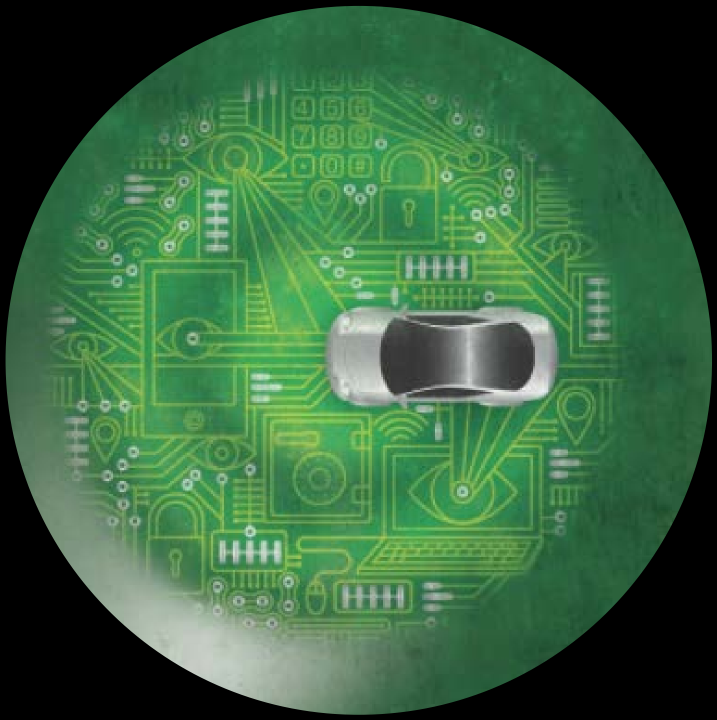
Deloitte.

With thanks to our funding partner

Ontario



Connected and autonomous vehicles in Ontario

Implications for data access, ownership, privacy and security

Table of contents

Executive summary

The transition to widespread adoption of connected and autonomous vehicles is underway in Ontario. Researchers estimate that about two-thirds of vehicles in Canada currently have some connectivity (i.e., embedded telematics); by 2022, approximately 70% – 95% of new cars in Canada will have vehicle to infrastructure (V2I), vehicle to vehicle (V2V), and other telecommunications capabilities (e.g., vehicle to smartphone).[1] Currently, vehicles available to consumers are primarily Level 1 or 2 automation (see Figure 1).[2] While a number of major manufacturers plan to launch autonomous passenger cars in the next year, consensus in the literature is that deployment of Level 4 or 5 vehicles on public roads will not be commonplace until the 2030s or 2040s.[3] In fact, major auto manufacturers including Ford and GM have indicated their first autonomous fleets will be dedicated to commercial operations.[4]

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
Human driver **monitors the driving environment**						
0	no Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
Automated driving system **("system") monitors the driving environment**						
3	conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	high Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Figure 1 - SAE Automation Levels for Connected and Autonomous Vehicles[5]

The Ontario government, working across a number of ministries, commissioned this report in order to gather more evidence on the implications of CV/AVs for data access, ownership, privacy, and security in Ontario, including key themes,

[1] Nowak, P. (Apr. 2017). In-car connectivity in Canada lags far behind US. https://www.theglobeandmail.com/globe-drive/news/industry-news/in-car-connectivity-in-canada-lags-far-behind-us/article34695060/.
[2] Ontario Centres of Excellence. "How It Works". Connected Vehicle/Automated Vehicle (CVAV) Program. http://www.oce-ontario.org/programs/industry-academic-collaboration/cvav-research-program/how-it-works.
[3] Ticoll, D. (2015). Driving Changes: Automated Vehicles in Toronto, Discussion Paper. Munk School of Global Affairs, University of Toronto.
[4] Gilboy, J. (2018). General Motors: Autonomous Vehicle Production Begins Next Year. The Drive; Edelstein, S. (2017). Ford's Upcoming Self-Driving Car Will be 'Commercial Grade'. The Drive.
[5] United States House of Representatives Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection. (2017). Self-Driving Cars: Levels of Automation Hearing, Statement of SAE International S. William Gouse, Director, Federal Program Development.

gaps in knowledge, and areas requiring further investigation. This research reinforces Ontario's position as a North American leader in transformative automotive technologies, as well as transportation and infrastructure systems. Filling these important research gaps and making the research public will support Ontario's innovation ecosystem and enable it to capitalize on the opportunities presented by the projected mass adoption of CV/AVs in the decades to come.

Context, key themes and implications for Ontario

Connected and autonomous vehicles generate or transfer data through two primary channels: telematics and "infotainment systems".[6] Telematics systems employ sensors to detect vehicle operations and condition, driver behaviour, driver location, and related data and can connect with other systems (e.g., emergency or roadside assistance) to transmit this information.[7] Infotainment systems transfer information back to the driver, including navigation, traffic, weather, or entertainment (e.g., audio streaming). This can be done by connecting the vehicle directly to the internet or by pairing with the driver's mobile device.[8]

Uncertainty around the pace and scope of transition to fully autonomous vehicles means that a number of "future states of mobility" might co-exist over time, evolving and depending on two major forces: the extent to which autonomous vehicle technologies become widely adopted and the extent to which vehicles are personally owned or shared. During the transition (over the next ten to twenty years), personally owned and shared, partially automated and fully automated, and somewhat connected to fully connected vehicles will co-exist. Twenty-five or more years in the future, Level 4 and 5 autonomous vehicles will be common, one mode of a personalized and integrated set of mobility options (including trains, bicycles, etc.) available to passengers and connected to each other and the ecosystem.

These transition and potential end states frame a number of key findings related to the emerging state of connected and autonomous vehicles in Ontario and the implications for data access, ownership, privacy, and security:

The purported benefits of connected and autonomous vehicle data for government, private sector companies, and the public at large are promising, but remain uncertain in practice during the short-term transition phase. Unprecedented volumes and new types of data generated by connected and autonomous vehicles and related connected technologies stand to improve safety, environmental outcomes, and accessibility, streamline movement

---

[6] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[7] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.
[8] Ibid.

of goods and people, and bring direct commercial benefit based on improved consumer experience. Realizing these benefits, however, is contingent on establishing standards around safe and sustainable use of vehicles, protocols for secure transmission, storage, and use of data, supporting, interoperable infrastructure to enable data flows, and compliance with privacy laws and best practices related to efficient and secure sharing of data across partners.

Implications for Ontario: CV/AV data will only improve conditions for Ontario citizens, businesses, organizations, and governments if the vehicles are deployed safely, sustainably, and accessibly and if the ownership and use of that data is clearly defined, whether in accordance with voluntary standards or regulatory guidelines.

Stakeholders across sectors and industries will have different needs from the same vehicle-generated or related data, resulting in a greater need for increasingly customized data sharing models. Two broad models exist for data sharing: voluntary (ad hoc or based on a memorandum of understanding or official partnership) or mandated (by legislation or regulation). While some stakeholders call for open data in the interest of research and development across industries or public acceptance of connected and autonomous technologies, others are pursuing strategic partnerships or turning proprietary data into a business opportunity. The availability and flow of data becomes particularly important where that flow might enhance public safety or other interests.

Implications for Ontario: Consortia of industry, academic, and public sector actors are already forming with the purpose of sharing information on research and testing results, information related to traffic, infrastructure, and the surrounding environment, and emerging technologies. Technical standards might improve the consistency and applicability of the data shared in these partnerships, while CV/AV-specific guidelines around what can and should be shared in the public interest would enhance predictability.

While Canada and Ontario have privacy frameworks in place, there is no specific legislation or regulations that speak to the ownership and security of personal information generated or transferred by connected and autonomous vehicles. The way in which Canada and Ontario's privacy frameworks apply to new technologies, including connected and autonomous vehicles, has been the focus of legislative debate as Big Data analytic techniques increase the ability to use data that was previously deemed anonymized to identify individuals through a combination of personal, vehicle, and location data. Similarly, the range of use cases for data ownership and access are under-explored, creating the need for clarity related to ownership, consent, and Privacy by Default design throughout the data lifecycle.

Implications for Ontario: The issue of data ownership and consent still needs to be resolved, with the risk that the technological capabilities to aggregate, analyze, and use personal and other sensitive information will outpace attempts to develop policy guidance, standards or regulation in this space.

Connected and autonomous vehicles have a number of vulnerabilities to cyberattacks; a combination of best practices and innovative advanced technologies are being explored to mitigate the risk.

Five key threats are associated with connected and autonomous vehicles: theft of property, theft of data, physical destruction and sabotage, invasion of privacy, and fraud.[9] A number of key leading practices for industries at varying levels of cyber security maturity include: following international best practice and ensuring defensive depth, building security into the Software Development Life Cycle, operating by "Privacy by Default" and "Privacy by Design" principles as the basis for products and services, and committing to risk-focused controls, vigilance, and resilience throughout the data lifecycle. Advanced technologies such as blockchain have the potential to help accelerate cyber security capabilities.[10]

Implications for Ontario: Cyber security should be an increasingly central part of private and public sector organizational strategies in Ontario, following international standards to harmonize with other jurisdictions and set up security infrastructure from the start, before threats become realities.

Digital, physical and regulatory interoperability or harmonization will be required to fully optimize the operations and benefits of connected and autonomous vehicles. The World Economic Forum (WEF) writes: "The full realization of the SIMSystem vision includes all modes of transport and the functionality to use and deploy those modes as well as the infrastructure on which they operate, across geographies, for the movement of people and goods, globally." The extent to which harmonization is feasible and desirable across these three layers may shift depending on the scale of mobility systems (i.e., cross-provincial, national, international) and the pace of transition to greater levels of autonomy and connectedness. That said, connectivity becomes more seamless with greater standardization and harmonization of data, physical infrastructure, and regulations and standards across industries and jurisdictions.

Implications for Ontario: As a Canadian leader in this space, the Ontario government is well-situated to create a space and convene different sectors to collaborate on a rules-based framework or similar protocol for regulatory and physical infrastructure interoperability within provincial borders and with

[9] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html.
[10] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html.

neighbouring jurisdictions (e.g., Michigan, Quebec), potentially shaping a nationally harmonized approach.

Governments at all levels have various roles to play in providing, generating, or managing data from connected and autonomous vehicles, from setting cross-jurisdictional frameworks for harmonized understanding, supporting innovation while ensuring public safety, and improving quality of life for citizens. The Federal Government currently focuses on vehicle safety, though has become increasingly involved in developing national regulations and frameworks, policy research and development, and funding for connected and autonomous related initiatives. Provincial governments are responsible for creating the legislative framework within their own jurisdictions related to safety, testing, and data ownership and management, as well as licensing, registration, insurance, and road rules. The province also operates highway and transit infrastructure corridors across the province and any related intelligent transportation systems planning. Finally, municipalities are the primary owners of intelligent infrastructure and connected transit systems within their region and make key urban planning and land use decisions, increasingly using a "Smart Cities" lens to do so.

Implications for Ontario: The provincial government will at once be working with federal counterparts to shape national CV/AV frameworks for data management, data ownership, cyber security, and others, while also creating the conditions for innovation within provincial borders. Other levels of government might learn from municipalities and their experiences becoming Smart Cities, including establishing partnerships, planning for data storage, transmission, and related security, and deploying technology using citizen-centred techniques to accelerate success.

The skills required to effectively develop, adopt and maintain connected and autonomous vehicles and related technologies has not been a core focus in many impacted industries to date. The collection, storage, management, use, disposition, and regulation of connected and autonomous vehicle data will require specific skillsets across industries. Automotive-related occupations and some auxiliary occupations such as emergency services, public/city planners, transit operators, and other public sector agencies will likely require upskilling and/or retraining while ICT jobs will be in greatest demand. Despite investments from the federal government and key industry players, automotive innovation and research experts suggested that some industries (e.g., technology providers, financial services firms) may be more prepared from a skills capacity perspective than others (e.g., public sector entities, auto parts suppliers).

Implications for Ontario: A comprehensive skills inventory, business requirements assessment, and gap analysis across industries (potentially led by an academic institution, the provincial government, or a neutral third party), with a focus on connected and autonomous vehicle development and deployment, could help inform the province's approach to skills training.

Gaps in the research and recommended areas for further analysis

While this report offers a summary look at what is known about the implications of connected and autonomous vehicles on data access, ownership, privacy, and security, the report outlines a number of key areas where further research might clarify this topic in the Ontario context. Opportunities are classified, depending on whether organizations should prioritize laying the groundwork in the given area now, monitoring the evolution of the topic before acting, or investing in understanding the gap and its implications over the long-term.

Areas to address now to enable future success

Safety incentives during the transition (Recommendation 1): Provincial and municipal governments could work with industry, public safety organizations, and community organizations to develop policy tools specific to incentivizing safe passenger behaviour and driver responsibility as vehicles transition to Level 3 automation and above.

Opportunities to enhance accessibility and inclusion (Recommendation 5): All mobility ecosystem actors could further study the implications of connected and autonomous vehicles on accessibility and inclusion, with a focus on how data might be used to help maximize these benefits.

Establishing data needs for public interest (Recommendation 7): The provincial government could further consider the need for standards or regulation with respect to data access for specific data types that might contribute to public interest or materially help research and business development across the ecosystem and might be shared for mutual benefit.

Models for connected and autonomous vehicle data ownership (Recommendation 9): Ownership of personal and non-personal information specifically generated or transferred by connected and autonomous vehicle data has not been clearly defined. The provincial government or other body (e.g., a standards-setting organization) might convene stakeholders from other levels of government, academia, and industry to study potential models, including a rules-based framework (focused on outcomes) or definitive standards by data type.

Data ownership and residency capacity needs (Recommendation 13): Regulators and industry might conduct further study to identify capacity needs, current state gaps, and potential models to fill gaps in parallel with discussion on data ownership and broader data residency frameworks.

Requirements for interoperability (Recommendation 16): The provincial government might develop a deeper understanding of the current state of interoperability between data structures and platforms across the ecosystem in order to determine requirements for establishing interoperability and the feasibility of such an endeavour.

Mapping the Ontario ecosystem (Recommendation 17): Research and development hubs made up of consortia of academic institutions, non-profits, research organizations, community groups and industry associations are emerging as catalysts for technological advancement and cross-sector collaboration. Mapping of these organizations, led by the provincial government or another province-wide body or association would allow a deeper understanding of the current Ontario ecosystem, including an assessment of gaps and needs to compete and lead the future of mobility.

