AVIN
CONNECTED. AUTONOMOUS.

Ontario

AVIN SPECIALIZED REPORTS

MAY 2019

DATA IN THE CONTEXT OF CAVS

Challenges and Recommendations

Ontario Centres of Excellence

Where Next Happens

TABLE OF CONTENTS

INTRODUCTION

To achieve their targeted operation, connected and autonomous vehicles (CAVs) depend heavily on floods of diversified data. This operational data is either generated by the in-vehicle sensors or received from other data sources through the communication capabilities on board. In the previous AVIN report[1], we started a two-part series of reports specialized in data in the context of CAVs. The first part of this series discussed the various types of CAV data and highlighted examples of their use cases and operational opportunities. This report is the second in this data-focused series.

It targets completing the picture through shedding light on the challenging side of accessing this wealth of data.

Although accessing vehicular data brings a variety of benefits and operational opportunities to the driving experience and information service domain, such data access comes with challenges that need to be critically tackled to have the desired safety and quality of experience levels users expect of CAV technology. For instance, people are concerned about the privacy of their data when it comes to sharing it with other parties for service provisioning or offering remote access to their in-vehicle computing resources for the sake of data collection and/or processing.

01 **Autonomous Vehicle Innovation Network. (2018). Data in the Context of CAVs - Types and Operational Opportunities. Retrieved from** https://tinyurl.com/y9kkwlqy

Cybersecurity is another major challenge impacting the full operation of CAVs. Over the past few years, many hacking incidents of connected vehicles have been reported, resulting in increased public fears of CAVs and economic loss to original equipment manufacturers (OEMs), who have been forced to initiate vehicle safety recalls to handle the corresponding vulnerabilities[2].

There have also been debates regarding the ownership of CAV data, given that there are multiple entities involved in CAV data collection and use processes.

Given the huge volumes and diversified quality of the data collected from CAVs, these two issues have also been drawing the attention of research and development stakeholders in the CAV sector. Fortunately, these two issues can be handled through frameworks and solutions proposed to other data-rich service domains such as the Internet-of-Things (IoT)[3], tweaking them to the specifications and requirements of the CAV applications.

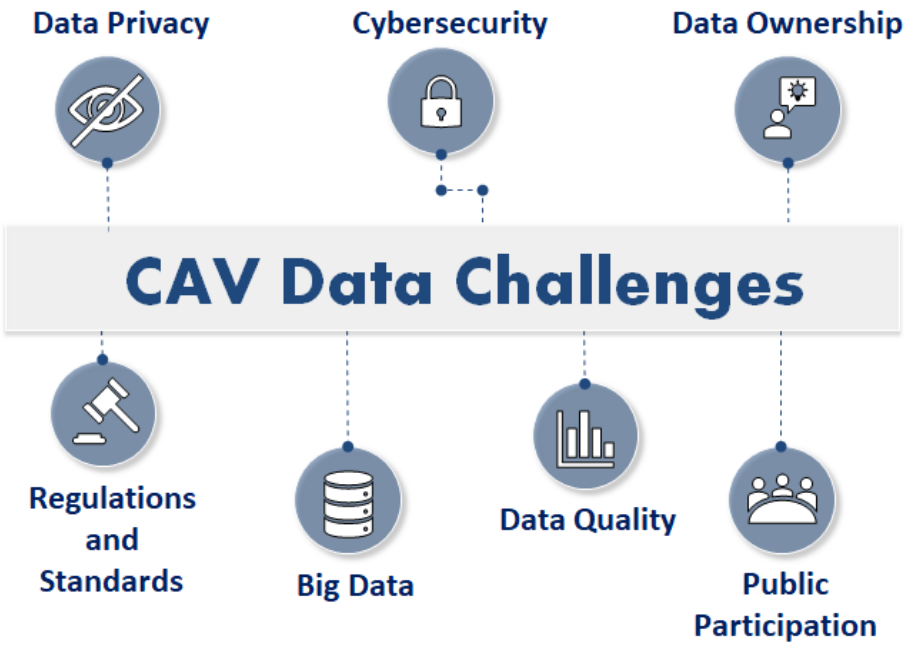
The **Internet of Things (IoT)** is a large-scale networking paradigm connecting smart objects to the Internet with a capability for controlling, identifying, and harvesting data through them remotely.

In our previous AVIN report, we discussed some of the major benefits crowdsensing data by CAVs and using this data for information-based service provisioning. For example, the in-vehicle sensors can be used for detecting traffic and road conditions. The road events detected can then be reported to authorities to take timely actions. To facilitate such a data collection paradigm, CAV owners need to be adequately incentivized using rewards to ensure they remain engaged in the data crowdsensing and collection loop.

Motivated by the pressing and critical needs to investigate and facilitate the data collection and access requirements in CAVs, this report draws attention to the major challenges facing this target.

