroughfares has ***no reasonable expectation of privacy*** in their movement.

Transportation Data Privacy

- *City of Ontario v. Quon (2010)*
  - Both technology and its meaning in society changing too rapidly for Court to define a reasonable privacy expectation
  - Supreme Court reluctant to make new privacy rules

- *U.S. v. Jones* (2012)
  - GPS unit attached to suspect's car and tracked for a month
  - Ruling: police need a warrant to do this
  - Justices do not agree on rationale/test

Transportation Data Privacy – Mobile Telephone Data

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

- *Riley v. California (2014)*
  - Data from Mobile phone searched incident to arrest
  - Ruling: police need a warrant to do this
  - Phone = "minicomputer"
  - Would transportation / location data fit this definition?

- *Carpenter v. US* (2018)
  - Location data from Cell phone towers
  - 21st "Pen Register?"
  - Ruling: No, police need a warrant to do this

Personal Information

- Federal law is a source for personal information protections.
- Chapter 13 is less robust.
- You will find protections for personal information elsewhere in Minnesota law, especially as related to data breaches.

The Data Practices Act

- Defines “government data”
- Presumes government data are public and available to view and inspect
- Classifies certain data as not public
- Provides rights for the public and data subjects
- Requires that not public data are only accessible to those whose work assignment reasonably requires access

Classification	Meaning of Classification	Example
Public	Available to anyone for any reason	Name of employee
Private / Nonpublic	Available to: • Data subject (and persons authorized by data subject) • MnDOT employees whose work requires access or other entities authorized by law	Social security numbers Employee identification numbers
Confidential / Protected Nonpublic	Available to: • Not available to data subject • MnDOT employees whose work requires access or other entities authorized by law	Active investigative data

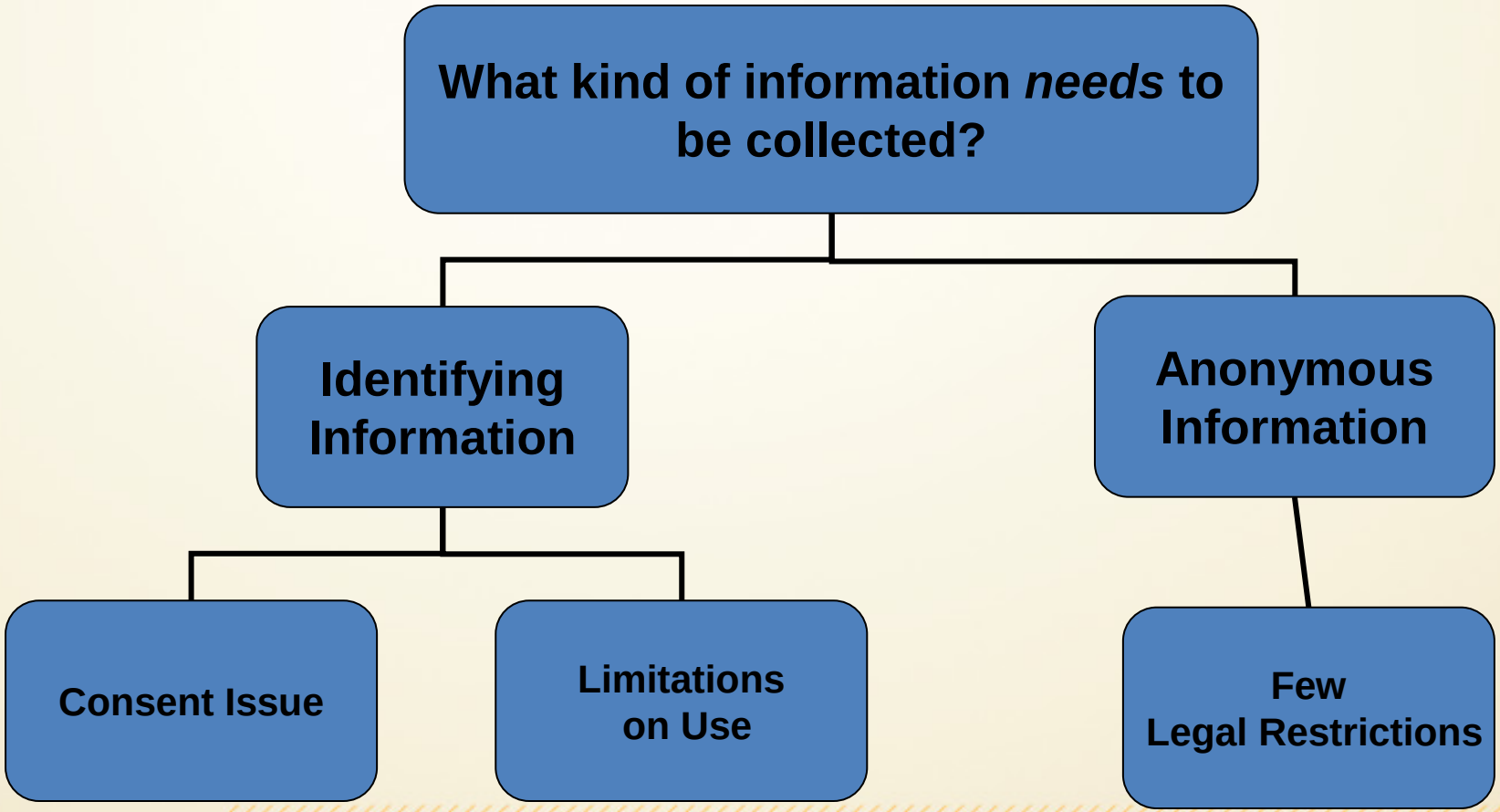
General Nonpublic Data, 13.37

- "Security Information" means government data the disclosure of which the [government entity] determines would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, or illegal disclosure.
- "Security information" includes … global positioning system locations.