Areas to monitor over the near-term as the industry evolves

The need for data ownership regulation (Recommendation 2): The provincial government might monitor decisions made by industry players and partnerships on data ownership and access to determine whether policy or regulatory intervention is needed as use cases for data sharing and monetization become more complex and operate cross-sector. Multiple levels of government will have a significant role in decisions related to data ownership.

Mapping of data needs and use cases (Recommendation 3): Academic, industry, and government actors could collaborate to develop a comprehensive taxonomy of datasets and types likely to be generated by connected and autonomous vehicles in order to identify particular data needs and determine best use for each type.

Determination of specific stakeholder data needs (Recommendation 6): As above, academic, industry, and government actors could deepen understanding of the particular data needs of each player and determine which group or partnership is best to collect, store and use different data types.

Data-sharing model pilots (Recommendation 8): Researchers, government actors, and representatives across industries could work together to pilot different data sharing models, developing a deeper knowledge of the benefits of each model for different contexts and use cases.

Exploration of anonymization and pseudonymization standards (Recommendation 10): As part of the study of ownership issues, regulators and provincial/federal governments might assess standards for anonymization and pseudonymization, use cases on risks to de-identification, and the appropriate timing and level of individual consent specific to connected and autonomous vehicles.

Cross-industry information sharing on cyber security (Recommendation 12): The provincial government might create a space for traditional and non-traditional automotive ecosystem players to convene and engage with leading practice industries (e.g., financial services) on cyber security, with the objective of identifying lessons learned that might apply in Ontario.

Balancing of voluntary and regulatory approaches (Recommendation 15): The balance between voluntary standards and regulation in any eventual Connected and Autonomous Vehicle Framework should be carefully considered.

Mobility ecosystem skills gap analysis (Recommendation 18): CV/AV industry representatives, led by either an academic institution, R&D hub or by the provincial government, might create a common set of capabilities for workers in CV/AV industries in order to inform strategies from the provincial government, industry associations, and academic institutions for cross-training and skills development.

Areas for long-term investment

Coordination between parallel innovations (Recommendation 4): Relevant provincial ministries could continue to coordinate on parallel innovations in electric, autonomous, and connected vehicles to identify areas for mutual benefit or complementary research and development.

Future state modelling (Recommendation 11): Academic and research institutions might conduct further modelling of future scenarios for ownership and consent depending on the pace and scale of transition to shared ownership or mobility subscription models.

Convergence of connected and autonomous vehicles and advanced technologies (Recommendation 14): Further study should be conducted on how blockchain and of other advanced technologies might converge to create opportunities for connected and autonomous vehicles. Recent public sector use cases in British Columbia and Ontario demonstrate an emerging role for government in this space.

Critically, all ecosystem players, including all levels of government, a range of traditional and non-traditional automotive industries, and academic and research hubs have a role to play in successfully transitioning towards the future state(s) of mobility.

1.0 Introduction and context

Background on connected and autonomous vehicles

Connected vehicles "use wireless technology to connect with other vehicles (V2V), transportation infrastructure (V2I), other connected technology (V2X) and mobile devices to provide information to drivers. There are two broad types of connected technologies: consumer conveniences and infotainment from vehicles connected to the internet and V2V, V2I communications over dedicated short-range communications systems.[11] Automated, or autonomous or self-driving vehicles (AVs), "rely on sensors and computer analytics to sense their environments and perform varying degrees of the driving task".[12] The Society of Automotive Engineers (SAE) International's J3016 Standard defines six levels of driving automation, a technical standard that reflects the transitional shift underway towards greater levels of automation (see Figure 2).[13]

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
Human driver **monitors the driving environment**						
0	no Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	System	Human driver	Human driver	Some driving modes
Automated driving system **("system") monitors the driving environment**						
3	conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	System	Human driver	Some driving modes
4	high Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	System	Some driving modes
5	full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	All driving modes

Figure 2 - SAE Automation Levels for Connected and Autonomous Vehicles[14]

Currently, AVs available to consumers are primarily Level 1 or 2 automation. A number of major manufacturers plan to launch autonomous passengers cars in the next year, with acceleration to occur after 2020 (see Figure 3).

[11] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communications.
[12] Ibid.
[13] Ontario Centres of Excellence. "How It Works". Connected Vehicle/Automated Vehicle (CVAV) Program. http://www.oce-ontario.org/programs/industry-academic-collaboration/cvav-research-program/how-it-works.
[14] United States House of Representatives Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection. (2017). Self-Driving Cars: Levels of Automation Hearing, Statement of SAE International S. William Gouse, Director, Federal Program Development.

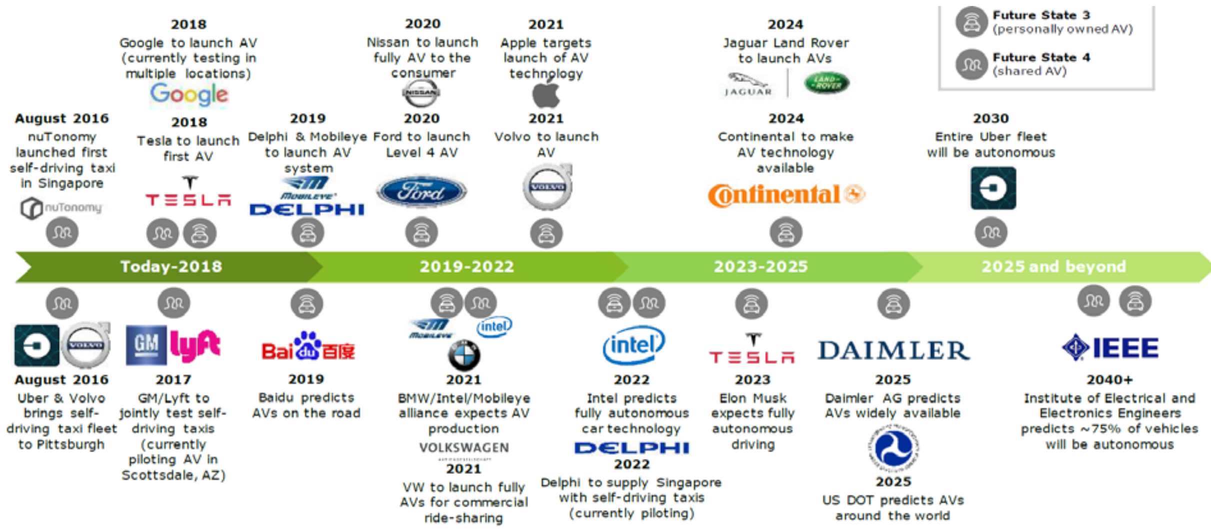


Figure 3 – Autonomous vehicles: Adoption and application[15]

That said, major auto manufacturers including Ford and GM have indicated their first autonomous fleets will be dedicated to commercial operations.[16] General consensus in the literature is that deployment of Level 3, 4 or 5 passenger and commercial vehicles on public roads will not be commonplace until the 2030s or 2040s (depending on the estimate). Based on experience with previous vehicle technology deployment and considering industry efficiencies and consumer adoption of AVs, the Victoria Transport Policy Institute estimates that AVs may be available "with minimum price premium" by the 2040s, representing 40-60% of new vehicle sales and 20-40% of the total vehicle fleet in Canada.[17] Similarly, a study by David Ticoll at the Munk School of Global Affairs suggests that the rate of deployment could more closely follow adoption rates in consumer technology markets, citing various consultant estimates that predict between 15%-25% of vehicles in use globally will have Level 3 to 5 automation by 2030.[18]

Connected and autonomous vehicles generate or transfer data through two primary channels: telematics and "infotainment systems."[19] Telematics systems employ sensors to detect vehicle operations and condition, driver behaviour, driver location, and related data and can connect with other systems (e.g., emergency or roadside assistance) to transmit this information.[20] Infotainment systems transfer information back to the driver, including navigation, traffic, weather, or entertainment (e.g., audio streaming). This can be done by

---

[15] CB Insights, TechCrunch, InformationWeek, Driverless Future, Xconomy, WSJ, Government Tech, Bloomberg.
[16] Gilboy, J. (2018). General Motors: Autonomous Vehicle Production Begins Next Year. The Drive; Edelstein, S. (2017). Ford's Upcoming Self-Driving Car Will be 'Commercial Grade'. The Drive.
[17] Litman, T. (2018). Autonomous Vehicle Implementation Predictions: Implications for Transport Planning. Victoria Transport Policy Institute.
[18] Ticoll, D. (2015). Driving Changes: Automated Vehicles in Toronto, Discussion Paper. Munk School of Global Affairs, University of Toronto.
[19] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[20] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.

connecting the vehicle directly to the internet or by pairing with the driver's mobile device.[21] These two systems can also be integrated to provide services to the driver (e.g., estimating arrival time, automated adjustments to sound based on engine noise).

Report purpose and structure

Purpose

The Ontario government, working across a number of ministries, commissioned this piece of research in order to gather more evidence on the implications of CV/AVs for data access, ownership, privacy, and security in the Ontario context. This research reinforces Ontario's position as a North American leader in transformative automotive technologies, as well as transportation and infrastructure systems. Filling these important research gaps and making the research public will support Ontario's innovation ecosystem and enable it to capitalize on the opportunities presented by the projected mass adoption of CV/AVs in the decades to come.

The purpose of this report is to:

- Identify existing research, key themes and trends on connected vehicles and autonomous vehicles (CV/AVs)
- Comment on the potential implications of findings for Ontario
- Identify gaps in research and/or collected data
- Recommend areas for further research and analysis

Research process

Findings were assembled through a combination of qualitative and quantitative research and consultations with a broad range of stakeholder experts (referred to throughout as "experts"), including auto manufacturers, software providers, insurers, innovation hub partners, community leaders, industry associations and academics. Sources include academic articles, reports from government, industry, and professional services/analysis firms, and news reports.

Research and consultations were structured around five key themes, with associated questions used to structure discussion with experts and review of the literature:

1. Opportunities and risks
2. Use of data (including monetization, public interest, ownership and access, and ethical considerations)
3. Use of data for the public good
4. Roles and responsibilities (including the three levels of government, private sector organizations, community or industry associations, etc.)

[21] Ibid.

5. Privacy and security frameworks and regulation

Report structure

This report first summarizes the Ontario landscape and mobility stakeholder ecosystem and establishes an understanding of the timelines and characteristics for the transition to connected and autonomous vehicles.

Key findings from the research are then organized according to a number of key topics:

- Changes in type, use and volume of data
- Data sharing
- Privacy and protection of personal information
- Cyber security risks
- Harmonization and interoperability
- Role of regulation
- Role of governments
- Capacity-building

Each theme contains commentary on transition state and end state implications, with description of how particular future states (e.g., mix of automation for vehicles on the road, mix of vehicle ownership models) might impact findings and key stakeholders. Direction on next steps for research and analysis on the given topic is included.

The Ontario landscape

Ontario is one of the leading Canadian jurisdictions with respect to the development, testing, and eventual deployment of connected and autonomous vehicles.

Government regulation and initiatives

- Beginning January 1, 2016, Ontario launched a 10-year pilot to allow for the testing of automated vehicles on Ontario's roads. Ontario is the first Canadian jurisdiction to permit AV testing on public roads.
- In December 2017, the provincial government commenced stakeholder consultations on enhancements to its AV testing regime. These proposed amendments would:
    1) Exclude from the pilot automated vehicles with Society of Automotive Engineers (SAE) Level 3 technology if they are originally manufactured with a driving automation system, and eligible and commercially available for sale in Canada;
    2) Allow the testing of driverless AVs as part of the pilot under stringent conditions;

3) Allow the testing of cooperative truck platoons on Ontario's roads under strict conditions as part of the pilot;
4) Increase the scope and robustness of data reporting required under the AV pilot.[22]

Research & development

- Ontario is investing $80 million over five years to create the Autonomous Vehicle Innovation Network (AVIN) project, in partnership with the Ontario Centres of Excellence. The main components of the network are as follows:

— The Demonstration Zone, enabling small- and medium-sized companies to validate and test technologies in live scenarios and weather conditions
— Up to six Regional Technology Development Sites across Ontario. Each site will have a unique focus to enable small-and-medium sized enterprises (SMEs) to validate new CV/AV technologies, access specialized equipment and obtain business advisory services
— A Research and Development (R&D) Partnership Fund to foster collaborations between automakers, technology leaders and Ontario-based small- and medium-sized enterprises (SMEs), post-secondary institutions and municipalities in the development and commercialization of CV/AV technologies
— The Talent Development Program to support student and recent graduate internships and fellowships with Ontario companies in areas strategic to advancing CV/AV technologies
— A Central Hub that will act as a resource and focal point to conduct research, share information, build connections and raise awareness.

- Ontario has permitted a number of organizations to test automated vehicles, including Blackberry QNX, The University of Waterloo, The Erwin Hymer Group, Continental Corporation, X-Matik, Magna, and Uber

Industry

- The province hosts five top OEMs (FCA, Ford, GM, Honda, Toyota), over 700 automotive parts manufacturers (e.g., Magna, Linamar, Martinrea, Multimatic), and over 500 tool, die and mould makers[23]
- Ontario has over 20,000 IT companies, 44 colleges and universities, and 40,000 yearly graduates in fields of science, technology, engineering and mathematics (STEM)[24]
- Ontario has 24 auto-focused public research facilities[25]

[22] Jones, A. (2018). Look both ways: Ontario seeks to allow testing of driverless cars. Globe and Mail.
[23] Automotive. (2018). InvestinOntario. https://www.investinontario.com/automotive#auto-intro
[24] Ibid.
[25] Ibid.