02 **Osborne, C. (2018). The most interesting Internet-connected vehicle hacks on record. Retrieved from** https://www.zdnet.com/article/these-are-the-most-interesting-ways-to-hack-internet-connected-vehicles/

03 **Morgan, J. (2014). A Simple Explanation of 'The Internet of Things'. Retrieved from** https://bit.ly/2LeBA6K



The report discusses the critical concerns of data privacy, cybersecurity, and data ownership in CAVs highlighting best practices and efforts being made to address these concerns. In addition, the report covers the challenge of having harmonized regulations and standards to govern the use and representation of data in CAVs. The report also sheds light on the challenges related to the volume and quality of CAV data. Finally, the report touches upon the challenge of public participation in CAV data collection and highlights the need for incentives/rewards to urge the public to participate and share CAV data generated by their own vehicles.

For each deliberated challenge, the report highlights some of the recommendations and endeavours being pursued by governments and stakeholders in the CAV sector to solve/overcome this challenge.

DATA PRIVACY

When it comes to data access, privacy is critical. The collected/reported vehicular data may reveal personal traits of the drivers and their driving habits and routes, raising a legitimate public concern regarding sharing CAV data. For example, reporting geotagged environmental data, such as road conditions, would involve precise live locations of the reporting vehicles. Also, collecting driving habits for the sake of fleet management or use-based auto insurance also brings privacy concerns to the corresponding drivers. As the data reveals personal traits, it should be considered private and solutions should be proposed to protect it from privacy breaches.

Due to the vital nature of the matter, privacy solutions are being sought and introduced by data collectors, service providers, and privacy researchers. Some effective solutions target deidentifying the reporting vehicle and driver.

Data **anonymization** and **pseudonymization**[4] are popular solutions for hiding the real identities of data providers and lowering the possibility of linking between the reported data and its providers.

Legal obligations and **agreements** should also govern the privacy terms of the data collection and use processes. When data is to be collected, consent should be obtained beforehand from each data participant for transparency and privacy agreements. The Office of the Privacy Commissioner of Canada, under the Personal Information Protection and Electronic Documents Act (PIPEDA), has defined seven guiding principles to be considered for obtaining meaningful consent[5]. These guidelines ensure that, through consent, data participants

04 **GDPR.Report. (2017). Data masking: anonymization or pseudonymization? Retrieved from** https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/

05 **Office of the Privacy Commissioner of Canada. (2019). Guidelines for obtaining meaningful consent. Retrieved from** https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

are told what personal information is being collected, with which parties that information will be shared, for what purposes, and the consequences and risk of harm. The consent should also ensure providing individuals with clear options to say "yes" or "no" on the type of data to be collected and its use cases.

To ensure that privacy practices are considered starting from the CAV manufacturing process, in 2017, the U.S. House of Representatives passed the H.R.3388 bill; the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act[6]. Through the U.S. Department of Transportation (USDOT), this act necessitates that vehicle manufacturers develop written cybersecurity and privacy plans for such vehicles prior to offering them for sale. The Canadian Senate Standing Committee on Transport and Communications has also recommended the development of a connected car framework with privacy protection as one of its key design considerations. The committee has also emphasized that OEMs need to ensure privacy and cybersecurity best practices are embedded in the overall manufacturing process[7].

As CAV technology continues to evolve, new sources of data privacy breaches may arise. Therefore, stakeholders should always keep data privacy top of mind and make sure that privacy practices evolve with advancements in CAV technology and its implications. They should also ensure that consent documentation is updated and shared with individuals as policies and terms of use are added/updated. OEMs and technology developers must recurrently ensure that data privacy is considered in the foundations and overall design process of CAVs by following rigorous **Privacy by Design** practices[8].

Privacy by Design is a benchmark data privacy framework that, through seven foundational principles, ensures that data privacy is proactively considered in the overall life cycle of a system including the system design, operation, and management.

06 **U.S. House of Representatives. (2017). H.R.3388 - SELF DRIVE Act. Retrieved from** https://www.congress.gov/bill/115th-congress/house-bill/3388

07 **Standing Senate Committee on Transport and Communications. (2018). Driving Change - Technology and the future of the automated vehicle. Retrieved from** https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf

08 **Ryerson University & Deloitte. Privacy by Design - Setting a new standard for privacy certification. Retrieved from** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF

CYBERSECURITY

Due to the critical nature of the CAV operation, cybersecurity has become a major concern in protecting vehicular data and systems from cyberattacks. With the introduction of telematics and communications between vehicles and their surroundings, CAVs have become a major part of a ubiquitously connected world. Although connectivity brings enormous operational opportunities to and from vehicles, it also brings a clear cybersecurity challenge. As vehicles become more connected, they may become more exposed to security vulnerabilities.