Data Breaches, 13.055 / 325E.61

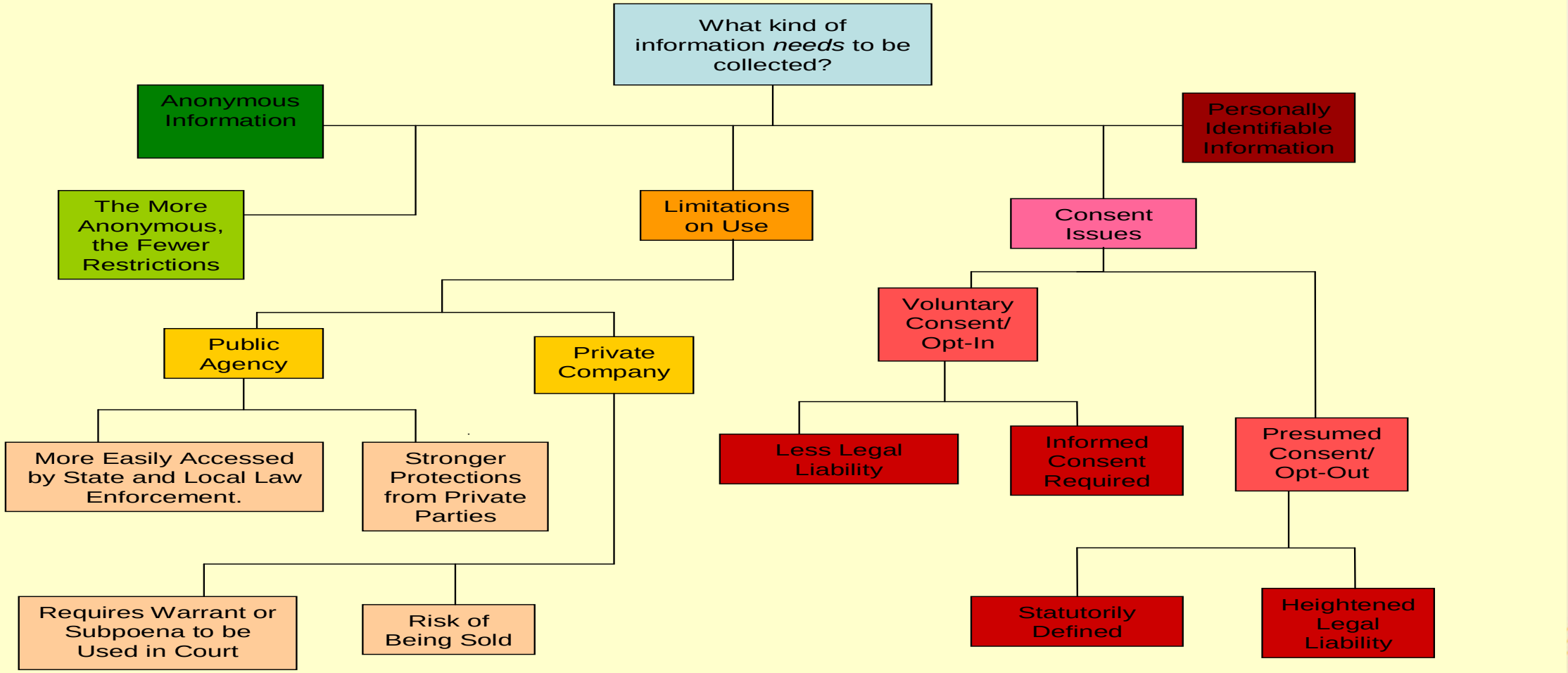
- Unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data.
- Includes data maintained by a person under a contract with the government entity that allows the government to access the data.
- Requires the government entity to disclose, notify, investigate, and report.
- 325E.61 extends similar requirements to non-governmental entities possessing personal information.

Privacy Legal Toolbox



ITS Privacy Legal Toolbox

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA



"Intelligent Transportation Systems: Personal Data Needs and Privacy Law" Transportation Law Journal, 39(3) Winter p.97 (2012)

Taxonomy of ITS Privacy Issues

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

- Type of observation
- Observation purpose
- Vehicle information/ID
- Personal information/ID
- Privacy expectation

Examples

HUMPHREY SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

Type of observation	Observation purpose	Vehicle information /ID	Personal information/ID	Privacy expectation
Anonymous individual vehicle observation Loop detector	Managing system use	None obtained	None obtained	None
Anonymous occupant observation Infra-red lane scanner	Regulation of transportation facilities	Unique vehicle identification obtained	Anonymous information about number of occupants; possibly gender and age.	Low
Individual vehicle observation & data Toll Transponder	Regulation of transportation facilities	Unique vehicle identification obtained	Owner information identified through vehicle registration system	Medium
Individual vehicle observation & data Red light camera	Civil or criminal sanction	Unique vehicle identification obtained	Owner information identified through vehicle registration system	High
Individual driver identification Biometric (voice ID)	Criminal charges	Unique vehicle identification obtained	Driver identified through vehicle registration and licensing system	Highest

Anonymous Individual Vehicles

PRIVACY EXPECTATION:

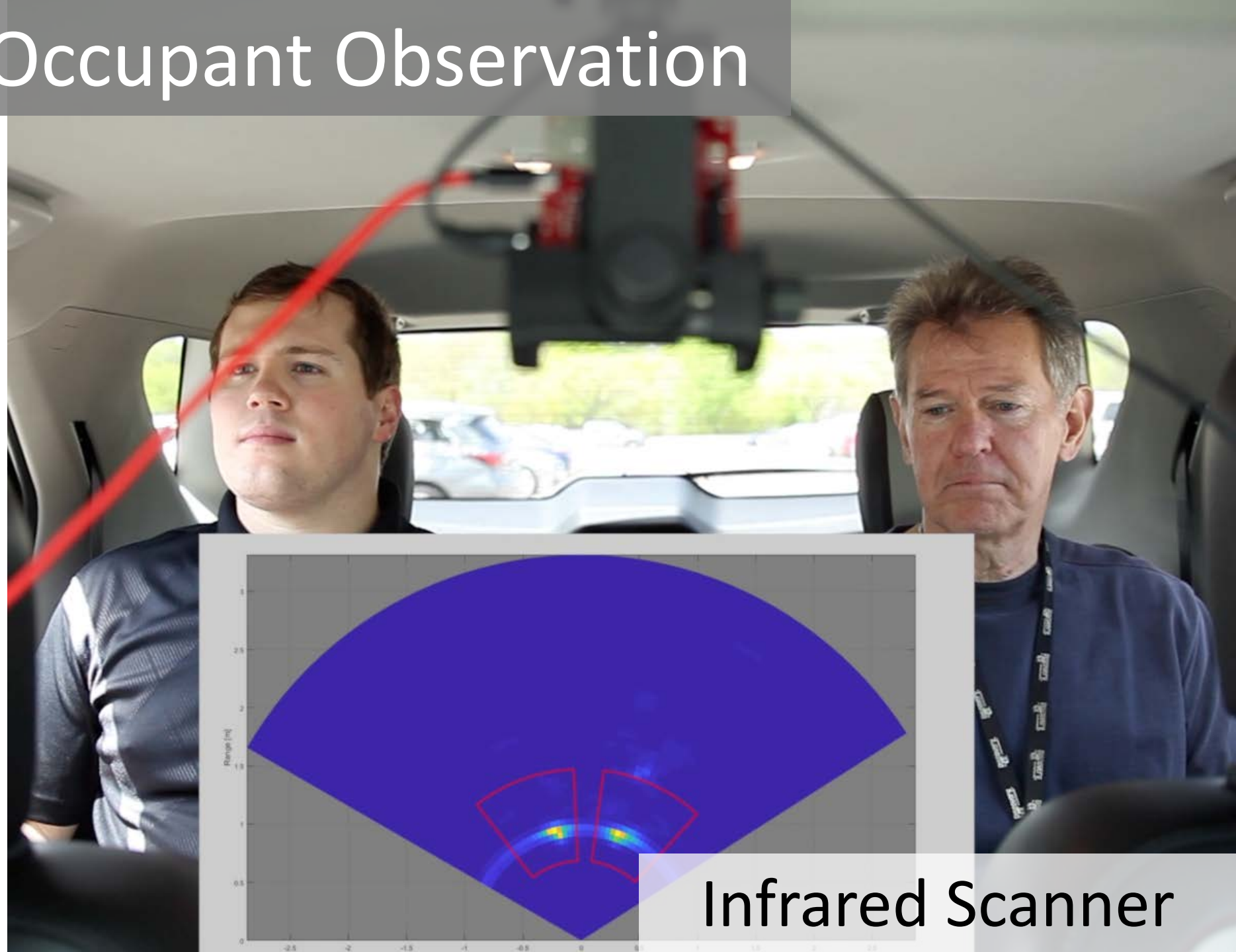
NONE

Pavement Loop Detectors

Anonymous Occupant Observation

PRIVACY EXPECTATION:

LOW

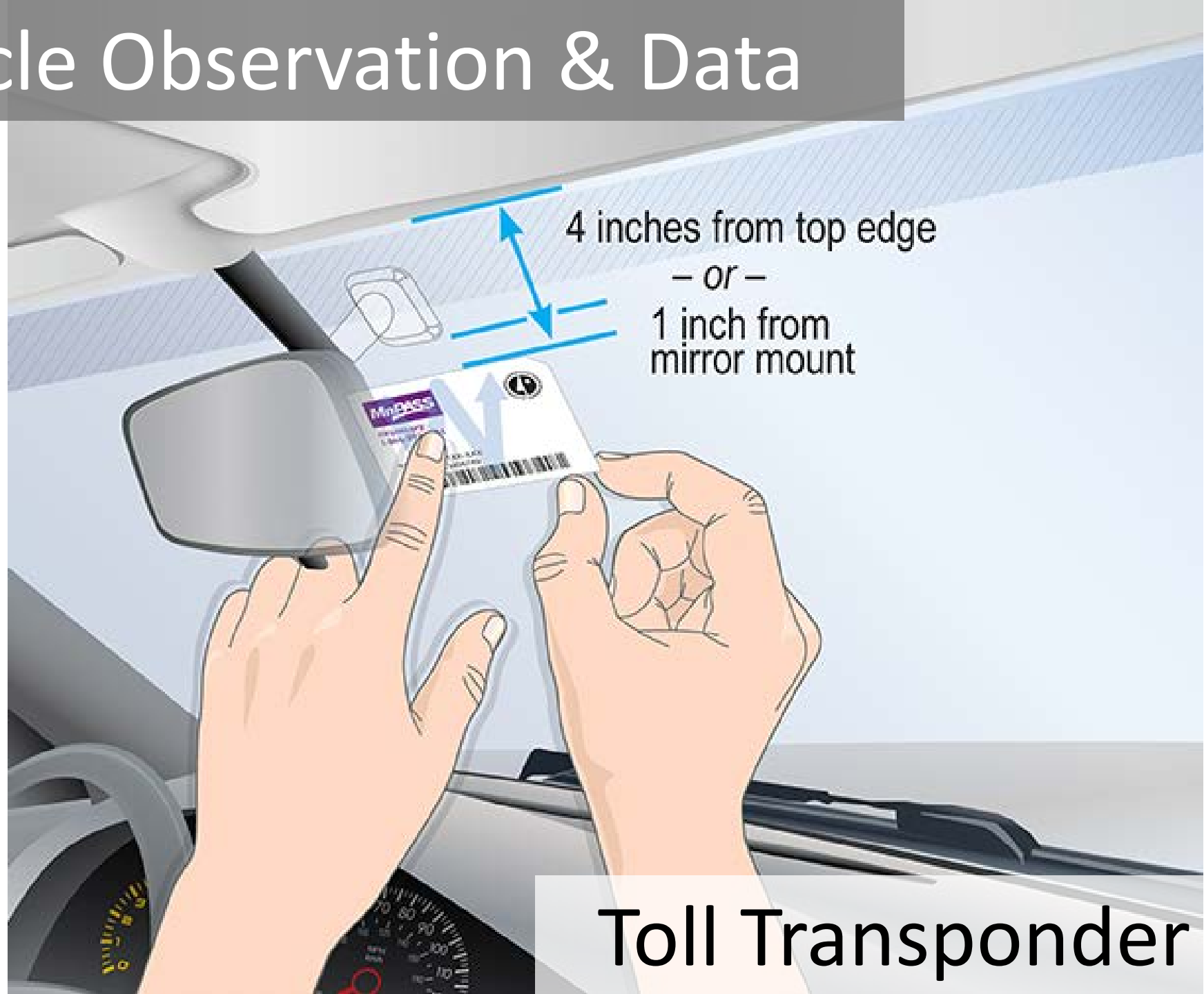


Infrared Scanner

Individual Vehicle Observation & Data

PRIVACY EXPECTATION:

MED



Toll Transponder

Individual Vehicle Observation & Data

PRIVACY EXPECTATION:

HIGH

Red Light Camera

Individual Driver Identification

PRIVACY EXPECTATION:

HIGHEST

Biometric (e.g., Voice ID, Face ID)

HUMPHREY SCHOOL
OF PUBLIC AFFAIRS
UNIVERSITY OF MINNESOTA

THANK YOU

Frank Douma
Humphrey School of Public Affairs
University of Minnesota
612-626-9946
Fdouma@umn.edu