Mobility stakeholder ecosystem

A number of sectors, industries, organizations, and individuals will be impacted by the shift to connected and autonomous vehicles and will in turn shape the future mobility ecosystem. Figure 4 illustrates the mobility ecosystem in which connected and autonomous vehicles will function and the key players shaping the landscape.[26]

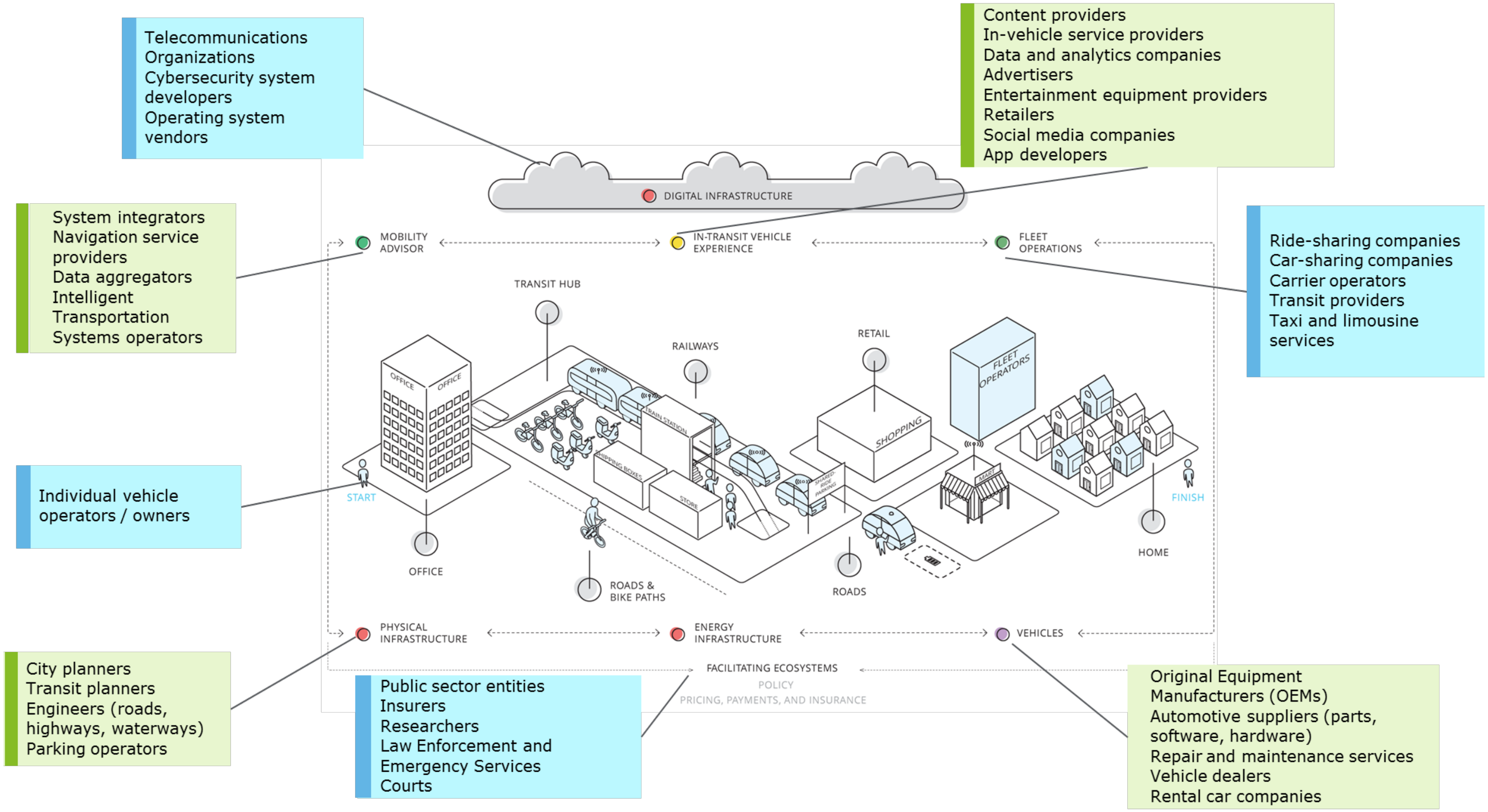


Figure 4 – Core groups active in the mobility ecosystem

[26] For more information on each segment, please see *Force of Change: The Future of Mobility*, *Navigating a Shifting Landscape: Capturing value in the evolving mobility ecosystem*, and *The Future of Mobility: What's Next?*

Understanding of transition and end states

There is uncertainty around the pace and scope of transition to full vehicle connectedness and autonomy, meaning that a number of "future states of mobility" might co-exist over time (see Figure 5):[27]

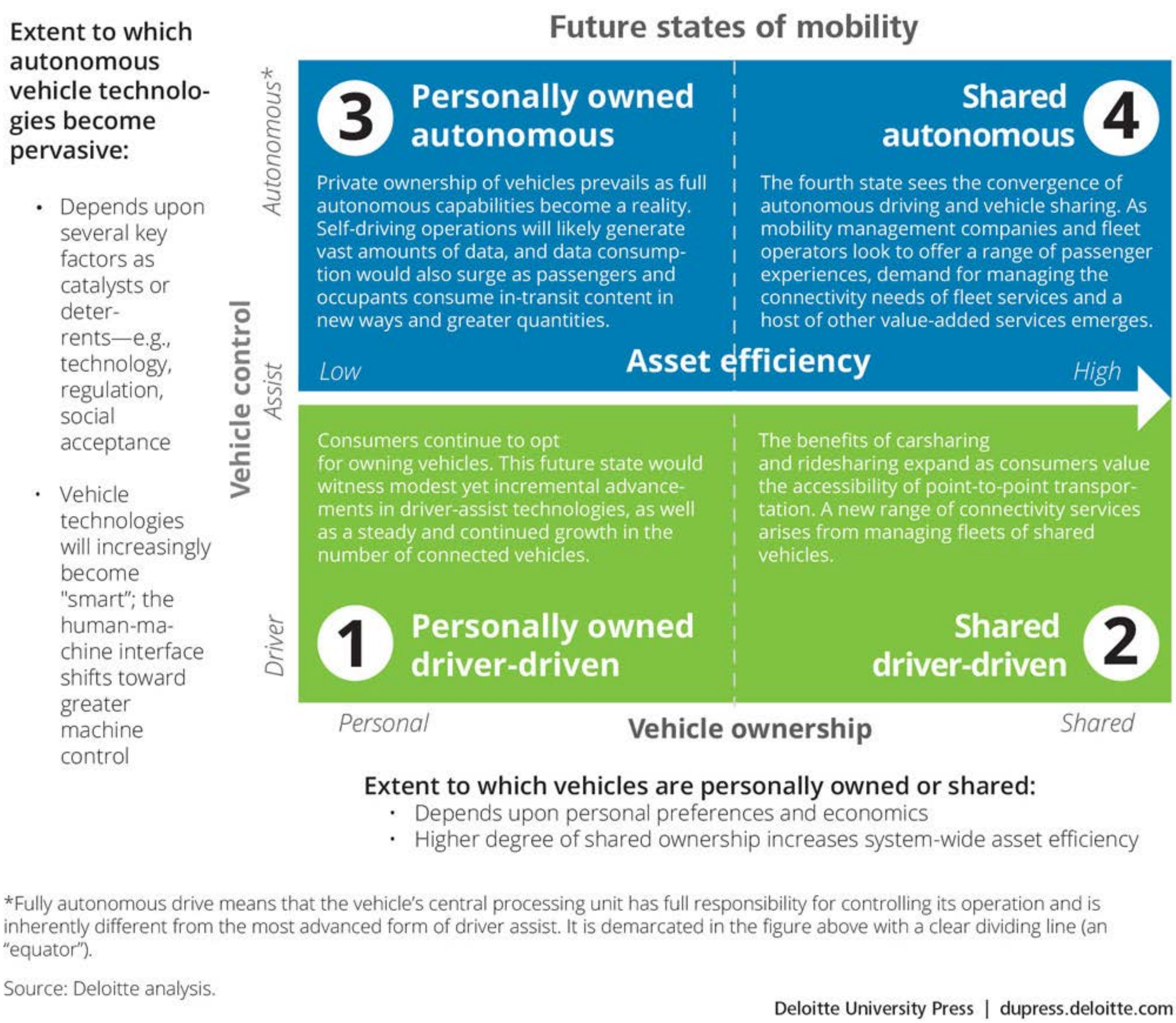


Figure 5 – Future states of mobility (Deloitte University Press)

1. **Personally owned driver-driven:** Private ownership remains the norm. Driver-assist technologies (SAE Level 2) are incorporated incrementally. The number of connected vehicles increases steadily

---

[27] Smud, D., Wigginton, C., Ninan, S., Ramachandran, K., & Moceri, P. (2017). Connecting the future of mobility: Reimagining the role of telecommunications in the new transportation ecosystem. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/role-of-telecommunications-in-new-mobility-ecosystem.html#endnote-sup-21

2. **Shared driver-driven:** Shared mobility serves a great and growing portion of transportation needs. New connectivity services are introduced to accommodate fleet management
3. **Personally owned autonomous:** Private ownership continues to dominate. Autonomous drive technology (SAE Level 4) is viable, safe, convenient, and economical. V2X connections are ubiquitous and data generation and consumption dramatically increases
4. **Shared autonomous:** Autonomous and vehicle sharing trends converge, where mobility management companies and fleet operators offer seamless mobility, enabled by advanced connectivity, to meet a variety of consumer needs and preferences

The balance between these future states depends on two major forces: the extent to which autonomous vehicle technologies become widely adopted and the extent to which vehicles are personally owned or shared. In the period over the next ten to twenty years, Future States 1, 2, and potentially 3 and 4 will co-exist to some degree. Experts expect to see full automation for some vehicles (e.g., agricultural or mining equipment, cargo trucks on the highway, platoons of automated vehicles in particular zones) in risk-controlled environments well within that time. The end state is understood as the period 25 or more years in the future when Ontario has transitioned to a mix of Future States 3 and 4.

Each of the four future states of mobility brings a unique set of data-related opportunities and risks. The following key findings further explore the implications during transition phases, developing an understanding that will be critical to defining a clear and balanced governance framework with respect to connected and autonomous innovations.

2.0 Key findings

Changes in type, use, and volume of data

Unprecedented volumes and new types of data generated by connected and autonomous vehicles and related connected technologies stand to improve safety and accessibility, streamline movement of goods and people, and spur economic development and direct commercial benefit if security, privacy and other supporting infrastructure can be established.

A 2015 report by the BC Freedom of Information and Privacy Association cites:

> A combination of increased connected car sales and a growing scale of information coming from connected cars will result in the collection of some 11.1 petabytes of connected car data by 2020. The rate at which the data are flowing from the connected car landscape is also growing dramatically…about 350 megabytes [of data will be collected] per second [in 2020], compared to about 15 megabytes per second in 2013.[28]

Types of data include owner and traveller information (e.g., driver behaviour, travel direction, time, conditions, mobility patterns, biometrics and health data, infotainment, communications), vehicle information (e.g., types of vehicles, vehicle health, speed, location, history of accidents), and information about the surrounding environment (e.g., weather conditions, road conditions, traffic).[29] Depending on the type of data, a number of entities may have access, including automakers, insurers, government agencies, mobile network and mobile device providers, emergency or other call centres, rental agencies, and aftermarket service providers.[30] Table 1 summarizes broad use cases for data that may be generated, relevant datasets, and the parties that may be interested in their use.

[28] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.
[29] Ibid; Autonomous Cars, Big Data, and the Post-Privacy World. (Oct. 2017). DMV.org. https://www.dmv.org/articles/self-driving-vehicles-privacy-concerns.
[30] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada; Securing the networked vehicle: Threat study. (June 2016). Deloitte.

Table 1 – Categories of data and use cases[31]

Data use Case	Public interest	Vehicle manufacturer/third-party commercial services	Vehicle operations	Product analysis and improvement	User or vehicle identification
Sample data	Local hazard warning light, accident location, position of emergency vehicles, roadblocks, potholes, traffic flow, etc.	Average speed, road sign recognition, parking locations, popular routes, ambient temperature	Engine operating map, lane perception, proprietary algorithms, etc.	Engine behaviour, fuel pump performance, automatic transmission shifting behaviour, fault data, battery status, break pad wear, tire pressure	Vehicle location, average speed, acceleration, fuel and consumption levels, common destinations, mobility patterns, address book, app accounts, infotainment settings, personalized in-car settings, etc.
Interested parties	Public sector authorities, delivery partner providers	Aftermarket commercial service providers, vehicle manufacturers	Vehicle manufacturers, service providers (e.g., dealers, repair facilities)	Vehicle manufacturers, suppliers, service providers	Legislated authorities (e.g., manufacturers, insurers, aftermarket providers granted consent

[31] Adapted from Connected and Autonomous Vehicles: SMMT Position Paper.

There are a number of opportunities and risks associated with the new volumes and types of data generated and the broad ecosystem of players in possession or interested in leveraging the information. As one autotech industry member said, "Roads will be more efficient and safer the more data we share, if consumers and automakers and other data owners can agree to the terms. Part of [success] will be making sure the security, integrity, and privacy of the data is not compromised."

Safety benefits

A connected vehicle can improve safety by using embedded sensors to respond to its environment, adjusting vehicle speed or direction based on the location of other vehicles, weather conditions, or driver behaviour. Data on vehicle performance under certain conditions could also be used to prompt timely software fixes.[32] In case of emergency, vehicles may also transmit information to emergency medical responders, including the location and cause of an accident, whether seat belts were used, and biometric information on the passenger and driver, so that they can respond in a prepared and timely manner.[33] Similarly, connected vehicles might detect safety hazards on the road and notify authorities to perform preventative maintenance.[34] Level 1 and Level 2 automated features, including forward collision and lane departure warning, blind spot assist, adaptive headlights, dynamic brake support, and combined function automation (for example, automated driving direction and speed), can already result in significant improvements.[35]

"Safety is the number one use case."

- Automotive supplier

Combining connectivity with automation in vehicles could improve safety even further by all but eliminating the human factor. Approximately 94% of traffic collisions worldwide are caused by human error.[36] Figure 6 below, using the Victoria Transport Policy Institute's estimates of autonomous vehicle deployment rates, shows how gradual uptake of autonomous vehicles might influence safety in Canada.[37]

---

[32] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication; Krawiec, RJ & White, V. (Aug. 2017). Governing the future of mobility. Deloitte; Mathieson, SA (Feb. 14, 2018). We already give up our privacy to use phones, why not with cars too? https://www.theregister.co.uk/2018/02/14/connected_vehicles_data_and_privacy/.
[33] Ibid.
[34] Anderson, J.M., Kalra, N., Stanley, K.D., Sorensen, P., Samaras, C., Oluwatola, O.A. The Promise and Perils of Autonomous Vehicle Technology. (2016). RAND Corporation.
[35] Ibid. The Insurance Institute for Highway Safety reported that property damage liability claims for cars with automatic braking had declined 7 – 15% by 2015. (Ticoll, D. (2015). Driving Changes: Automated Vehicles in Toronto, Discussion Paper. Munk School of Global Affairs, University of Toronto)
[36] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[37] Estimates are aggregated from a number of academic, policy, and independent consultant reports.