As more externally-connected software applications are used in vehicles, they can become a major target for attackers and hackers. Examples of such cyberattacks include data alteration and stealing, service disruption and misdirection, remote hijacking, and vehicle tracking and theft. These threats bring cybersecurity for CAVs to the headlines and impose stringent requirements for secure storage, processing, and transmission of CAV data.

Cybersecurity practices and **standards** are being developed to deal with cyberattacks and address vulnerabilities in CAV hardware and software[9]. Leading practices recommend integrating security into the software

09 **M. H. Eiza and Q. Ni. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. Retrieved from** https://bit.ly/2HtJGF7

development life cycle and following risk-tolerant architectures for CAV data and systems. Global standards are also being developed/enhanced to tackle CAV security threats. For example, IEEE 1609.2 defines standard mechanisms to authenticate and encrypt messages in the Dedicated Short-Range Communication (DSRC) technology[10]. Other cybersecurity practices follow a cloud-based model to provide centralized solutions instead of focusing on protecting each vehicle separately. An example of this approach is followed by Ericsson with its Connected Vehicle Cloud (CVC) system[11].

Blockchain has recently gained momentum as a possible solution to improve CAV cybersecurity. Through its distributed architecture, strong encryption mechanisms, and execution speed, blockchain technology is a promising candidate to solve the CAV cybersecurity challenge[12].

When vulnerabilities are detected, OEMs usually opt for vehicle recalls. Facilitated by connectivity, recommendations are being put forward to OEMs to securely release over-the-air (OTA) firmware updates and/or security patches to vehicles, instead of incurring costly recalls.

The standards association of the Institute of Electrical and Electronics Engineers (IEEE) is an organization within IEEE that develops global standards in a broad range of industries. Their IEEE 1609.x standard suite, along with the IEEE 802.11p standard, handle different functionalities of the DSRC vehicular communication technology.

Due to the critical impacts of cybersecurity, governments have been closely considering it in their CAV workplans and strategies. For example, Transport Canada and the U.S. Department of Transportation (USDOT) have been collaborating on policy and technical requirements to develop a cross-border connected vehicle security certificate management system proof-of-concept (SCMS POC) as part of the Canada-U.S. Regulatory Cooperation Council (RCC) Connected Vehicles Work-Plan[13]. In January 2019, Transport Canada created a safety

10 **IEEE Standards Association. (2016). IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages. Retrieved from** https://standards.ieee.org/standard/1609_2-2016.html

11 **Ericsson Connected Vehicle Cloud. Retrieved from** https://www.ericsson.com/en/internet-of-things/automotive/connected-vehicle-cloud

12 **R. Martin. (2018). 10 Applications for Blockchain in Connected Car Automotive. Retrieved from** https://igniteoutsourcing.com/blockchain/blockchain-automotive-industry/

13 **Government of Canada. (2016-2019). Canada-U.S. Regulatory Cooperation Council (RCC) Connected Vehicles Work-Plan. Retrieved from** http://www.tc.gc.ca/eng/acts-regulations/tc-usdot-871.html

assessment tool[14] to be used by automotive companies to ensure the safety of the highly automated vehicle technologies they develop. The outcomes of this assessment tool are grouped into three categories which include cybersecurity and data management. Also, in March 2019, Transport Canada, as part of the Advance Connectivity and Automation in the Transportation System (ACATS) program, has awarded a contract valued at up to $1.3 million to ESCRYPT to advance the development of a Canadian Security Credential Management System (SCMS) for connected vehicles[15]. The National Cyber Security Strategy announced in Canada's Budget 2018 is another effort towards fostering cybersecurity in Canada's digital world[16].

In the U.S., the National Highway Traffic Safety Administration (NHTSA) of the USDOT has adopted a multi-faceted research approach that leverages the National Institute of Standards and Technology Cybersecurity Framework[17] and pushes industry to adopt practices that boost the cybersecurity profile of their vehicles in the United States[18].

In August 2017, cybersecurity guidance has been published by the UK Department for Transport targeting protecting self-driving cars from being hacked. In 2018, this guidance has been evolved as a cybersecurity standard[19] developed by the British Standards Institute (BSI) in collaboration with public and private sector firms, including Jaguar Land Rover, Ford and Bentley, as well as the National Cyber Security Centre, and funded by the Department for Transport.

As CAV technology develops and adoption accelerates, these governmental and industry initiatives should continue to develop rigorous mechanisms to investigate the potential hardware and software vulnerabilities of the CAV systems and protect CAV data and systems in substantially different ways.