MnDOT's CAV Data Pilots

Brian Kary | Director of Traffic Operations

MnDOT Regional Transportation Management Center

Cory Johnson | CAV/ITS Program Lead

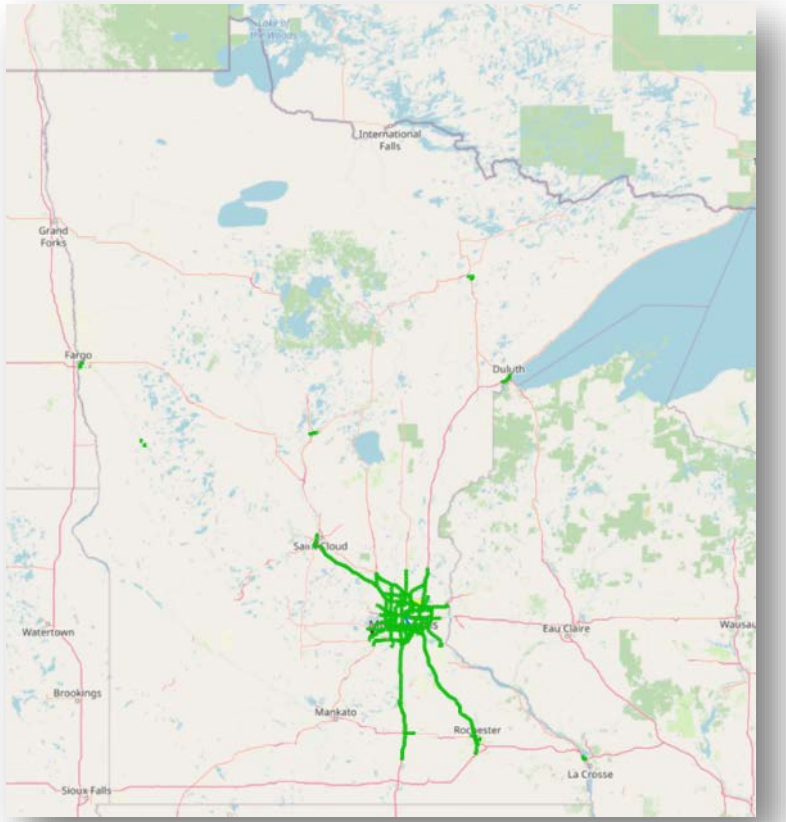
MnDOT CAV-X Office

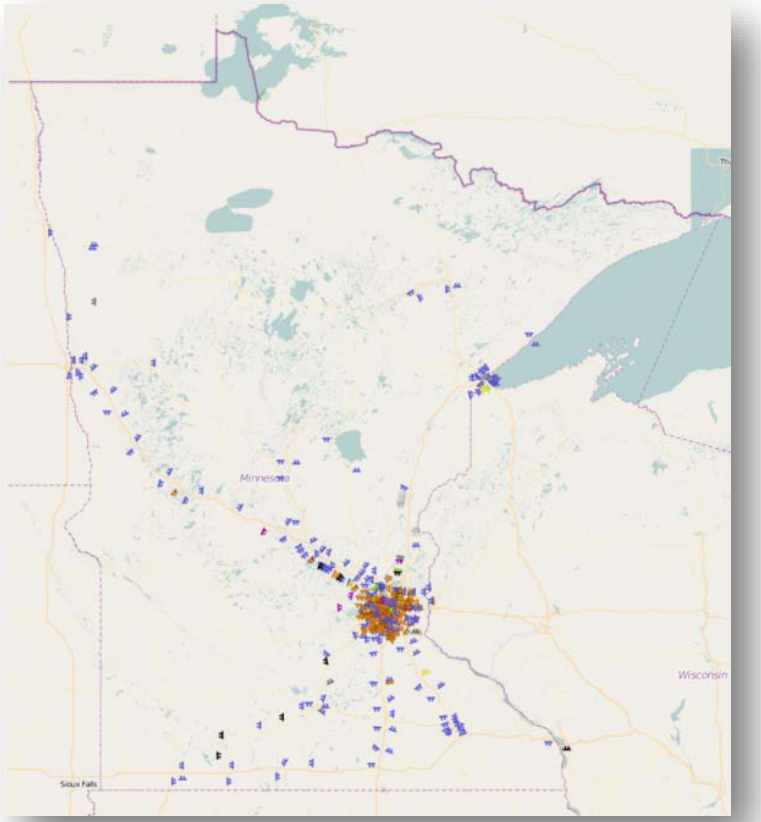
Regional Transportation Management Center

- Shared Operations Center
  - MnDOT Freeway Operations
  - MnDOT Signal Operations
  - MnDOT Maintenance Dispatch
  - State Patrol Dispatch
- Traffic Management System
  - 1000 Cameras
  - 400 Changeable Message Signs
  - 400 Ramp Meters
  - 890 Traffic Signals

MnDOT RTMC Network

- Dedicated network for traffic management communications
  - Fiber communications network, cellular devices, radio modems, VRF





Network Cybersecurity

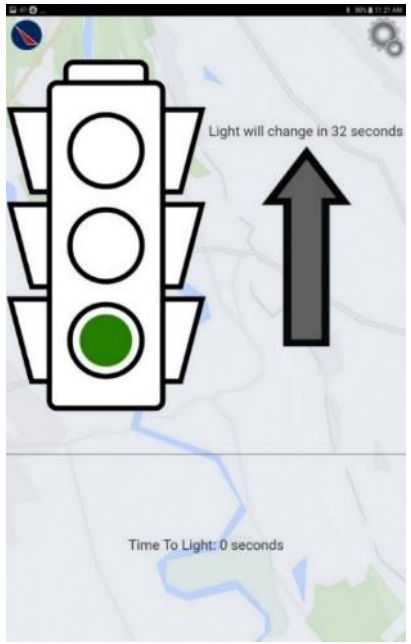
- Control network access for users and devices
- Physical security of field shelters and cabinets
- Central Logging of Activities
- Segmentation of Network to Restrict Movement
- System Scanning for Vulnerabilities

MnDOT RTMC Data

- Traffic Sensor Data
  - Primarily on metro area freeways
  - 30-second volume and speed data used for ramp meter timing, travel times, queue warning, MnPASS pricing, etc.
  - Database going back 20+ years
- 3rd Party Probe Data from HERE
  - Data from AVL systems, navigation devices, or cell phones
  - Statewide data providing speed and travel times
- StreetLight Data
  - Similar data to HERE but data is packaged to provide origin/destination patterns which is good for corridor planning studies.