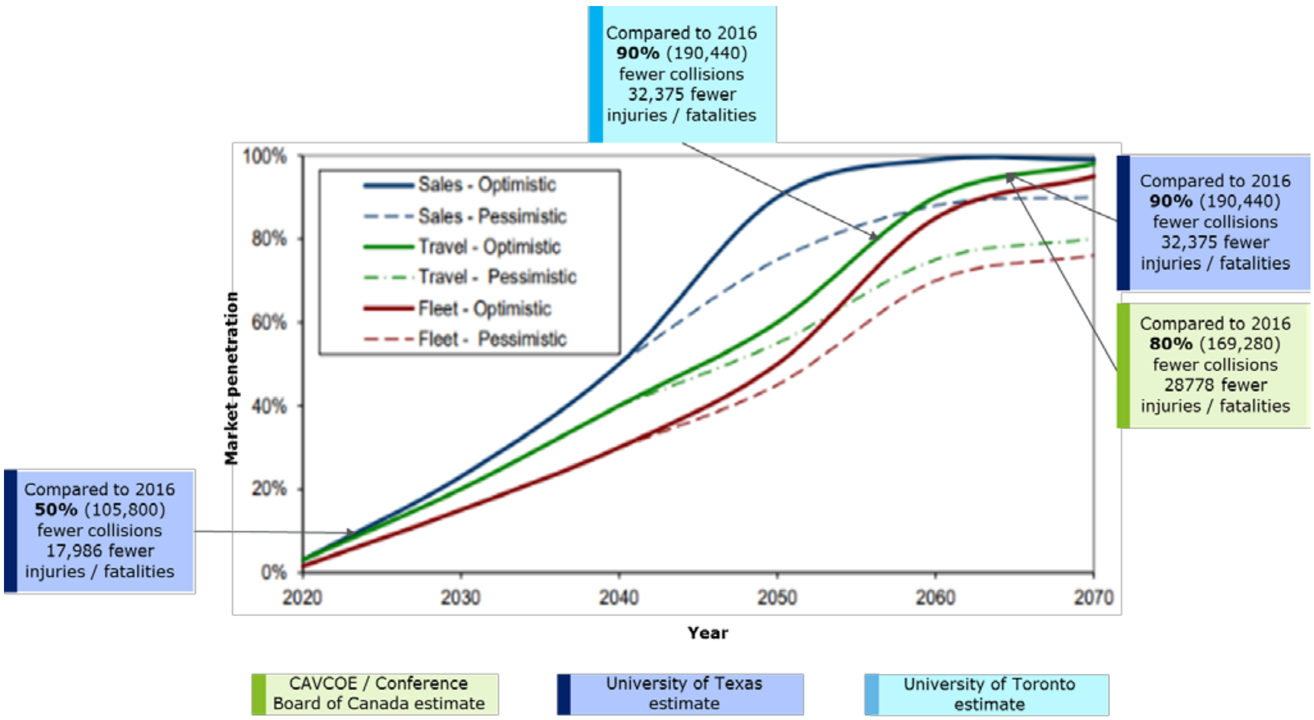


Figure 6 – Projected autonomous vehicle deployment, 2020 – 2070[38, 39]

Safety improvements are likely to become more significant as uptake of Level 4 or 5 AV technologies increases and the mix of driver-operated and automated vehicles on the road trends towards automation and connectivity. Around the 2030s, as Level 3 and 4 vehicles become more ubiquitous, Ontarians may start to see a reduction in collisions, injuries, and fatalities from road accidents. This is likely to accelerate in the 2040s as Level 3, 4, and even 5 autonomous vehicles make up a significant share of total new vehicle sales and an increasingly significant share of the total vehicle fleet.

In the near to medium-term, while the majority of automated vehicles are at Level 2 or Level 3 and still require human attention and intervention for specific tasks, safety benefits will remain contingent on responsible human drivers, supported by effective policy and vehicle design. Distracted vehicle operators may

---

[38] Image and analysis of projections from Litman, T. (2018). Autonomous Vehicle Implementation Predictions: Implications for Transport Planning. Victoria Transport Policy Institute (VTPI). VTPI projections assume autonomous vehicles at Levels 3 or higher become available starting in the 2020s. Estimates from An Interim Report: Infrastructure and Smart Communities. (Dec. 2017). Report of the Standing Committee on Transport, Infrastructure, and Communities; Ticoll, D. (2015). Driving Changes: Automated Vehicles in Toronto, Discussion Paper. Munk School of Global Affairs, University of Toronto; Gill, V., Kirk, B., Godsmark, P., and Flemming, B. (2015). Automated Vehicles: The Coming of the Next Disruptive Technology. The Conference Board of Canada.

[39] Note that safety improvement estimates from the Conference Board of Canada apply to Canada, University of Texas estimates apply to a mid-size American city, and University of Toronto estimates apply to the Canadian context with a focus on Toronto. Calculations assume that fatal and personal injury collisions account for approximately 18% of total reported collisions in Ontario, in line with the latest available statistics on total collisions. Using 2016 personal injury and fatality numbers, this assumes approximately 211,600 total collisions in 2016. Estimated reductions are based on 2016 collision rates and do not account for potentially significant changes in vehicle ownership or number of vehicles in use over time. (Preliminary 2016 Ontario Road Safety Annual Report Selected Statistics. Ministry of Transportation. http://www.mto.gov.on.ca/english/publications/pdfs/preliminary-2016-orsar-selected-statistics.pdf; Ontario Road Safety Annual Report 2014. Ministry of Transportation. http://www.mto.gov.on.ca/english/publications/pdfs/ontario-road-safety-annual-report-2014.pdf)

be unable to respond or take control of the vehicle when required, either causing or failing to prevent accidents. The vehicle itself might contribute to this distraction: "the entire connected vehicle system may become little more than a source of driver distraction."[40]

Ensuring operators maintain focus on the driving task will be particularly important as human and autonomous drive co-exist on public roads: "the driver may overestimate the amount of the driving task being controlled autonomously, leading to…distraction…At level 3, if a driver is able to safely engage in other activities, their ability to react to an emergency may be impaired".[41] Brandon Schoettle, from the Transportation Research Institute University of Michigan writes that the rate of fatalities as a result of distracted driving could even increase if the hand-off between vehicle and driver (when necessary) is not done properly and safely, negating safety benefits in the transition time.[42]

Economic benefits

Competitive advantage and monetization

A range of stakeholders have the opportunity to create value from telematics and infotainment data, either by identifying areas for cost savings or by opening new revenue streams.

Vehicle manufacturers, suppliers, and operators

- Over-the-air software updates to reduce recall and warranty costs[43]
- Remote diagnostics to lower roadside assistance and repair costs
- Greater knowledge of vehicle performance to benchmark against competitors, improve products, improve manufacturing efficiency, and reduce research and development lead time and costs
- In-vehicle add-on features (e.g., in-car apps)
- Data access for individual vehicle operators to benchmark driving and vehicle performance

Insurers

- Improved accuracy of pricing to improve loss ratio and maintain claims competitiveness

"This is a massive commercial opportunity. [Data] creates a window into parts of our lives that have been relatively opaque. We cannot emphasize enough the primacy of data. This is where competitive advantage lies."

- Consumer experience expert

[40] Report on Driver Distraction. http://www.transport.govt.nz/assets/Uploads/Our-Work/Documents/Report-on-Driver-Distraction.pdf.
[41] Ibid.
[42] Condliffe, J. (2016). Semi-autonomous cars could increase distracted driver death. MIT Technology Review.
[43] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.

- Usage-based policies for specific journeys, controlling risk of loss event
- Discounts on insurance for individual or fleet operators based on vehicles' level of connectivity or automation
- Real-time mapping and suggestions for alternative routing for trucks, delivery vehicles, or other fleets based on routes with a greater probability of accidents or a real-time blockage, incentivizing safety and minimizing claims (leveraging telematics, social feeds/news feeds, infrastructure sensors, etc.)
- Data sharing on claims and other driver or vehicle behaviour data with OEMs or automotive suppliers to encourage safety and other product improvements
- Data sharing with researchers, public sector entities, or OEMs/automotive suppliers to incentivize better driver behaviour
- Real-time evaluation of collision cause and impact to avoid potential fraud[44]
- Improved accuracy of algorithms to proactively initiate investigations

Physical infrastructure providers

- Streamlining movement of goods, planning public transit or fleet deployment to under-served or high demand areas, optimizing available parking space, and targeting preventative infrastructure maintenance to deliver cost savings[45]
- Improved traffic flow management and traffic enforcement deployment based on real-time congestion, weather, accident, and infrastructure data
- Dynamic usage pricing or smart tolling based on vehicle behaviour and traffic flow information

Mobility advisors

- Development of proprietary, real-time navigation maps based on non-connected sources of data (e.g., real time traffic data)
- Personalized, optimized routing for premium customers

In-transit vehicle experience: A number of opportunities related to consumer experience are explored in the following section.

Fleet operators

- Streamlined movement of vehicles, goods, or people based on real-time traffic, congestion, weather, and infrastructure data
- Efficient and effective use of assets, cutting down on "empty miles" through visibility into utilization

---

[44] A recent report from Aviva found that auto repair fraud across Ontario costs consumers approximately $547 million annually; Aviva fraud investigation reveals urgent need to reform auto insurance. (2018). Aviva. https://www.insurancebusinessmag.com/ca/industry-news/aviva/aviva-fraud-investigation-reveals-urgent-need-to-reform-auto-insurance-94671.aspx

[45] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem); The future of mobility: What's next? Deloitte University Press.

- Over-the-air software updates to reduce recall and warranty costs[46]
- Remote diagnostics to lower roadside assistance and repair costs
- Automatic routing for repair based on vehicle condition
- In-vehicle add-on features (e.g., in-car apps)

Generally, revenue opportunities fall into four categories: add-on in-vehicle features, in-vehicle customized advertising, secondary marketing, or selling data (to drivers or third party buyers).[47,48] A recent report estimated that the average connected car today has up to 200 data points with more than 140 market opportunity use cases. In 2017, the market opportunity from data including location, driver behaviour, vehicle use, high-definition mapping, and environmental information is estimated at $2 billion globally, growing to ~$33 billion by 2025 if all opportunities for monetization were leveraged.[49] Auto executives have started to take notice, citing connected car data as a key innovation enabler and source of new revenue.[50] In all instances, the monetary and non-monetary value of this data is exponential when considering the power of analytics to draw on data and system metadata for more complex insights.

Besides private commercial gain, savings from traffic accidents, congestion avoidance, fuel cost savings, and drivers' time in Canada could be up to $65 billion per year, or $20-$30 billion in Ontario.[51] Changes will be particularly notable if shared ownership becomes the dominant model. That said, if connected and autonomous vehicles reduce the cost of driving, congestion might increase rather than decrease over the short-term.[52]

Three models are starting to crystallize on a global level, and have begun to penetrate the Ontario and Canadian marketplace as new industries emerge around data monetization: data bartering, or information-based data exchanges; data brokering, or the sale of data on a marketplace; and business intelligence, or the analysis of data for business purposes (see Figure 7).[53]

The Ontario ecosystem may have particular opportunities to capitalize due to the saturation of automotive production and information technology industries, with

---

[46] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.
[47] Ibid.
[48] Connected and Autonomous Vehicles: Position Paper. (2017). Society of Motor Manufacturers and Traders Ltd.
[49] Singh, S. (2017). Are Car Companies Going to Profit from your Driving Data? Forbes. https://www.forbes.com/sites/sarwantsingh/2017/11/06/are-car-companies-going-to-profit-from-your-driving-data/#a44f7f0143c8
[50] Ibid. Buckland, K. & Alpeyev, P. (2018). Israeli start-up Otonomo takes on Google in rush to process car data. Bloomberg. http://canada.autonews.com/article/20180220/COPY01/302209956/israeli-startup-otonomo-takes-on-google-in-rush-to-process-car-data
[51] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[52] Anderson, J.M., Kalra, N., Stanley, K.D., Sorensen, P., Samaras, C., Oluwatola, O.A. The Promise and Perils of Autonomous Vehicle Technology. (2016). RAND Corporation.
[53] Singh, S. (2017). Are Car Companies Going to Profit from your Driving Data? Forbes. https://www.forbes.com/sites/sarwantsingh/2017/11/06/are-car-companies-going-to-profit-from-your-driving-data/#a44f7f0143c8

nearly 100 companies involved in connected-car technologies.[54] Government investments in connected and autonomous vehicle pilot projects, research and development, and related initiatives including Smart Cities and Superclusters may help propel Ontario in a key emerging industry.

[54] Better data fuels better driving. (2017). InvestinOntario Spotlights. https://www.investinontario.com/spotlights/better-data-fuels-better-driving.

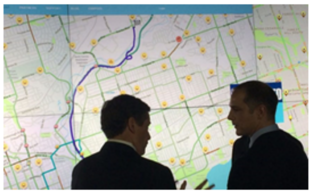
Data Bartering	Data Brokering	Business Intelligence
		mojio
Waze, the Google-owned navigation app, has made an agreement with the City of Toronto to trade data for mutual benefit. Waze will have access to city data such as road and lane closures, areas of heavy and light traffic, traffic-inducing special events, accident locations and construction sites. The City will get anonymized data from more than 560,000 local Waze users, which will help transportation staff ease congestion by steering people away from traffic, improve planning based on a new source of traffic-flow information, and warn vehicles about closures, road construction and major traffic-inducing events.	Otonomo, an Israeli start-up, collects data from automakers and operators, secures, anonymizes, standardizes, and aggregates the data (in compliance with local regulations) to sell back to automakers, insurance companies, city planners, retailers, financial institutions, and so on. Over the long-term, customer data might be used for in-vehicle customized advertising or to target advertising based on a driver's preferred routes, common destinations, and so on. Otonomo is currently conducting pilot projects with a number of automakers, suppliers, and ride-hailing companies. While not explicitly active in Canada, Otonomo is working with nine global automakers and expanding.	Mojio is a Canadian start-up providing an open, hardware-agnostic cloud-based connected car platform. Mojio offers a small plug-in dongle that contains a wireless modem (carried by Canada's three largest telecommunications companies), a GPS tracker, an accelerometer, and the ability to read diagnostic assessments of component trouble or failure. Data is uploaded to Mojio's cloud platform and can then be made available to vehicle operators, auto makers, carriers, insurers – whichever organization is implementing the connected car service.
Source: Rider, D. (2017). Waze and Toronto Agree to Trade Traffic Data. Toronto Star.	*Source: Otonomo website.*	*Source: Mojio website. https://www.moj.io/connected-car-platform/*

Figure 7 – Business models for data monetization

Automotive innovation and auto insurance experts cautioned that in order to capitalize on this opportunity, stakeholders will need to invest in the infrastructure to support large-scale connectivity, whether digital (e.g., operating systems, cloud platforms), physical infrastructure (e.g., sensor-embedded roadways), or data analysis capabilities.