14 **Transport Canada. (2019). Safety Assessment for Automated Driving Systems in Canada. Retrieved from** http://www.tc.gc.ca/en/services/road/documents/tc_safety_assessment_for_ads-s.pdf

15 **Transport Canada. (2019). Transport Canada awards contract to ESCRYPT to enhance the privacy and security of connected vehicles. Retrieved from** https://tinyurl.com/y4ppfzxq

16 **Public Safety Canada. (2018). National Cyber Security Strategy. Retrieved from** https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

17 **National Institute of Standards and Technology. Cybersecurity Framework. Retrieved from** https://www.nist.gov/cyberframework

18 **National Highway Traffic Safety Administration (NHTSA). Vehicle Cybersecurity. Retrieved from** https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

19 **UK Department for Transport. (2018). New cyber security standard for self-driving vehicles. Retrieved from** https://www.gov.uk/government/news/new-cyber-security-standard-for-self-driving-vehicles

DATA OWNERSHIP

Data sharing is a matter of debate among the stakeholders of the CAV ecosystem. Some stakeholders call for having the CAV data openly accessible to support the research and development efforts going on in the sector. Others are against this open access model and are looking for opportunities to turn the CAV data into business opportunities[20]. As a best practice, whether CAV data will be openly or proprietarily accessed, data ownership should be guaranteed for its own provider.

The issue of CAV data ownership is a challenge that needs to be resolved.

The challenging part is that multiple parties are involved in the data generation and collection processes.

For example, service provisioning using crowdsourced data, such as CAV-based traffic monitoring, would involve the participating vehicles and the service provider in the data collection loop. If a participating vehicle happens to work with a ride-hailing company, a third party would come in place. Moreover, if this collected data is transferred over a carrier network and/or stored in a cloud server, more players might disperse the data ownership.

When it comes to personal data, the default practice should be the pledge that this data is owned by the individual it belongs to.

Legal consent should be obtained from that individual if someone wants to access this data.

Ownership of non-personal data is the main challenging side of this CAV data ownership debate given that clearly-defined ownership models have not been devised yet.

20 **Deloitte LLP (2018). Connected and autonomous vehicles in Ontario – Implications for data access, ownership, privacy and security. Retrieved from** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-EN-CVAV-Research-Final-Data-Privacy-Security-Report-20180425-AODA.PDF

In this regard, CAV ecosystem stakeholders have been actively calling for solutions to decide on this controversial matter and help them proceed with their research and development activities on solid legal footing. Specialized work groups are being recommended to study potential data ownership models and devise well-defined ownership frameworks and/or standards, taking into consideration the various types, use cases, and business models of the CAV data. Such modeling efforts will need to be continuously updated to reflect the advances and changes in mobility, including the transitions to shared car ownership and rides. One of the models that is worth investigating is the use of data trusts. A data trust can be a person or agency taking on the trustee role and managing the overall data governance process including data ownership rights. Ongoing efforts that can be considered in this regard is the civic digital trust[21] convened by the MaRS Solutions Lab for the Quayside project of Waterfront Toronto and the Sidewalk Labs in Toronto, Canada.

As an initial effort in this regard, the European FIA Region I has started a campaign named My Car My Data[22]. The main target of this campaign is to support putting vehicle owners in the driver's seat when it comes to their data. The campaign does so through empowering vehicle owners, educating them about connectivity and the operational opportunities of their data, and making sure they are aware of their data ownership rights.

In its report on the future of automated vehicles in Canada, the Canadian Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicles and the Council of Ministers Responsible for Transportation and Highway Safety (COMT) suggested **considering cross-sector and cross-jurisdiction regulatory engagements in devising ownership models for CAV data.** They highlighted that such engagements would facilitate the modeling decisions and implementations through learning from the practices implemented and challenges faced in other data-rich sectors and by regulatory bodies in other jurisdictions[23].

21 **MaRS Solutions Lab. (2018). A Primer on Civic Digital Trusts. Retrieved from** https://marsdd.gitbook.io/datatrust/

22 **FIA Region I. The My Car My Data campaign. Retrieved from** http://www.mycarmydata.eu/

23 **Council of Ministers of Transportation and Highway Safety. (2018). The Future of Automated Vehicles in Canada. Retrieved from** https://comt.ca/reports/autovehicle2018.pdf

REGULATIONS AND STANDARDS

As CAVs start to become ubiquitous, a universal data language will be needed by these vehicles to facilitate seamless, cross-border connectivity and operation and to benefit from a globally-connected Internet of Vehicles (IoV).

Automotive technology researchers and developers have concluded that, without a single regulatory body or governance structure, the worldwide advances in the CAV technology will never converge to a harmonized, seamless, and homogenous automotive environment[24].

By contrast, if the CAV data is used in a uniform format and structure, the benefits of CAVs and their operational opportunities will be massively augmented.

To facilitate having a unified data standard, it is worth noting the efforts being conducted by international standardization bodies such as the Society of Automotive Engineers (SAE) International[25] and the International Organization for Standardization (ISO)[26].

In addition to data formats, standardized cybersecurity practices and harmonized privacy regulations are recommended in order to accelerate and facilitate tackling these two major data challenges. Global recommendations regarding data privacy and cybersecurity often adhere to NHTSA or the European Union (EU).