Connected Corridors – Urban

Connected Corridors – Delivery



Planned, designed and deployed by a consortium of partners

- MnDOT
- Minnesota Department of Information Technology (MnIT)
- Consultants and vendors
- Local governments located along corridor

Lessons Learned

The program was valuable to MnDOT even though the technology remains uncertain and ever changing

- Security and networking protocols
- Foundational infrastructure and systems
- Organizational capacity
- Understanding of technology readiness
- Operations and maintenance

Next steps

Evaluation and improvement:

1. Physical hardware footprint- Do we need all this field equipment?
    - No – “Smart Snelling” project
2. Data sharing approach- Can we just share the signal data from central server?
    - Yes – “3rd Party data sharing” project
3. Are there other solutions where we can share central data sources?
    - Yes – “Connected vehicle traveler alert” project

CONNECTIVITY & DATA COMMITTEE GOALS & PRIORITIES

Co- Chairs Damien Riehl and Frank Douma

COMMITTEE GOALS

WHAT DO WE WANT TO ACHIEVE?

1. Determine DOT/CAV Data Needs
2. Develop privacy principles
3. Develop a high-level Policy Framework Document
4. Identify privacy/security by design best practices
5. Find ways to collaborate with private sector

COMMITTEE WORK PLAN

SPECIFIC TASKS TO ACCOMPLISH OUR GOALS

Short-Term Goals (2021)	Mid-Term Goals (2022)	Long-Term Goals (2023-2024)
1. Determine DOT/CAV data nee 2. Develop privacy principles 3. Develop a high-level policy framework Document (includin retention standards) 4. Identify best practices for privacy/security by design 5. Find ways to collaborate with private sector	1. Identify what CAV data MnDO has/the state needs 2. Review state law on CAV signal priority and develop CAV priority policy 3. Conduct a Work zone data exchange pilot	1. Develop a plan to collect/analy (or decline to collect/analyze) various 3rd party CAV data 2. Develop design standards for fiber installation 3. Develop CAV network integration guidance/security policy 4. Pilot a CAV network management system

COMMITTEE WORK PLAN

SPECIFIC TASKS TO ACCOMPLISH OUR GOALS

#	Committee Goals	Tasks	Deliverable	Lead(s)	Timeline	Alignment with Council and CAV Strategic Plan	Resources
1	Develop privacy principles	Review resources and best practices on CAV privacy principles (including Integral Mobility Management Architecture [IMMA] Privacy Architecture and Future of Privacy Forum's Privacy Playbook for Connected Car Data). Identify areas/fields of "personally identifiable information" (PII) that are most likely to be implicated by current and near-term CAV efforts.	Develop principles to help define "personally identifiable information" in the context of connected and automated vehicles. Create a summary document/white paper that summarizes the best practices and fields of PII, including the handling of CAV PII	Damien Riehl Frank Douma	January 2021	**Advisory Council Executive Report (Rec. # 96-98)** Update Minnesota Data Practice Act to address CAV Data and protect personal data by anonymizing, aggregating and summarizing private data. **CAV Strategic Plan (Rec. # 30)** Revise the definition of "personally identifiable information" to align with federal standards, address what private data is shared and with whom it is shared with.	Staff time
2	Develop a Policy Framework Document	Review other states and federal best practices (including Europe's General Data Protection Regulation [GDPR] and California's Consumer Privacy Act). Identify privacy values that support and conform to existing law and public expectations, including: 1. Identify what PII can or cannot be collected by CAV technologies 2. Prescribe what, if any, PII may be shared with other companies/organizations 3. Address who, if anyone, can share PII, and with whom.	Develop a policy framework document. Assess whether framework operates within existing legislation, or outlining key provisions in a bill. Draft definitions related to Goal 1 (e.g., define "personally identifiable information").	Damien Riehl Frank Douma Craig Gustafson?	April 2021	**Advisory Council Executive Report (Rec. # 99)** Clarify and set policies around data to create both a uniform roadway user experience and simplify data. **CAV Strategic Plan (Rec. # 30)** Revise the definition of "personally identifiable information" to align with federal standards, address what private data is shared and with whom it is shared with.	Staff time
3	Find ways to collaborate with private sector	Engage Minnesota companies and private industry to identify opportunities and challenges for data collection and connected vehicles. Identify 3 companies and host offline meeting.	Meeting summaries, outlining 1-3 next steps on how industry can support the state's CAV goals. If they do, optional CAV Challenge Stage 1	TBA	March 2021	**Advisory Council Executive Report (Rec. # 102)** Partner with industry to adopt common security standards and avoid adopting specific technologies.	Staff time May require allocation of CAV Challenge funding
			meeting to discuss partnership.				
4	Retention standards for CAV data	Review other states' laws on CAV data retention and government data classifications. Develop MnDOT policy on CAV data retention.	Document summarizing other states' CAV data laws Draft CAV data retention schedule	Craig Gustafson Eric Bell Damien Riehl? Kristin White	Dec. 2020 April 2021	**Advisory Council Executive Report (Rec. # 100)** Adopt other state, federal, and international best practices for uniform data storage, collection and use. **CAV Strategic Plan (#35)** Update Agency Data Stewardship and Records Retention Policies to Address CAV Data	Staff time
5	Identify security by design best practices	Identify potential "privacy by design" and "security by design" best practices (e.g., OWASP) that stakeholders might consider implementing.	Best practices document shared on website	?	Mid-term/ 2021-2022	**Advisory Council Executive Report (Rec. # 101)** Adopt security-by-design to integrate security protocols early in applications, which significantly minimizes costs	Staff time
6	Determine DOT/CAV data needs.	Identify and understand which data fields the DOT and/or CAV teams collect, desire, or anticipate in the current and near-term.	Add results to summary document/white paper discussed above.	? (MNDOT?)	March 2021	**Advisory Council Executive Report (Rec. # 96-98)** Update Minnesota Data Practice Act to address CAV Data and protect personal data by anonymizing, aggregating and summarizing private data.	Staff time
7	Identify what CAV data MnDOT has/the state needs	Develop a list of CAV data and metadata that MnDOT/MnIT (1) can access currently and (2) to which it will likely have access in the short-, mid-, and long-term horizons. Identify what of this data raises privacy and/or security issues, and which ones do not (e.g. SPAT data).	Documented list	Brian Kary Steve Misgen Cory Johnson Ray Starr Jed Falgren ?	April 2021	**CAV Strategic Plan (Rec. # 14, 37)** Research Data Use models and identify data needs to sources to support MnDOT Operations.	Staff time