Finally, organizations seeking value from data will have to contend with the ethical responsibility that comes with data ownership. Companies including Amazon, SiriusXM and GM have been asked to provide audio recordings or live location information for use in emergency response, investigations, or court cases. The rules around obligation to act are unclear but it will become increasingly important to identify and test use cases as vehicle connectivity increases.[55]

Consumer experience

In the near-term, the private sector is focused on improving the driving experience and therefore customer satisfaction: "The first go-to-market is around driver experience, driver efficiency and convenience."[56] As OEMs rebrand themselves as mobility providers, consumer experience becomes an increasingly important differentiator throughout the customer lifecycle, "turning customers into advocates".[57]

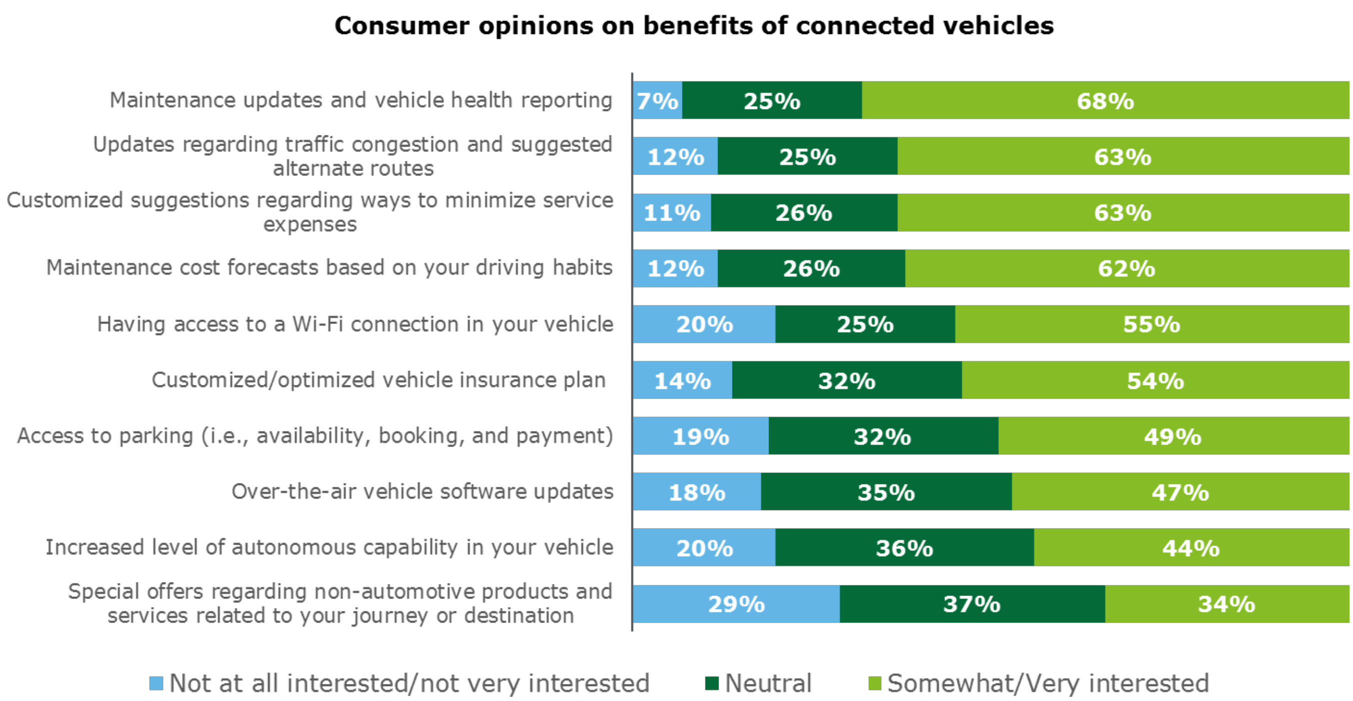


Figure 8 – Consumer opinions on the benefits of connectivity

According to the 2018 Global Automotive Consumer Study, over half of Canadian consumers would see great value in a number of personalized services delivered directly to their vehicle, increasing the value of the connected features and data generated by these vehicles, from personalized content to complex analytical models running on board a vehicle to predict service needs, notify the driver in

[55] Fox-Brewster, T. (201). Cartapping: How Feds Have Spied on Connected Cars for 15 Years. Forbes.
[56] Coppola, G. & Welch, D. (Feb. 20, 2018). The Car of the Future Will Sell Your Data. Bloomberg.
[57] The Connected Vehicle: Big Data, Big Opportunities. (2015). SAS Institute.

real time, and direct that driver to the nearest dealership (see Figure 8).[58] Mobility providers (including automakers, suppliers, and technology providers) will likely need to leverage a data-driven understanding of customer journeys and preferences to offer a truly differentiated in-transit entertainment experience.

Automakers including Toyota, BMW, and GM already have built in features to customize the driving experience based on data pulled from connected cars, including service scheduling, customized infotainment settings, and deals from third party service providers.[59] These manufacturers emphasize that data will allow them to build a better driving experience – enabling cars to predict flat tires, find a parking space or charging station, alert municipal services to intersections with frequent collisions or help protect drivers from crime.[60]

As technology providers told us, there is an unprecedented opportunity to personalize the vehicle experience, yet OEMs may not have the digital capabilities to act today. As a traditionally capital-intensive, "wholesale" industry, OEMs will need to shift to managing "customer lifetime value."[61] Figure 9 illustrates the positioning of OEMs in terms of customer experience maturity today.[62]

Figure 9 – OEM maturity in customer experience capabilities

Traditional players seeking to offer a differentiated customer experience might invest in internal capacity or seek out non-traditional partnerships. OEMs might look to e-commerce providers, financial services, or hospitality providers as

---

[58] The Connected Vehicle: Big Data, Big Opportunities. (2015). SAS Institute.
[59] Muller, D. (Feb. 2018). Connected cars serve up a feast of consumer data, but who will benefit? Car and Driver. https://blog.caranddriver.com/connected-cars-serve-up-a-feast-of-consumer-data-but-who-will-benefit/.
[60] Ibid.
[61] Dinsdale, A. & Berdichevskiy, A. (2018). The Future is Now: Transforming the Automotive Customer Experience.
[62] Reproduced from Dinsdale, A. & Berdichevskiy, A. (2018). The Future is Now: Transforming the Automotive Customer Experience.

leading practice in the customer experience space. One customer experience expert stated: “Customer understanding will be the biggest enabler for all and the biggest gap for some in cornering the connected and autonomous vehicle market”.

Telecommunications companies, media producers, and advertisers will also play key roles in crafting the in-transit experience. Wireless personalized audio/video streaming and web browsing through mobile devices, behaviour-based advertising, and vehicle entertainment systems will become increasingly important, with demand for personalized content growing as the need for human intervention in monitoring the environment and performing driving tasks decreases.[63] Deloitte estimates that revenue from connected car services including infotainment and navigation could reach $40 billion globally in 2020, with demand for network services following to telecommunications firms and other providers. In turn, media producers and advertisers in turn might capitalize on opportunities by partnering with automakers and mobility managers to participate in shaping the in-vehicle experience.[64]

Improved efficiency

Mobility researchers are optimistic about the possibilities to use data to better understand the movement trends of people across the province. Advanced public transit providers today have good information on movement patterns related to trains and buses, but this is the first time city and transportation planners as well as mobility providers could have available real-time data on the origin and destination of vehicles (depending on data ownership and sharing agreements, as discussed further below).

This will allow a number of stakeholders to strategically plan for maximum efficiency and effectiveness:

- Transit providers and public sector entities might incentivize distribution of peak hours to manage congestion
- Transit providers (e.g., Metrolinx) might leverage data on where passengers travel to next and in what vehicle for a range of transit planning purposes
- Employers might change working hours to allow for worker flexibility

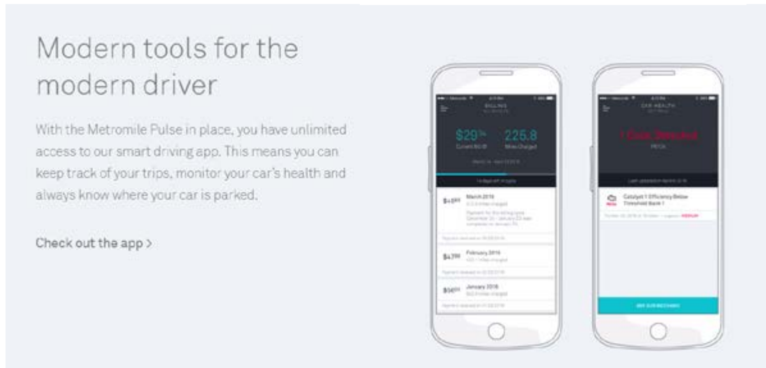
[63] Smud, D., Wigginton, C., Ninan, S., Ramachandran, K., & Moceri, P. (2017). Connecting the future of mobility: Reimagining the role of telecommunications in the new transportation ecosystem. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/role-of-telecommunications-in-new-mobility-ecosystem.html#endnote-sup-21
[64] Merchant, G., Schlaff, D., & Pankratz, D. (2017). Experiencing the future of mobility: Opportunities for the media and entertainment industry. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/opportunities-for-media-and-entertainment-industry.html

- Providers of auxiliary services (e.g., retail) might plan physical locations and advertising strategies according to common routes

Municipal governments will have to contend with a loss in annual revenue from fuel taxes, public transportation fees, tolls, vehicle sales taxes, municipal parking, and registration and licensing fees, driven today by individual ownership models.[65] The City of Toronto collected almost $60 million in parking violation fines alone in 2016;[66] a recent report found that the 25 largest municipalities in the United States generated up to $5 billion dollars in vehicle usage-related revenue, with smaller jurisdictions most likely to rely significantly on parking or traffic enforcement revenues that might be all but eliminated as autonomous vehicles reach significant saturation in the market. Municipalities might explore new options, including taxing movement through road usage tolls or dynamic pricing for particular times of day, routes travelled, and vehicle type, to optimize the use of public assets and supplement some of the lost revenue.[67]

Autonomous and connected vehicles will complement rather than replace public transit as "one mode of a multi-modal transportation system." Research from the Bloomberg Philanthropies and the Aspen Institute claims, "The most common anticipated role for AVs is bridging existing gaps at the edges of transit systems, a crucial link that planners call the last mile."[68] Their research

Case Study: metromile



Metromile is considered leading practice in giving consumers ownership over their mobility experience.

The company is a digital pay-per-mile insurance provider active in 7 states. Drivers plug in a wireless device to measure the number of miles driven over a month. Consumers pay a monthly base rate plus a per-mile rate based on age, type of vehicle, and driver history. As part of their monthly rate, consumers get access to their data through the Metromile App, allowing them to keep track of miles, monitor the vehicle's health and locate the vehicle at any time.

Source: Metromile website. https://www.metromile.com/insurance/

[65] Corwin, S., Vitale, J., Kelly, E., & Cathles, E. (2015). The Future of Mobility: How transportation technology and social trends are creating a new business ecosystem. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/transportation-technology.html
[66] Parking Ticket Activity. (2016). GM19.15 Report for Action. Toronto Parking Authority. https://www.toronto.ca/legdocs/mmis/2017/gm/bgrd/backgroundfile-102102.pdf
[67] Ibid.
[68] Berman, B. (2018). An Open Network of Autonomous Vehicles Could Solve the "Last Mile" Problem. Medium.

estimates that the last leg of a trip is associated with up to one-third of the overall cost.[69]

The World Economic Forum (WEF) writes, there is a role for public sector entities as system operators to "create a more optimal equilibrium of supply and demand across modes." [70] While system-wide balance and efficiency might mean fewer public transit and other related assets, it might also provide insight into where gaps in adequate, accessible transport exist (e.g., rural areas).[71] For this to occur, however, transportation specialists emphasized the necessity of building interoperable infrastructure to support connected systems.

Powerful wireless technology infrastructure will be a critical enabler for collecting and acting on traffic data, vehicle alerts, energy consumption, and countless other use cases.[72]. 5G, or next generation networks, are software-controlled platforms that improve bandwidth and allow for seamless connectivity between technologies.[73] The Government of Canada is investing $200 million in a 5G corridor, working through a public-private partnership with the Ontario and Quebec governments and five global digital technology organizations.[74] The Evolution of Networked Services through a Corridor in Quebec and Ontario for Research and Innovation (ENCQOR) will use the federal funding for research into 5G wireless technology, with private technology companies investing another $200 million to develop a network of linked research facilities and laboratories that will be open for testing.[75] Canada's three major wireless carriers are also running 5G tests and are planning to deploy 5G technology for commercial use by 2020 at the earliest – coinciding with the introduction of the first commercial launches of Level 4 automated vehicles.[76]

Environmental benefits

The scale of environmental benefits will rely on the level of shared vehicle ownership and the impact autonomous vehicles have on reducing congestion and collision rates. As discussed above, data generated by autonomous vehicles could allow drivers to avoid congestion by selecting an optimal speed or route of travel: "When combined, vehicle automation and infrastructure connectivity can mitigate many of the factors that contribute to congestion."[77] Less time spent idling and on the road will reduce fossil fuel consumption and emissions. Figure 10 illustrates an estimate of per capita fuel economies to be realized from

---

[69] Ibid.
[70] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem)
[71] Ibid.
[72] Benjamin, S. (2018). Super-fast, next-generation 5G wireless to get $200M research boost from governments. CBC News.
[73] Building Digital Infrastructure in Ontario to Develop New Tech Products. (2018). News Release, Government of Ontario.
[74] New Canadian partnership in next-generation wireless technology. (2018). Innovation, Science and Economic Development Canada.
[75] Benjamin, S. (2018). Super-fast, next-generation 5G wireless to get $200M research boost from governments. CBC News.
[76] New Canadian partnership in next-generation wireless technology. (2018). Innovation, Science and Economic Development Canada; Dobby, C. (2018). Ottawa to announce funding for '5G corridor' in Ontario and Quebec. Globe and Mail.
[77] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.

autonomous vehicles, assuming that networked AVs that are smaller and safer could increase fuel economies over more conventional vehicles.