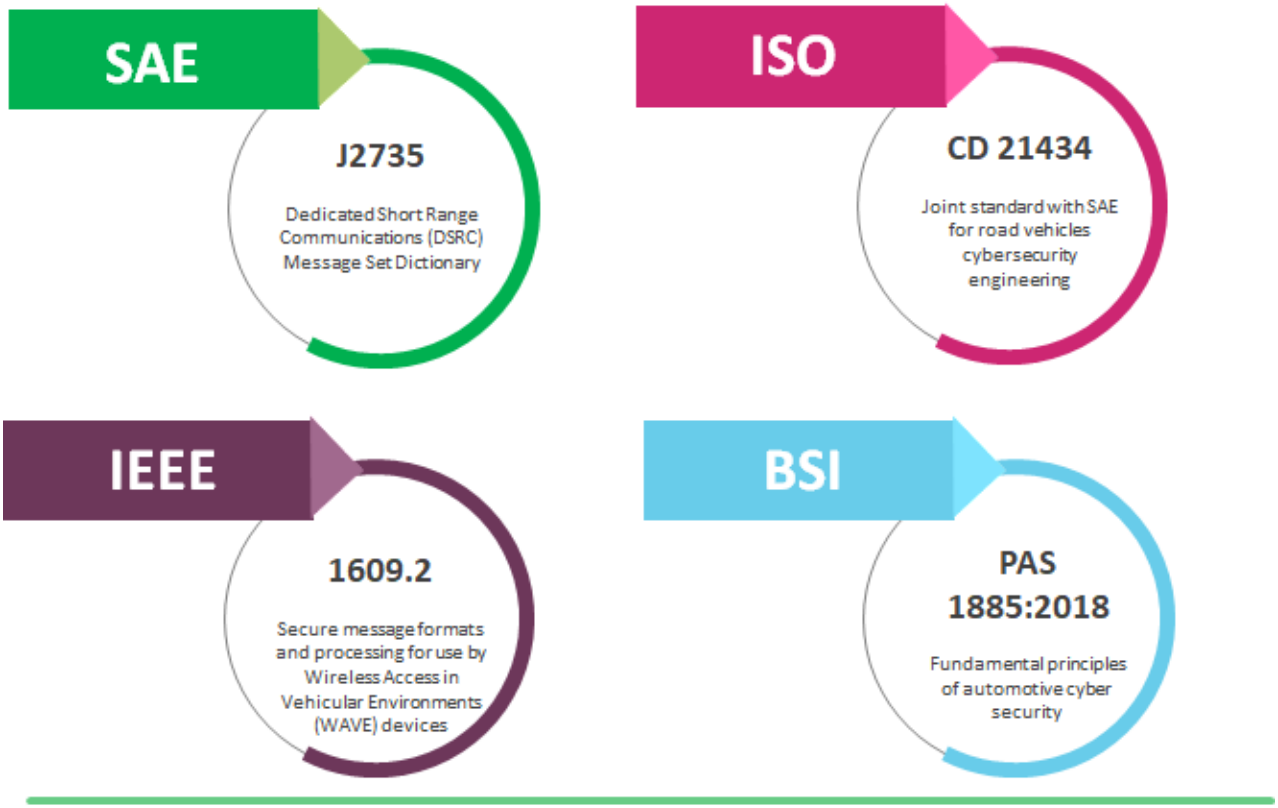
24 **Deloitte LLP (2018). Connected and autonomous vehicles in Ontario – Implications for data access, ownership, privacy and security. Retrieved from** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-EN-CVAV-Research-Final-Data-Privacy-Security-Report-20180425-AODA.PDF

25 **SAE International. (2016). Dedicated Short Range Communications (DSRC) Message Set Dictionary J2735_201603. Retrieved from** https://www.sae.org/standards/content/j2735_201603/

26 **International Organization for Standardization. ISO/TC 204 Intelligent transport systems. Retrieved from** https://www.iso.org/committee/54706/x/catalogue/

The recent General Data Protection Regulation (GDPR) is an example of popular EU data legislation[27] to address data privacy.

For universal standards to be adopted, it is necessary to dedicate work groups to analyze the strengths and weaknesses of existing standards and call for world-wide adoption of those that are globally agreed-upon. To avoid lagging behind the fast pace of the CAV technological advances, initiatives need to be developed to fast-track global standards that balance regulations with innovation.



Exemplary International Standards for CAV Data Formatting and Cybersecurity

27 **EU GDPR - Information Portal. Retrieved from** https://eugdpr.org/

BIG DATA

According to Intel[28], a CAV acquires around 4 terabytes of real-time data a day through its internal sensors, which is equivalent to the data generated daily by almost 3,000 people. This data is fed into in-vehicle artificial intelligence (AI) modules for analysis, decision making, and automation. A big portion of this data also needs to be transferred to a remote computing platform for data analytics, especially in the training phases of CAVs. Given the fact that data is transferred to the remote analytic platform from multiple vehicles, this brings a major big data challenge in **transfer, storage** and **processing.**

For the AI side of the CAV technology, the more data collected for training and validating the autonomous systems, the more accurate and safer the vehicle autonomy will be. Also, such collected data can be utilized for provisioning a wide variety of information-based services.