- View "Connectivity and Data Charter" for full details

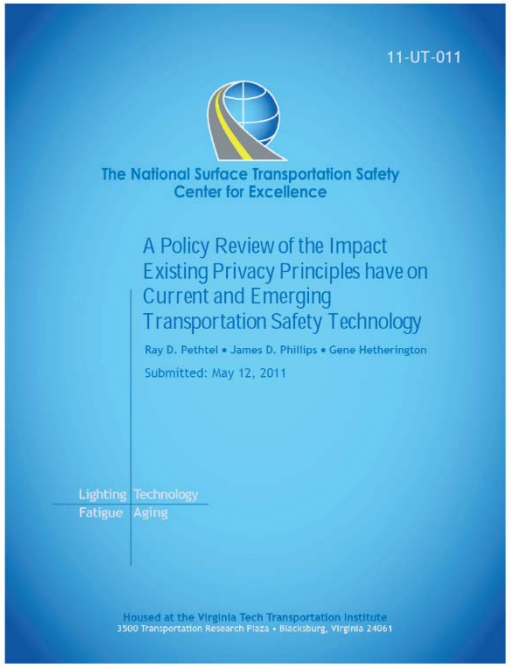
MINNESOTA PRIVACY PRINCIPLES

CREATE A SUMMARY DOCUMENT SUMMARIZING BEST PRACTICES AND FIELDS OF PII BY JANUARY 2021

1. Reviewed int'l resources and best practices
   - Minnesota Gov't Data Practice Act (MGDPA)
   - General Data Protection Regulations (GDPR)
   - Calif. Consumer Privacy Act (CCPA)
   - Automotive Future Mobility Connected Car Principles
   - Integral Mobility Management Architecture (IMMA)
   - Shared Use Mobility Center/Twin Cities Shared Mobility Collaborative principles
   - Washington state law
   - Uniform Law Commission model code
2. Developed list of common themes

COMMON PRIVACY THEMES

1. Consent
2. Opt out/non-discrimination/choice
3. Specific use/clear purpose
4. Security by design/privacy by design
5. Breach, notice, investigation, reporting
6. Transparency/plain language
7. Right to correct
8. Retention and destruction policies
9. Education/notice/multiple channels to educate (web, app, video)
10. Minimal data – only collect least amount of data needed
11. De-identify/anonymize/aggregate
12. Equity
13. Data integration for shared mobility
14. Contracts/MOUs for data sharing between agencies
15. Data collaborative/trusted brokers



DESTINATIONCAV

DEPARTMENT OF TRANSPORTATION

COMMON THEMES BY REGULATION

	Data Principle	MGDPA	GDPR	CCPA	IMMA	SUMC	Automotive Privacy Principles
1	The right to know about the personal information a business collects about them and how it is used and shared	X	X	X	X		X
2	Businesses are required to give consumers certain notices explaining their privacy practices.	X	X	X	X		X
3	The right to delete personal information collected from them		X	X	X		X
4	The right to consent/opt-out of the sale of their personal information		X	X	X		X
5	The right to non-discrimination for exercising their data rights		X	X		X	X
6	Must notify authorities about a security breach that could result in a serious negative impact on personal data. Must notify data subjects of potential breach.	X			X		
7	Only collect the minimal data needed to achieve intended goals				X		X
8	De-identify, aggregate and secure data						X
9	Invest in security by design infrastructure		X		X		X
10	Educate stakeholders and users					X	X
11	Data must be assigned a retention period. Data is destroyed or made anonymous when no longer needed. Specify retention periods in privacy statements.	X			X		X

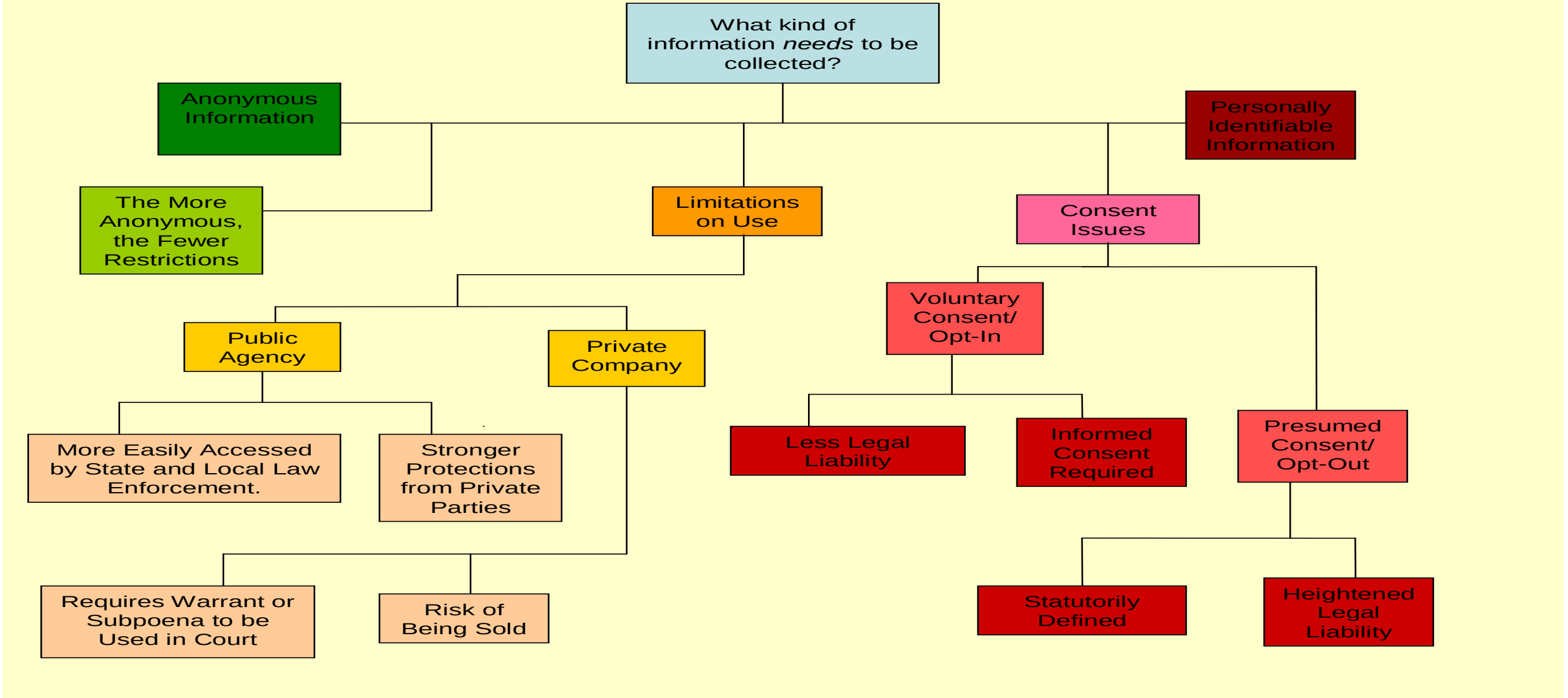
MINNESOTA CAV PRIVACY PRINCIPLES

(1) Equity
(2) Education
(3) Transparency
(4) Consent
(5) Specific use/clear purpose
(6) Minimal data
(7) Opting-out/non-discrimination
(8) Right to correct
(9) De-identify/anonymize/aggregate data
(10) Incorporate security/privacy by design
(11) Collection, retention and destruction
(12) Breach
(13) Data sharing MOUs
(14) Data collaboration/trusted brokers