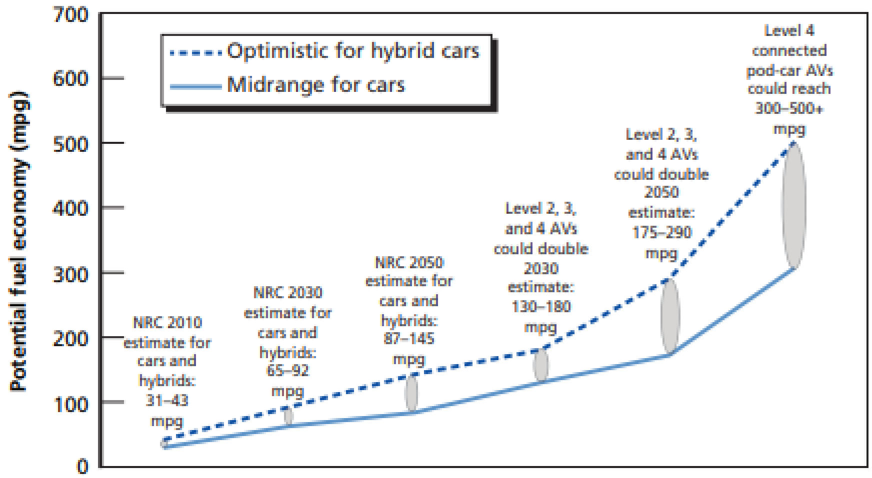


Figure 10 – Range of potential fuel economy improvements for conventional, hybrid, and autonomous Cars (Image from RAND Corporation RR443-2.6)

Anderson et al. summarize three impacts that connected and autonomous vehicles might have on congestion: reducing traffic delays due to crashes, optimizing vehicle throughput, and changing the total vehicle-kilometer-traveled (VKT). The scope of benefits, however, is uncertain, depending on the level of autonomy and the level of adoption. Advanced driver assistance systems have already caused modest improvements in collision rates globally and greater levels of automation and connectivity will allow central management of vehicle movement flow. That said, a number of factors during the transition stage, including driver distraction, mix of vehicle capabilities on the road, and more demand for travel might actually increase collisions, traffic flow, and total VKT.[78]

Some experts contend that "self-fueling and self-parking, increased use of AVs by those unable to drive, an increased number of trips (both unoccupied and occupied), [and] a shift away from public transport and longer commutes" will all contribute to an increase in VKT (the U.S. National Highway Traffic Safety Administration, or NHTSA, has estimated by 10%).[79] Convenience, accessibility, cost, time use, privacy, and facilitated commuting will all contribute to this growing demand. Some researchers, however, maintain that increasing fuel

[78] Hart, A. (2016). How autonomous vehicles could relieve or worsen traffic congestion. SBD Automotive/HERE.
[79] Bagloee, S.A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous Vehicles: challenges, .opportunities, and future implications for transportation policies. Journal of Modern Transportation, 24 (4), pp. 284-303. https://link.springer.com/article/10.1007/s40534-016-0117-3#Sec17; Planning for Autonomous Vehicles: Imagining Alternative Futures Technical Report. (2016). Ryerson University, prepared for City of Toronto Transportation Services. http://transformlab.ryerson.ca/wp-content/uploads/2016/12/Ryerson.University.Nov_.2016.Studio.Technical.Report.pdf.

prices, the rise of the electric vehicle and a younger generation not as interested in purchasing personally owned vehicles will outweigh the increase in VKT, resulting in a net decrease in energy consumption.[80]

The Canadian Standing Senate Committee on Transport and Communications has emphasized that maximizing environmental benefits will rely on controlling vehicle use through efficient road and traffic pricing policies and complementary technological advances (e.g., electric vehicles).[81] Norway, the UK, and France have all established phase-out plans for gas and diesel powered vehicles over the next decade, while ten other countries have set official electric vehicle sales targets.[82] The European Commission may be considering an EU-wide electric car quota to be achieved by 2030, similar to the approach taken by California and a number of other states.[83] These measures appear to be successful, with Norway leading the world in electric vehicle uptake.[84]

A recent study from the University of Michigan found that without a parallel shift to battery-powered electric vehicles, the added weight, electricity demand, and aerodynamic drag from sensors and computers in autonomous vehicles will drive the lifetime energy use and greenhouse gas emissions of autonomous vehicles.[85] Electric vehicles tested can have up to 40% lower lifetime greenhouse gas emissions than vehicles with internal combustion engines.

Ontario has established multiple incentive, education and awareness programs to encourage uptake of electric vehicles and achieve its climate change goals, including rebates for individual, commercial, and school bus vehicle operators and the installation of an electric vehicle charging station network.[86] Ontario, British Columbia, and Quebec – provinces with consumer incentives programs in place – lead EV adoption across Canada, with Ontario driving a 68% increase in electric vehicle sales over 2017.[87] Experts remain skeptical, however, that these measures have created sufficient momentum for Ontario to reach its unofficial goal of electric vehicle sales making up 5% of total sales by 2020.[88] Some of the barriers currently limiting uptake in Ontario (e.g., short-range travel limitations, reliance on charging stations) might be overcome by embedding connected and autonomous technology in electric vehicles. For instance, a vehicle might notify

---

[80] Ibid.
[81] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[82] Petroff, A. (2017). These countries want to ditch gas and diesel cars. CNN Money; Fickling, D. (2017). Electric cars reach a tipping point. Bloomberg.
[83] Neslen, A. (2017). EU 'increasingly likely' to implement electric car quota, despite denials. Climate Home News.
[84] Rasmussen, G. (2017). Electric vehicle subsidies needed to entice Canadian buyers: Report. CBC News.
[85] Gawron, J.H., Keoleian, G.A., De Kleine, R.D., Wallington, T.J., and Chul Kim, H. (2018). Environmental Science & Technology, 52(5), 3249-3256.
[86] Cars are Evolving. (2018). Government of Ontario.
[87] Lambert, F. (2018). Report shows electric vehicle sales grew 68% in Canada last year. Electrek.
[88] Jones, A. (2017). Ontario will miss its 2020 electric vehicle target. Toronto Star

its operator when charging is needed and self-direct to the nearest charging station at the optimal time.[89]

Overall, the potential gains in environmental benefits will be significantly influenced by the rate of convergence of connected and autonomous vehicles with electric powertrains, as well as complementary features designed to curb unproductive increases to VKT. Ontario is working with Transport Canada, Innovation, Science and Economic Development Canada, other provincial and territorial governments, and industry stakeholders, to develop a Canada-wide zero-emissions strategy by 2018.[90] These complementary initiatives may help in advancing sustainable transportation options.

Accessibility and inclusion

Finally, data generated by CVs and AVs might allow increased mobility for a greater segment of the population, including those living in underserved areas, rural populations, seniors, and those unable to drive due to a disability. Benefits of increased automation could include greater independence, reduction in social isolation, and access to essential services.[91] Autonomous vehicles might be routed to particular locations or pre-programmed to transport those with mobility issues to their destination.

Data on driver preferences and in-vehicle needs might also allow for automatic programming of vehicle

Case Study:

Uber has been acting as public transit in Innisfil, a small Ontario town with a sprawling population of 36,000. Since the pilot launched in May 2017, the town has spent just under $150,000, or an average of $5.62 per trip, partially subsidizing fixed route and regular Uber rides as a more cost effective option than implementing a fixed-route bus service to bridge gaps in transit service. The pilot has been extended and could be monitored for to determine its impact on accessibility and its sustainability as a model.

Source: Siekierska, A. (2018). Innisfil, Ontario sticks with its Uber-as-public-transit plan, extending its pilot project. National Post.

[89] Planning for Autonomous Vehicles: Imagining Alternative Futures Technical Report. (2016). Ryerson University, prepared for City of Toronto Transportation Services. http://transformlab.ryerson.ca/wp-content/uploads/2016/12/Ryerson.University.Nov_.2016.Studio.Technical.Report.pdf.

[90] Transportation 2030: Green and Innovative Transportation. (2018). Government of Canada. https://www.tc.gc.ca/eng/future-transportation-canada-green-innovative-transportation.html

[91] Anderson, J.M., Kalra, N., Stanley, K.D., Sorensen, P., Samaras, C., Oluwatola, O.A. The Promise and Perils of Autonomous Vehicle Technology. (2016). RAND Corporation.

settings to accommodate different driver abilities. The greater the level of automation (moving to future states 3 and 4), the greater the population able to use the vehicle.

This is tied to broader interoperable mobility. A WEF report claims that greater data accessibility and transparency can lead to new insights on the mobility patterns of passengers and goods, allowing government, in partnership with private-sector providers, to invest in rural or underserved areas (e.g., new roads, transit, space planning), enabling consumers to make informed choices on how and when they travel or move goods, and providing the private sector visibility in utilization, with opportunities to optimize “empty miles” and other waste.[92]

The WEF has suggested mandated coverage areas and accessibility requirements as a standards-based approach to ensuring equity.[93] Experts interviewed for this report thought that accessibility in general was an area that merited further study, as global research and development to date has focused on core operations and safety.

Implications for Ontario: CV/AV data will only improve conditions for Ontario citizens, businesses, organizations, and governments if the vehicles are deployed safely, sustainably, and accessibly and if the ownership and use of that data is clearly defined. Federal, provincial, and municipal governments could work together and with industry to determine appropriate standards that enforce these principles while allowing flexibility and space for innovation.

Areas for further research

1. Provincial and municipal governments could work with industry, public safety organizations, and community organizations to develop policy tools specific to incentivizing safe passenger behaviour and driver responsibility as vehicles transition to Level 3 automation and above.
2. The province might monitor decisions made by industry players and partnerships on data ownership and access to determine whether policy or regulatory intervention is needed as use cases for data sharing and monetization become more complex and operate cross-sector.
3. Academic, industry, and government actors could collaborate to develop a comprehensive taxonomy of datasets and types likely to be generated by connected and autonomous vehicles in order to identify particular data needs and determine best use for each type.
4. Relevant provincial ministries could continue to coordinate on parallel innovations in electric, autonomous, and connected vehicles to identify areas for mutual benefit or complementary research and development.

[92] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem).
[93] Ibid.

5. All mobility ecosystem actors could further study the implications of connected and autonomous vehicles on accessibility and inclusion, with a focus on how data might be used to help maximize these benefits.

Data sharing

Data sharing models

Data generated by connected and autonomous vehicles will be available to a range of stakeholders – both in the public interest, as discussed below, and for commercial gain or business intelligence.

Except in cases where that data is deemed to be personal (as discussed in the following section), the issue of ownership and access for shared data is still being debated in Ontario and globally. What is clear from the literature and through consultations across sectors is that the same data type or dataset might be useful to a number of stakeholders and might actually improve safety outcomes. As an example, anonymized collision data would be of use to manufacturers looking to improve products and services, insurers to determine claims payments, other manufacturers to evolve their technology, and public sector entities for transit planning. One data management expert emphasized that the best opportunity for developing data-sharing protocols is when the solution can be applied to problems that plague an entire industry and all stakeholders in that industry stand to benefit.

Two broad models exist for data sharing:

- Voluntary data sharing (ad hoc or based on a memorandum of understanding or official partnership)
- Mandated data sharing (by legislation or regulation)

Table 2 illustrates examples of where these data sharing models are being explored, with platform developers, academics, and other data experts divided on which structure is most effective (e.g., whether negotiated through reciprocal agreements or legislated and hosted by a single party – likely government – on an open platform).

Table 2 – Emerging Data Sharing Models

	Voluntary data sharing	Mandated data sharing	
Where is it being explored?	Research hubs in Canada (e.g., Waterloo Centre for Automotive Research), research hubs and demonstration sites in the United States (e.g., Mcity)	California automated vehicle testing zones	UK autonomous vehicle policy
Who is involved?	Automotive companies, technology developers, digital and physical infrastructure providers, researchers, local municipalities	California Department of Motor Vehicles	UK Department for Transport, Center for Connected and Autonomous Vehicles
How does it work?	*Waterloo Centre for Automotive Research:* Research is ongoing to develop an open data platform. Multiple companies across sectors would have access to information generated through connected and autonomous vehicle research, including on safety, navigation/HD mapping, data analytics and cyber security, among other areas. Mapping in particular would involve partnerships with regional municipalities (e.g., Stratford, Windsor-Essex, Detroit) to share data on streets and vehicle performance.	California Regulation states that a Report of Traffic Collision Involving an Autonomous Vehicle (form OL 316) must be submitted within 10 business days of the incident. Reports are posted on the DMV website. Further, every manufacturer authorized to test autonomous vehicles on public roads must submit an annual report summarizing the disengagements of the technology during testing.[94]	The proposed policy includes a data sharing framework, as well as transmission, processing, and storage of data, in consultation with the EU Collaborative ITS Platform and at United Nations Economic Commission for Europe (UNECE).

[94] Testing of Autonomous Vehicles with a Driver. (Jan. 2018). State of California Department of Motor Vehicles.