4 TB

of real-time data acquired a day by a CAV through its internal sensors

28 **Krzanich, B. (2016). Data is the New Oil in the Future of Automated Driving. Retrieved from** https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/

Although these operational opportunities are worth the collection of huge amounts of data, mechanisms should be employed to overcome the corresponding big data challenge.

For example, for the **storage** side of the challenge, data filtering, aggregation, and fusion mechanisms should be applied to the data once it is received at the remote servers. After the filtering and aggregation stage, distributed computing frameworks, such as Apache Hadoop[29], should be used for storing the data files.

Searching such huge amounts of data is another major side of the big data challenge. Fortunately, the computing technologies available for big data analytics[30] have taken this issue into consideration and embedded fast search mechanisms in their solutions. Other data structure techniques can be used to optimize and boost the search capability of big data. The Bloom filter technique[31] is an example of such effective techniques.

Data **transfer** is also a challenging part of this asset, since transferring such huge amounts of data incurs a high cost and consumes a substantial amount of energy and bandwidth. Moving part of the data filtering and aggregation phase to the in-vehicle processing units helps reduce the amount of useless data transferred to the remote repository and mitigate such a resource-consuming challenge. Robustness and protection of the data transfer pipe should be seriously taken into consideration to avoid attacks and interruptions in the transfer of this data that may cause further retransmissions and waste of resources.

29 **Apache Hadoop. Retrieved from** https://hadoop.apache.org/

30 **Vasist, P. (2018). 7 Trending Big Data Tools and Technologies. Retrieved from** https://acadgild.com/blog/7-trending-big-data-tools-technologies

31 **Talbot, J. (2015). What are Bloom filters? Retrieved from** https://blog.medium.com/what-are-bloom-filters-1ec2a50c68ff

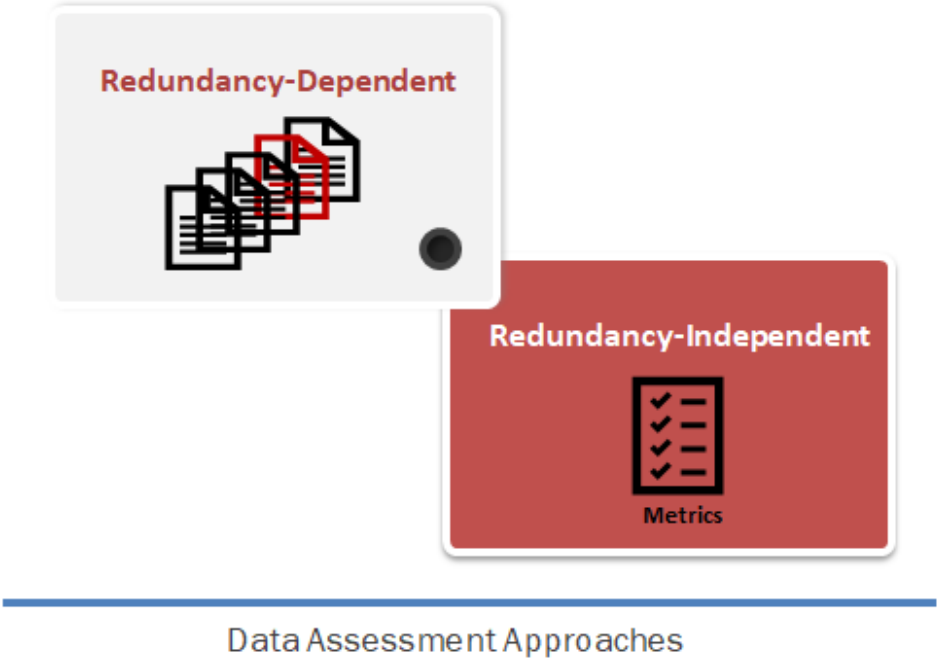
DATA QUALITY

Having diversity in the quality of hardware and software resources of CAVs and the commitment levels of their drivers brings a challenge related to the quality of data collected from CAVs. Not all the CAV data collected would be applicable for use in terms of its accuracy, relevance, and freshness. This concern brings a requirement for having a data assessment framework used by the data host once data is received and before proceeding with storing this data, sharing it with the public, and/or using it for decision making. Through assessing the received data, poor-quality data can be identified and ignored avoiding the implications of affecting/redirecting the data-driven decisions.