Items not addressed:

- Private right of action
- Government subscriptions to 3rd party data
- Data monetization and costs of managing big data

ITS PRIVACY LEGAL TOOLBOX



"Intelligent Transportation Systems: Personal Data Needs and Privacy Law" Transportation Law Journal, 39(3) Winter p.97 (2012)

TAXONOMY OF ITS PRIVACY ISSUES

- Type of observation
- Observation purpose
- Vehicle information/ID
- Personal information/ID
- Privacy expectation

SECURITY BY DESIGN FOR CAV

- What is ‘security by design’?

- Core pillars

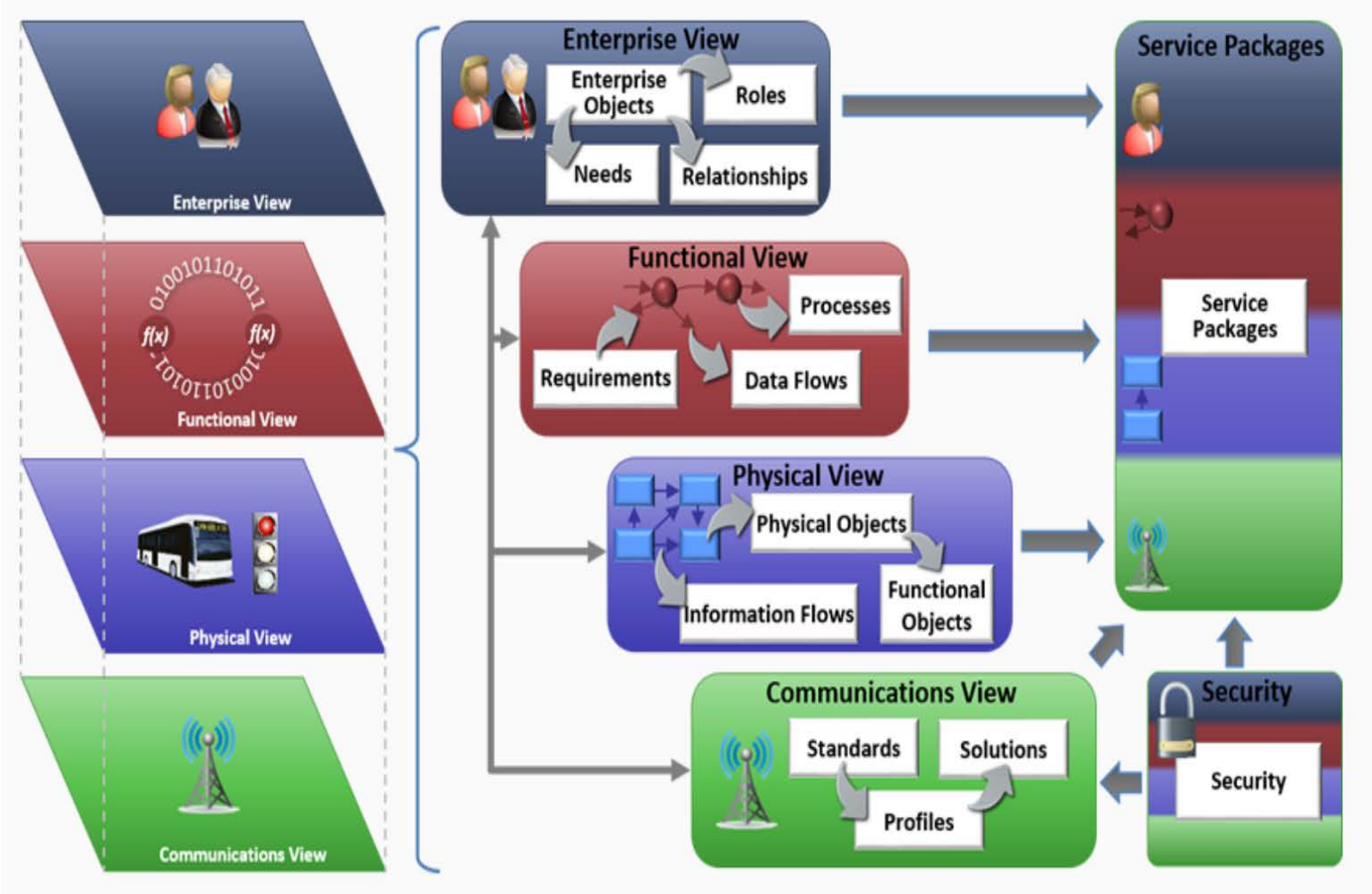
- **Confidentiality** – only allow access to data for which the user is permitted
- **Integrity** – ensure data is not tampered or altered by unauthorized users
- **Availability** – ensure systems and data are available to authorized users when they need it

SECURITY BY DESIGN PRINCIPLES

1. Minimize attack surface area
2. Establish secure defaults
3. The Principle of Least Privilege
4. The Principle of Defense in Depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

SECURITY BY DESIGN PRINCIPLES

- National ITS Reference Architecture (ARC-IT 9.0)



SECURITY BY DESIGN PRINCIPLES

ITS Reference Architecture Layer	Security By Design Principles	CAV Examples

Enterprise	• Minimize attack surface area
	• The Principle of Least Privilege
	• Don't trust services
	• Separation of duties
	• Keep security simple
	• Fix security issues correctly
		• The CAV network needs to be isolated from other networks
		• Don't collect data
		  o without a specific use in mind
		  o from outside the roadway
		• Prevent PII data collection and driver re-identification