	Mcity: Participants in Mcity share data outputs with other Mcity partners, allowing early access to research information and findings. Participants have discussed formalizing sharing through a data co-operative or data vault.	
How might this model be delivered?	• Neutral open data platforms (run by partners, by public sector entity, or by academic institution) • Data co-operatives • Data marketplaces	• Public sector entity or independently hosted data repository/"vault"/platform, with varying degrees of openness depending on the data • Regular reporting from private sector data handlers/owners, with data stored privately

With so many parties holding data, there may be confusion over which one is the "true" source for use by insurers, law enforcement, regulators, and others. Some industry players have suggested a neutral, government-controlled repository of vehicular data, where auto manufacturers might transfer data to be used by relevant stakeholders.[95] The Insurance Bureau of Canada (IBC) recommends that the provincial government consider making testing and collision data available publicly, as in California. This would be a key input to insurers seeking to understand emerging vehicle risks and adapt their products and underwriting and rating practices accordingly.[96]

[95] Proposed Amendments to Ontario Regulation 306/15: Pilot Project – Automated Vehicles. (2018). Submission to the Ministry of Transportation by the Insurance Bureau of Canada.
[96] For a more detailed discussion of the implications of connected and autonomous vehicles for the insurance industry, see Connected and Autonomous Vehicles in Ontario: Implications for Insurance

Some stakeholders suggested that as “first mover” advantages are removed across the ecosystem, there will be more of a move towards sharing (as seen in Mcity). Others emphasized the competitive advantage of partnering early. Industry consortia are already forming: as one example of many, the Automotive Information Sharing and Analysis Center (Auto-ISAC) was formed in 2015 between Global Automakers, Auto Alliance, and 14 automakers to foster collaboration “that creates a safe, efficient, secure and resilient connected vehicle ecosystem”. Auto-ISAC shares and analyzes actionable intelligence on cyber security risks, exchanges best practices, and collaborates with solutions providers, industry associations and non-profits, and government, academic and research organizations.[97] Larger consortia such as Auto-ISAC and B2B partnerships between auto manufacturers, technology providers, and other third parties, are brokered on mutual benefit, exchanging data for analysis or business intelligence capabilities.

Use of data in the public interest

Use of data from connected and autonomous vehicles is widely seen as an opportunity to promote public interest. Some data elements might be critical for public sector organizations to better serve citizens and to promote safety, accessibility, equity, and prosperity – for instance, using data generated by connected and autonomous vehicles for smart and sustainable urban planning that optimizes use of space, or funding research to spur innovation and economic growth. The public sector might also use data to design incentives for private companies to align with public priorities (e.g., accessibility, mobility for rural areas, etc.). This might be done through subsidies, preferential access to digital infrastructure, or other means.

In a recent report, the WEF writes:

> As data sheds light on the mobility patterns of passengers and goods, the entire system becomes more predictable. Increased availability of data allows for better and more informed transport planning and investment, such as where and when to carry out road maintenance, for example, or whether to add additional bus services to a particular neighbourhood.[98]

“The public sector will have to regulate service providers to ensure consumers are appropriately protected and broader societal goals are met, while also creating conditions that encourage and incentivize private-sector innovation.”

- **World Economic Forum**

[97] Auto-ISAC Launches Strategic Partnership Programs. (2017). PR Newswire.
[98] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem)

In order to advance the public interest, the report encourages "foundational standards" for data sharing between the public and private sectors, as well as focused efforts to determine which data elements are critical to each organization's operation and "how, by whom and for what purpose data will be used."[99] A number of experts stressed that a foundational framework or set of standards could determine who is collecting data, what data they are not collecting (whether due to regulation or because it is not of value to them), and what gaps exist. This framework would be especially important for data that might be of use to both the public and private sector, such as accident or traffic flow data that might be monetized while also used to promote public safety.

In testimony to the Canadian Senate Standing Committee on Transport and Communications, several witnesses suggested that guidelines be developed to determine when information sharing between sectors or between the public and public sector entities is appropriate. Anonymized data collected for public safety purposes (e.g., related to collisions, unsafe environments, or cyber security threats) was seen as distinct from information collected for purely economic purposes.[100]

Use of data in the public interest must always respect privacy and security, particularly as the flow of data from connected devices increases. The Information and Privacy Commissioner of Ontario (IPC) has commented on how best to balance the Open Government imperative with privacy and security as the flow of connected data increases, stating: "while Open Government offers many benefits to government, businesses, and the public, the pursuit of increased government transparency and public engagement could negatively affect individuals' privacy if initiatives are not properly designed, implemented, and monitored".[101] The Commissioner offers five best practices to protecting privacy while enabling Open Government, including defining one's purpose, ensuring one has the appropriate authority to collect, use, or disclose personal information, data minimization, clear exceptions to Open by Default, and de-identification.

The US Department of Transportation has begun drafting policy on this topic, recently conducting consultations on its *US DOT Guiding Principles on Voluntary Data Exchanges to Accelerate Safe Deployment of Automated Vehicles*. A summary report of recent consultations on the principles and associated framework states: "Within and across all modes of transportation, data exchanges will be key to accelerating the safe deployment of automated vehicles in the United States. This includes the mutually beneficial exchange of data among private sector entities, infrastructure operators, and policy makers from

[99] Ibid.
[100] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communications.
[101] Open Government and Protecting Privacy. (March 2017). Office of the Privacy Commissioner of Ontario.

various levels of government."[102] The report outlines seven high-priority use cases for voluntary data exchange, each with specific data types, datasets, and key stakeholders and data exchange models for consideration.[103]

Data might also play a role in encouraging public acceptance and adoption of connected and autonomous vehicles, as benefits to the public are likely to increase as the mix of levels of automation on the road decreases and vehicle behaviour harmonizes.

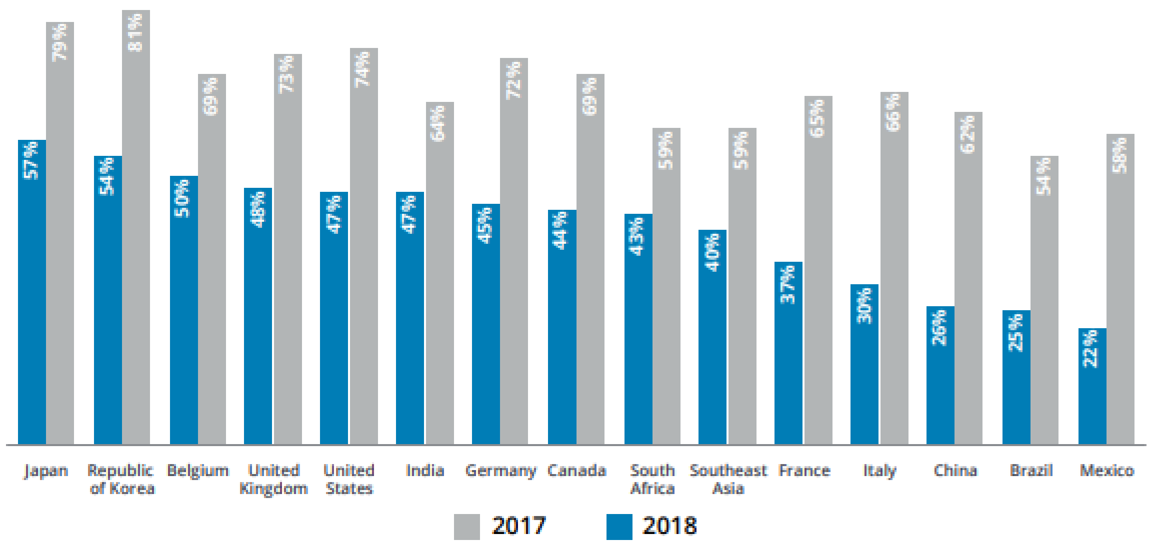


Figure 11 - Percentage of consumers who think fully self-driving vehicles will not be safe (2017 vs. 2018)

The 2018 Deloitte Global Automotive Consumer Study on advanced vehicle technologies found that safety, brand trust, and cost are all major factors that could increase the share of consumers accepting of autonomous technology.[104] Today, approximately 51% of Ontarians trust autonomous vehicles.[105] Figure 11 shows the percentage of Canadian consumers who think self-driving vehicles will not be safe is decreasing with increased exposure and testing, in line with other global regions.

Many experts spoke about the unique challenges in exposing Ontarians to autonomous vehicles. One autotech industry expert explained: "One of the issues is geography. Companies are not testing as much in Canada because they haven't

[102] Roundtable on data for automated vehicle safety. (Jan. 2018). U.S. Department of Transportation.

[103] Use cases include: Monitoring planned and unplanned work zones, providing real-time road conditions, diversifying automated vehicle testing scenarios, improving cyber security for automated vehicles, improving roadway inventories, developing automated vehicle inventories, and assessing automated vehicle safety features and performance

[104] Giffi, C.A., Vitake Jr., J., Schiller, T., Robinson, R. (2018). A reality check on advanced vehicle technologies. Deloitte Global Auto News Supplement

[105] Half of Canadians trust self-driving cars. (2017). Canadian Press. https://www.thestar.com/business/tech_news/2017/09/14/half-of-canadians-trust-self-driving-cars-survey-says.html

figured out how to deal with snow. In California, you see them driving around occasionally, but in Ontario they only drive around specific areas".[106] A technology provider echoed: "Gradual exposure is what people will need. Gradual exposure and a willingness for companies to go out and test these vehicles in Canadian conditions."

Implications for Ontario: Consortia of industry, academic, and public sector actors are already forming with the purpose of sharing information. Technical standards might improve the consistency and applicability of the data shared in these partnerships, while CV/AV-specific guidelines around what can and should be shared in the public interest would enhance predictability.

Areas for further research

6. As above, academic, industry, and government actors could deepen understanding of the particular data needs of each player and determine which group or partnership is best to collect, store and use different data types.
7. The provincial government could further consider the need for standards or regulation with respect to data access for specific data types that might contribute to public interest or materially help research and business development across the ecosystem and might be shared for mutual benefit.
8. Researchers, government actors, and representatives across industries could work together to pilot different data sharing models, developing a deeper knowledge of the benefits of each model for different contexts and use cases.

[106] Researchers at the Waterloo Centre for Automotive Research and companies testing autonomus vehicle components and parts at the Kanata North Tech Park in Ottawa are investing in solutions to inclement weather. Canada's more difficult driving conditions have actually been a draw for researchers and developers looking to test products in harsh conditions. See: Lampert, A. (2018). In Canada, Driverless Cars Learn to See in the Snow. https://www.reuters.com/article/us-autos-selfdriving-canada/in-canada-driverless-cars-learn-to-see-in-the-snow-idUSKBN1GX2V9

Privacy and protection of personal information

Legislation and regulation

As organizations explore data sharing models, compliance with federal and provincial privacy frameworks will be critical and increasingly complex. According to Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), organizations cannot require an individual to consent to the collection, use, or disclosure of personal information "beyond that required to fulfil the explicitly specified, and legitimate purposes" or "for purposes that a reasonable person would consider are appropriate in the circumstances."[107] A Government Accountability Office review found that surveyed automakers' policies only partially reflected leading privacy practices. All written privacy notices were easily accessible, but none were written clearly and none clearly identified data sharing and use practices.[108] In addition, automakers only represent one group of stakeholders potentially accessing consumer data. The complex ecosystem of players to whom consumers would have to consent and the similarly unclear language of many policies in Canada has prompted Canadian experts to call consent impossible under many circumstances.[109]

As the volume, complexity, and real-time availability of data increases, the IPC and the Office of the Privacy Commissioner of Canada have sought to clarify how existing legislation applies to new contexts. Notably, both organizations have issued guidance to aid compliance with existing federal and provincial provisions on the issue of meaningful consent.[110] Draft guidelines from the Privacy Commissioner of Canada currently undergoing public consultation include practical principles such as:[111]

- Emphasize key elements: purposely surface key information including what personal information is being collected, which parties will share that data, for what purposes, and the risk of harm
- Allow individuals to control the level of information they get and when: structure information in manageable, layered form
- Provide individuals with clear options to say "yes" or "no": individuals should be given a choice as to whether their data is used in all possible cases; the only exceptions are where the information is integral to fulfilling an "explicitly specified and legitimate purpose"
- Be innovative and creative: use interactive tools and customized interfaces to make the consent process digital

[107] Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act. (2018). House Standing Committee on Access to Information, Privacy and Ethics.
[108] Vehicle Data Privacy (Aug. 2017). Government Accountability Office. https://www.gao.gov/products/GAO-17-656
[109] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[110] Draft Online Guidelines: Obtaining Meaningful Online Consent. (2018). Office of the Privacy Commissioner of Canada.
[111] Ibid.

- Consider the consumer's perspective: make consent accessible and valid; consent is not legitimate unless the consumer knows what they are doing
- Stand ready to demonstrate effectiveness: be prepared to demonstrate the presence and effectiveness of a consent process
- Make consent a dynamic and ongoing process: allow policies to evolve with an organization or technology and solicit consent and feedback from consumers for any policy changes

Different privacy laws apply to different organizations depending on who is handling personal information, what type of information is involved, and whether the information is shared (see Figure 12).[112]

[112] Summary of Privacy Laws in Canada. (2018). Office of the Privacy Commissioner of Canada; *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31*; *Personal Health Information Protection Act, 2004, c.3, Sched. A; Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5)*