In the area of data assessment, two approaches are often used; namely **redundancy-dependent** and **redundancy-independent.** The former approach depends on receiving correlated data from different participants doing the same data collection task. **Outlier detection**[32] is a popular example of this approach. In the redundancy-independent approach, data from other participants is not required. Data assessment is done based on pre-defined **quality metrics** such as data timeliness, spatial relevance, and temporal relevance to the desired data features.

Whether obtained in a redundancy-dependent or independent manner, the final data assessments can be used for computing reputation scores for their participants.

32 **Santoyo S. (2017). A Brief Overview of Outlier Detection Techniques. Retrieved from** https://towardsdatascience.com/a-brief-overview-of-outlier-detection-techniques-1e0b2c19e561



These scores can be recorded and used for evaluating later data from their corresponding participants. This strategy is known as reputation-based data assessment[33]. It has become popular in crowdsensing applications because of its higher assessment fairness and reliability compared to the assessment techniques that do not take the participant history into consideration.

In addition to being used for evaluating data, the reputation scores of participants can also be used for participant recruitment.

After assessing the data, **feedback** can be given to its providers about the quality of their data and their reputation score. This can nudge participants to learn from mistakes and later improve their reputation and data quality.

33 **Abdelhamid, S., Hassanein, H. S., Takahara, G. (2018). Reputation-aware, trajectory-based recruitment of smart vehicles for public sensing.**
Retrieved from
https://ieeexplore.ieee.org/document/8011479

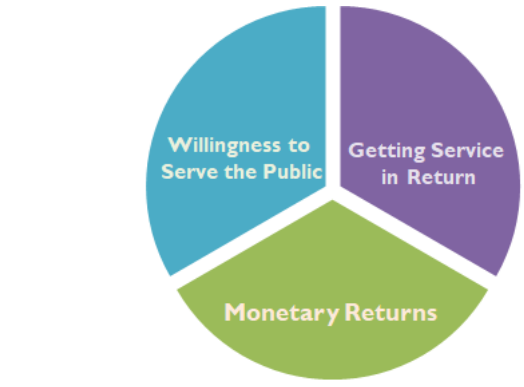
PUBLIC PARTICIPATION

It is not possible for CAV technology to achieve its full potential without active public participation. Data collected through crowdsensing is a major part of the CAV data and a valuable resource for provisioning information-based services. For example, using their in-vehicle sensors and connectivity, CAV owners can help monitor and report road and traffic conditions to authorities and/or service providers.

Such a crowd/public participation needs a form of **incentive** to urge vehicle owners to use their vehicular resources for **crowdsensing** purposes. In other words, these participants would need to be guaranteed rewards in return to stay engaged in the crowdsensing process.

Incentives come in three types: 1) willingness to serve the public, 2) getting service in return, or 3) earning monetary returns[34].

Relying on participants' desire to serve the public cannot guarantee the quality and level of participation required. Therefore, the return-based incentives have been dominating in the crowd participation models with various forms of reward.



Public Incentives

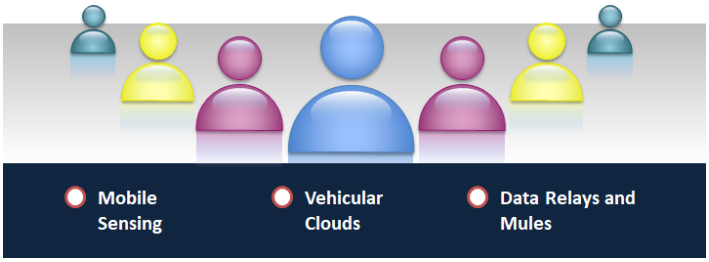
34 **Abdelhamid, S., Hassanein, H. S., Takahara, G. (2015). Vehicle as a Resource (VaaR). Retrieved from** http://www.queenstrl.ca/uploads/4/6/3/1/4631596/2015_vehicle_as_a_resource_(vaar).pdf

A popular incentive model for crowdsensing using connected vehicles is to give returns in a form of driving/parking vouchers that can be used, for example, for free parking and/or accessing toll roads.

When it comes to determining the value of monetary incentives, two general categories of **pricing models** can be considered. The first category is collector-based, where the recruiting data collector takes care of determining the reward value for each participant based on the level of participation and the quality of the collected data. The second pricing category is participant-based, waiving the task of determining the monetary reward to the participants themselves as an asked-for price for their reported data. The data collector has the right to accept, negotiate, or decline the requested price before getting access to the data.

Public participation is not only considered for the sake of CAV data collection.

Crowdsourcing can also be utilized for accessing and sharing the overall resources of CAVs including their on-board computing resources as a vehicular cloud and their communication capabilities as data relays and mules. In order to use their resources for these purposes, vehicle owners need to be sufficiently incentivized and rewarded while being reassured that the privacy and cybersecurity issues highlighted throughout this report are no longer concerns.