Functional	• Establish secure defaults • Fail securely • Don't trust services • Keep security simple	• Secure baseline configurations • Implement systems to patch all equipment on the CAV network • Use the USDOT route anonymizing software to increase the difficulty of re-identification
Physical	• The Principle of Defense in Depth • Keep security simple • Fix security issues correctly	• Need a non-production network/test site that mimics the production environment as close as possible
Communications	• Minimize attack surface area • The Principle of Defense in Depth • Fail securely • Don't trust services • Avoid security by obscurity • Keep security simple	• Use a management network to securely access remote devices • Use firewalls to block non-CAV network traffic

OTHER COMMITTEE PRIORITIES

- Coordination with Blue Ribbon IT Council g
- COVID-19 application best practices
- Coordination with Education & Outreach Committee
- CAV Data Legislation and Policy Subgroup

CONVERSATION WITH COUNCIL

1. *How do these privacy principles reflect the Council's goals?*
2. *How do we integrate an equity lens into this work?*
3. *What voices are missing from this conversation that we need to reach out to?*
4. *What other partners can we work with?*
5. *Recognizing there are few industry standards for CAV data, how do we advance this work to meet Minnesota's needs?*
6. *What other issues does the Committee need to focus on?*

2021 ANNUAL REPORT

6

REPORTING REQUIREMENTS

CAV ADVISORY COUNCIL

- Council must prepare a written annual report to the Governor by February 1st each year.
- Report must include
  - Update on the Council's activities
  - Actions needed to ensure Minnesota is advancing CAV, intelligent transportation, and emerging technologies.

REPORT UPDATES

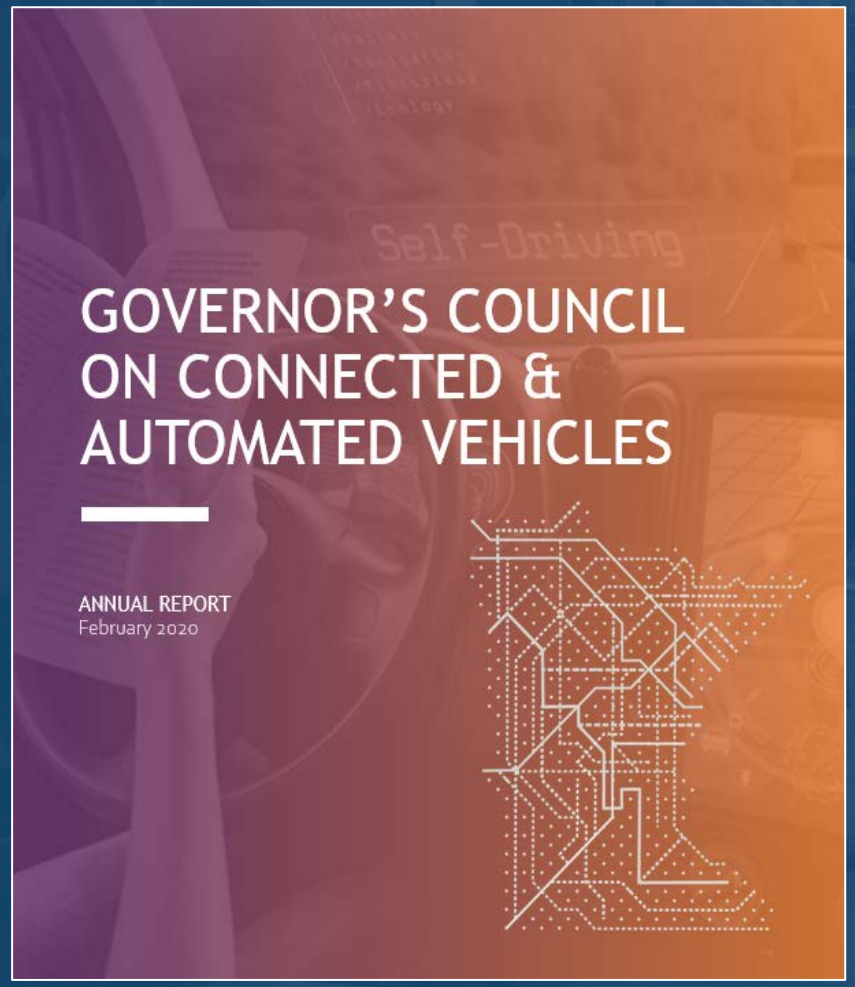
What should we include in the 2021 CAV Annual Report?

Note from chairs

Background on CAV

Council's vision and goals

How we prepare for CAV



2021 Sneak Preview

What are other states doing?

Regional & national update

State and local activities

Launching the new Alliance

OPPORTUNITY FOR PUBLIC COMMENT

Please enter “?” or type your question into the chat box

UPDATES & INFO

Next Meetings:

- April 14, 2020 – Report out from Outreach & Education Committee & Panel on Federal Policy Updates

Upcoming Events:

- Transportation Research Board Annual Meeting - January 21-22, 25-29
- MnDOT Webinar – Drones: A Community Issue – January 212.00-3.30pm
- Minnesota Transportation Conference – March 9-11, 2021
- Fiber Optic Buildout And Partnership Feasibility Study Published – Spring 2021
- MAASTO CAV Summit Report & 10-year Regional Strategy Published – Spring 2021
- Statewide CAV Communications & Engagement Plan Published – Spring 2021

THANK YOU LAURIE!

Thank you, Laurie McGinnis, for all your contributions. We wish you a happy retirement!

CLOSING

Co-chair Margaret Anderson Kelliher, MnDOT Commissioner

Co-chair Phil Magney, VSI Labs

THANK YOU

GOVERNOR'S COUNCIL ON CONNECTED AND AUTOMATED VEHICLES

MARGARET ANDERSON-KELLIHER
Co-Chair

PHIL MAGNEY
Co-Chair

DESTINATIONCAV

DEPARTMENT OF TRANSPORTATION

WHAT DATA ARE WE TALKING ABOUT?

Type of observation	Observation purpose	Vehicle information / ID	Personal information/ ID	Privacy expectation
Anonymous individual vehicle observation Loop detector	Managing system use	None obtained	None obtained	None
Anonymous occupant observation Infra- red lane scanner	Regulation of transportation facilities	Unique vehicle identification obtained	Anonymous information about number of occupants; possibly gender and age.	Low
Individual vehicle observation & data Toll Transponder	Regulation of transportation facilities	Unique vehicle identification obtained	Owner information identified through vehicle registration system	Medium
Individual vehicle observation & data Red light camera	Civil or criminal sanction	Unique vehicle identification obtained	Owner information identified through vehicle registration system	High
Individual driver identification Biometric (voice ID)	Criminal charges	Unique vehicle identification obtained	Driver identified through vehicle registration and licensing system	Highest