CONCLUSIONS

In this report, we have discussed the major challenges of data access and collection in CAVs with the aim of establishing awareness of key areas open for research, development, standardization, and policy management in the CAV sector. We have also highlighted some of the emerging best practices and recommendations to address these challenges in order to have a smooth, trusted, and rewarding user experience reporting and collecting CAV data.

First, the importance of data privacy and cybersecurity to the overall operation of CAVs has been discussed. Data ownership has also been highlighted as a major topic of debate when it comes to using CAV data. The advantages and difficulties of having harmonized regulations and standards across different jurisdictions for defining and representing CAV data have been also delineated. The challenges of storing, processing, and transferring huge amounts of CAV data and assessing the quality of this data have been discussed as points of interest that can make benefit of earlier solutions devised for other data-rich service domains. Finally, the challenge of engaging the public in CAV data collection has been discussed highlighting the need for incentives to get and keep the public in the crowdsourcing loop.

In tackling and trying to solve the existing challenges, priority should be given to the data privacy and cybersecurity challenges because of their critical nature and serious impact on the overall operation of CAVs.

Stringent privacy frameworks must be considered in the design and full data cycle of CAVs to make sure the identity and other private traits of the data providers cannot be identified or predicted.

Rigorous cybersecurity practices should be developed and deployed at all levels of CAV technology, including vehicles, their enabling infrastructure, and the different tiers and equipment of their supply chain.

While Canada and Ontario have data privacy and cybersecurity frameworks in place, neither has been fully tailored to the context and use cases of CAVs.

As the Canadian leader in the CAV sector, Ontario is well-suited to lead on national and cross-border harmonized regulations and policies to govern the collection, access, and use of CAV data with a focus on resolving the corresponding challenges highlighted in this report.

Cross-disciplinary and cross-jurisdiction work groups can be formed to collaborate in achieving this mission. These work groups should be maintained as the technology evolves to ensure the regulations and solutions are adapting to the advances and changes brought by and in the technology.

MEET THE AVIN TEAM

Raed Kadri
Director, Automotive Technology and Mobility Innovation
(416) 861 1092 x9-7400
raed.kadri@oce-ontario.org

Sherin Abdelhamid
Technical Data and Global Trends Analyst
(416) 861 1092 x 9-1097
sherin.abdelhamid@oce-ontario.org

Mona Eghanian
Senior Manager, Automotive and Mobility
(416) 861 1092 x 9-1076
mona.eghanian@oce-ontario.org

Daniel Graham
Manager, Automotive and Mobility Portfolio
(416) 861 1092 x1107
daniel.graham@oce-ontario.org

Martin Lord
Senior Sector Manager, Automotive and Mobility Portfolio
(905) 823 2020 x9-3236
martin.lord@oce-ontario.org

Viraj Mane
Sector Manager - Automotive and Mobility
(416) 861 1092 x 9-1073
viraj.mane@oce-ontario.org

Shane Daly
Automotive and Mobility Team Coordinator
(416) 861 1092 x9-5017
shane.daly@oce-ontario.org

ABOUT AVIN

The **Autonomous Vehicle Innovation Network (AVIN)** initiative is funded by the Government of Ontario to support Ontario's competitive advantage in the automotive sector and to reinforce its position as a North American leader in advanced automotive and mobility technologies, including transportation and infrastructure systems.

This initiative capitalizes on the economic potential of connected and autonomous vehicle (CAV) technologies by supporting the commercialization of best-in-class, made-in-Ontario solutions that create jobs, drive economic growth and enhance global competitiveness. AVIN also helps Ontario's transportation systems and infrastructure adapt to these emerging technologies.

AREAS OF FOCUS

AVIN programs focus on supporting the development and demonstration of CAV technologies in light vehicles (e.g., cars, trucks and vans), heavy-duty vehicles (commercial vehicles, trucks, buses and RVs), transportation infrastructure, intelligent transportation systems (ITS) and transit-supportive systems.

AVIN is administered on behalf of the Government of Ontario by Ontario Centres of Excellence (OCE). The initiative comprises four distinct programs and a central hub. The AVIN programs are:

- AV Research and Development Partnership Fund
- Talent Development
- Demonstration Zone
- Regional Technology Development Sites

The AVIN Central Hub is a dedicated team that supports delivery and administration of AVIN programming, and provides the following key functions:

- Connect & Coordinate - a focal point to help coordinate activities among industry, academia, research organizations and governments, and connect interested stakeholders and members of the public;
- Opportunity Identification - knowledge translation, research, data/information, trend analysis, and acting as a bridge between technology and policy; and
- Awareness & Education - promote AVIN programs and Ontario's AV testing pilot and build awareness of Ontario's growing CAV community.

AVIN has five Objectives:

We would like to thank the Government of Ontario for supporting AVIN programs and activities.

We would also like to thank the partner organizations that work with OCE to deliver AVIN programs, including the Regional Technology Development Sites and the Demonstration Zone.