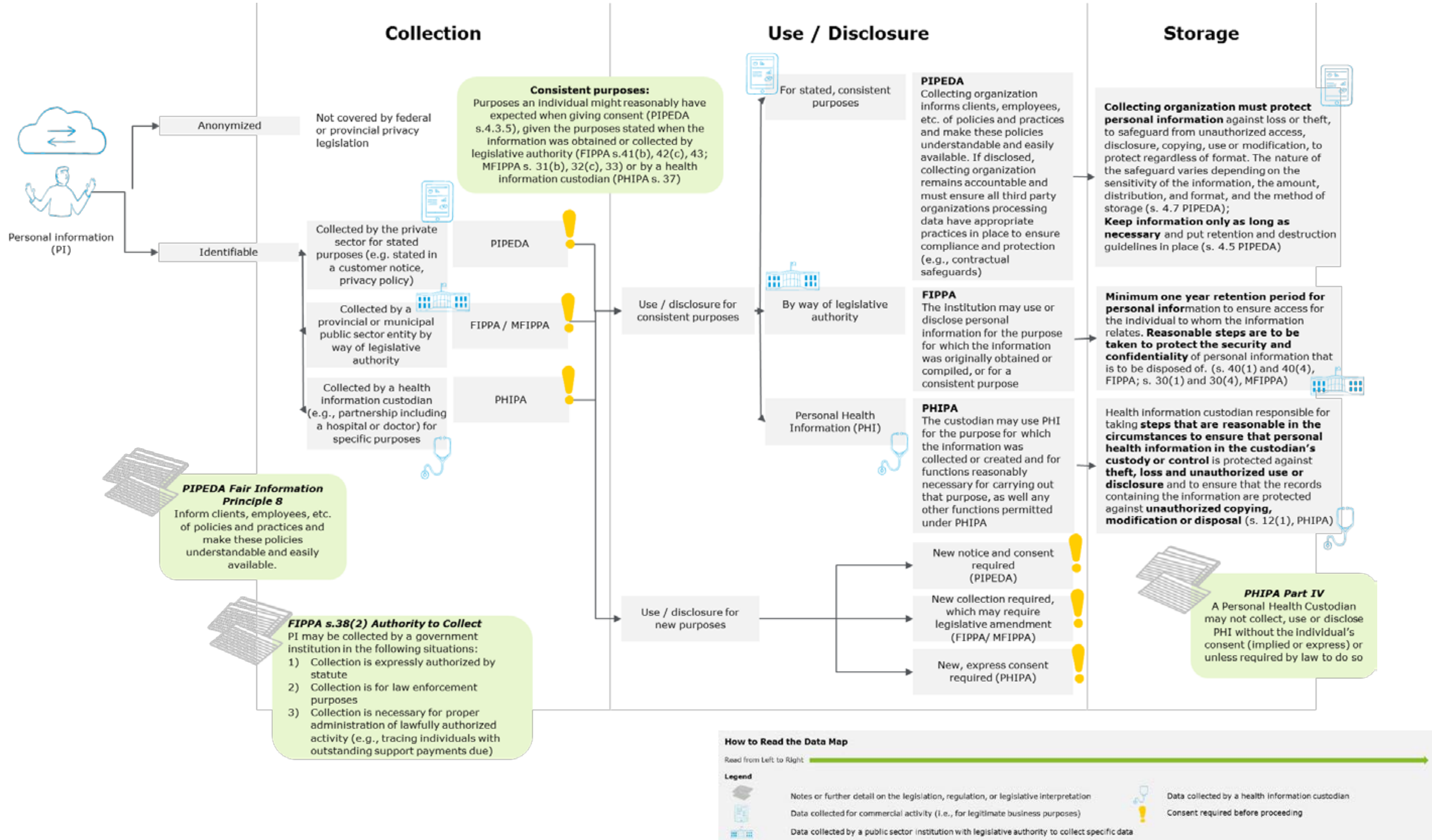


Figure 12 – Legislative data map

PIPEDA protects the collection, use, or disclosure of personal information in the course of a commercial activity, with personal information defined as "any factual or subjective information, recorded or not, about an identifiable individual."[113] This could include age, name, ID numbers, income, ethnic origin, or blood type; opinions, evaluations, comments, social status, or disciplinary actions; and employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant or intentions (e.g., to acquire goods or services). PIPEDA operates according to ten principles: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, accuracy, safeguards, openness, individual access, and challenging compliance.[114] As discussed below, PIPEDA is purposely broad in order to apply to a wide range of sectors and contexts and its interpretation continues to evolve over time.

Organizations subject to PIPEDA may only collect personal information that is necessary for identified purposes (for instance, in order to provide services and features, safety and security, or customer support, as specified in their privacy policy). This collection must be limited to what is reasonable in the circumstances and must consider the balancing of customer needs against privacy rights. This applies to all private sector parties in the mobility ecosystem, including vehicle manufacturers, digital product and infrastructure providers, and insurers. New amendments to PIPEDA are making privacy breach notification clauses and logging of security incidents mandatory under the recently enacted *Digital Privacy Act* (DPA).[115] Once enacted, the breach notification provisions of the DPA will amend PIPEDA to require organizations to notify not only affected individuals but also the OPC in the event of a breach, and other relevant stakeholders.

Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to provincial government agencies and their handling of personal information. Similarly, Ontario's *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) applies to Ontario's municipal sector. These acts seek to make information held by government available to the public, with only limited and specific exemptions, to protect personal information held by government organizations, and to provide individuals with access to their own personal information. This might include transit passenger ID numbers or name, vehicle registration information, or payment information captured by public sector providers. Finally, the *Personal Health Information Protection Act, 2004* (PHIPA), protects the confidentiality of personal health information in the control of health information custodians and to provide individuals with access and right of correction to that information.[116] Biometric information collected through sensors

---

[113] PIPEDA in brief. (2018). Office of the Privacy Commissioner of Canada.
[114] PIPEDA Fair Information Principles. (Reviewed 2018). Office of the Privacy Commissioner of Canada.
[115] Breach of Security Safeguards Regulation: Regulatory Impact Analysis Statement. (2017). Government of Canada.
[116] Summary of Privacy Laws in Canada. (2018). Office of the Privacy Commissioner of Canada.

in a connected, autonomous vehicle could fall under this regulation if the sensor manufacturer, third party data aggregator or platform, or auto manufacturer has a formal partnership with a public sector entity (for instance, a hospital, provincial crown corporations, a university, etc.).

The Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics recently recommended changes to increase the relevance and rigour of the legislation, heavily influenced by the EU General Data Protection Regulation (GDPR), which is seen as best practice and ensures a common, technology neutral standard across EU member states.[117,118] In addition, a new Privacy and Electronic Communications Regulation, building on the privacy-by-design requirements of the GDPR, would mandate manufacturers and retail distributors across EU member states to ensure third parties are unable to access and process vehicle data without consent.[119]

The Standing Committee recommendations that are most relevant to protecting personal information generated by connected and autonomous vehicles include:[120]

- to explicitly provide for opt-in consent as the default for any use of personal information for secondary purposes, and with a view to implementing a default opt-in system regardless of purpose;
- to provide for a right to data portability;
- the consideration of measures to improve algorithmic transparency;
- to modernize the *Regulations Specifying Publicly Available Information* … in order to make the *Regulations* technology-neutral;
- to clarify the terms under which personal information can be used to satisfy legitimate business interests;
- the examination of the best ways of protecting depersonalized data;
- to make privacy by design a central principle and to include the seven foundational principles of this concept, where possible;
- to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance; and
- to give the Privacy Commissioner broad audit powers, including the ability to choose which complaints to investigate.

Similarly, Australia's National Transport Commission (NTC) is currently studying the adequacy of the national regulatory framework in preparing for and

[117] Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act. (2018). House Standing Committee on Access to Information, Privacy and Ethics.
[118] 2018 reform of EU data protection rules. (2018). European Commission.
[119] Appt, S. (2018). The 'connected car' raises new world of data management, privacy and ownership. https://www.acq5.com/post/the-039-connected-car-039-raises-new-world-of-data-management-privacy-and-ownership/.
[120] Ibid.

accommodating the deployment of Level 3 autonomous vehicles.121One ongoing project is studying the sufficiency of Australia's current information privacy framework applying to government collection and use of information generated by cooperative intelligent transport systems (C-ITS; the systems that exchange information with connected vehicles) and autonomous vehicles.[122] This follows recommendations from previous stages of the NTC's autonomous vehicle regulatory reform agenda:

- "That the NTC develops options to manage government access to automated vehicle data, having regard to achieving road safety and network efficiency outcomes and efficient enforcement of traffic laws, balanced with sufficient privacy protections for automated vehicle users."[123]
- "In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information."[124]

Work is ongoing to determine whether the existing framework is sufficient, whether guidance is needed to interpret existing laws in the new context of autonomous vehicles, or if specific privacy legislation is required.

PIPEDA and similar provincial privacy laws do not apply to information that has been rendered anonymous, "as long as it is not possible to link that data back to an identifiable person."[125] While vehicle and passenger data could be anonymized and used to promote public health, fraud detection, service improvement and transportation efficiency, there is the risk that the use of Big Data analytics could "undo de-identification measures that were designed to protect individual privacy while allowing for the benefits of data analytics."[126] Big data refers to extremely large sets of data that may be computationally analyzed to reveal patterns, trends, and associations, especially relating to human behaviors and interactions. This might also be combined with metadata (e.g., data generated by technology that provides information about other data, such as an emergency transmission from a connected car) to reveal further insights about an individual or transaction. Data that might otherwise have been useable by private and public sector entities becomes personal when combined with a host of other contextual information. This might have particularly significant implications for rural or less

[121] Automated vehicles in Australia. (2018). National Transport Commission. http://www.ntc.gov.au/roads/technology/automated-vehicles-in-australia/
[122] Regulating government access to C-ITS and automated vehicle data. (2018). National Transport Commission. http://www.ntc.gov.au/current-projects/regulating-government-access-to-c-its-and-automated-vehicle-data
[123] Ibid.
[124] Ibid.
[125] Summary of Privacy Laws in Canada. (2018). Office of the Privacy Commissioner of Canada.
[126] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.

populated areas where even anonymized information on mobility patterns might be sufficient to identify an individual.

As above, the House Standing Committee on Access to Information, Privacy, and Ethics recommended that the federal government examine best practices for protecting depersonalized or de-identified data. The IPC will be releasing guidance on de-identification of data, stating that this is an important emerging issue, "which has the potential to provide the flexibility needed to achieve a better balance between privacy protection and economic value of data…[it] can be a viable solution provided it is managed appropriately."[127]

On this topic, the GDPR distinguishes between data anonymization (according to regulators, data controllers often fall short of actually anonymizing data) and data pseudonymization. Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."[128] In this way, data handlers and owners may hold de-identified data separately from "additional information," providing some flexibility around data use. Article 6(4)(e) lists pseudonymization (as well as encryption) as a safeguard for data controllers to meet legal obligations related to protection of personal information where consent has been given or where the data is being used in a manner consistent with its original collection purpose.[129] Recital 78 and Article 25 list pseudonymization as a key "technical and organisational measure" to meet "data protection by design" or "data protection by default" principles.[130] Opinions are divided in Ontario as to whether a similar distinction would be too lax or might strike the right balance between innovation in data collection and analysis and privacy.[131]

GDPR Article 22 states that individuals have "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." As algorithms are increasingly used as a tool to understand and apply data from connected and autonomous vehicles, standards for data privacy, transparency around data use, and ownership and consent (see below) might extend to these tools to understand what is being interpreted and processed and how.[132] This includes consideration for data residency during transmission,

[127] Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act. (2018). House Standing Committee on Access to Information, Privacy and Ethics; 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act and the Privacy Act.* (2017). Office of the Privacy Commissioner of Canada.
[128] Article 4(5), General Data Protection Regulation. (2018). https://gdpr-info.eu/art-25-gdpr/. This is consistent with the ISO/TS 25237:2008(E) Health Informatics—Pseudonymization, ISO, Geneva, Switzerland. 2008.
[129] Article 6(4)e, General Data Protection Regulation. (2018). https://gdpr-info.eu/art-25-gdpr/
[130] Article 25, General Data Protection Regulation. (2018). https://gdpr-info.eu/art-25-gdpr/; Recital 78, General Data Protection Regulation. (2018). https://gdpr-info.eu/art-25-gdpr/
[131] A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act.* (2016). Policy and Research Group, Office of the Privacy Commissioner of Canada.
[132] Turley, M. (2018). My algorithm doesn't fit. Deloitte Perspectives: the Future of Regulation.

management, processing, and storage (see below for discussion on Physical Data Storage).

Ownership and consent

As connected and autonomous vehicles create and transmit increasing volumes of data on passengers, vehicles, and the surrounding environment, ownership of connected and autonomous vehicle data may be dispersed across private sector organizations, public sector agencies and members of the public. In the face of increased and dispersed use, vehicle owners will continue to want their personal information protected and secure. That said, some personal information generated within connected and autonomous vehicles may be reasonably required for safety, policy or enforcement purposes (e.g., location data held by a vehicle manufacturer or service provider, constituting personal information, might be used by emergency services to locate a collision, by municipalities to improve city planning or service delivery, or by authorized officials to inform a criminal investigation).[133] Simultaneously, the private sector may want to retain this same data due to proprietary interests or potential commercial value.

Stakeholders identified issues of ownership and consent over data generated or gleaned from connected and autonomous vehicles as a current gap in policy, both with respect to personal and non-personal information.[134] One connected infrastructure provider saw this as a role for government: "Government has to step in to figure out guidance on who owns the data and making sure it's a priority and it matters." Autotech industry experts illustrated the complexity of ownership question: "To date, nobody knows who owns the telematics data. It could be a telecommunications carrier or mobile manufacturer, a Bluetooth manufacturer, an operating system provider, an automaker, a rental agency collecting information. Your information is all over the place". Some cyber security experts pointed out that the data generated by or transmitted through connected and autonomous vehicles is not so different from data generated through wearable watches or mobile phones: the data contains a range of personal and non-personal information, it may be available to a wide range of third parties (e.g., telecommunications firms, technology providers, data analysis firms) and it should be subject to the same frameworks for consent, collection, and use. One security professional suggested a model where data would belong to vehicle owners or individual passengers, with organizations offering rebates to use or access the data.

Academics working in the privacy space have emphasized the need for all stakeholders to think about privacy throughout the data lifecycle, according to

[133] Regulatory options for automated vehicles. (2016). National Transport Commission. Connected and Autonomous Vehicles: Position Paper. (2017). Society of Motor Manufacturers and Traders Ltd.

[134] Non-personal information refers to data generated or transmitted by a vehicle that does not relate to an identified or identifiable individual. In the context of connected and autonomous vehicles, non-personal information might refer to traffic flows, detected road blockages, etc. Personal information can be rendered non-personal through anonymization.

Privacy by Design principles. Privacy by Design relies on seven principles that ensure privacy is not solely a compliance exercise but rather embedded in the design of an organization, including IT systems, accountable business practices, and physical design of networks.[135] The first step is to define what is being collected, who can access it, and whether the data is sensitive. If done proactively, with the right knowledge and expertise engaged from the start, the right controls and policies can be put in place for success. Privacy consultants and academics interviewed warned that delaying this process will make data protection increasingly complex.

The European Commission has been considering similar issues, specifically looking at issues related to non-personal machine generated data, which is outside of GDPR scope. In its Communication on Building a European Data Economy, the EC recommended, among other options, that a licensing regime for anonymized data be considered, requiring manufacturers to provide access to the data they possess on fair, reasonable and non-discriminatory terms. As well, a "data producer's right" could be introduced to give the "owner or long-time user" (such as a vehicle owner) the automatic right to use and consent to use any personal or non-personal information generated by their connected or autonomous vehicle. This could at once allow a freer flow of data (by dispersing ownership rights among individuals versus having a single company – for example, an auto manufacturer – consenting to data sharing) while also solidifying the individual's right to their vehicle's data (importantly, ownership over personal information and the ability to consent or withdraw consent to its use would be maintained in all contexts). The plans will be further studied and elaborated on over the coming months.[136]

Issues of ownership become more complex as shared mobility increases. By 2020, it is predicted that ride sourcing will grow from 2.3 million to 26 million users worldwide, with traditional automobile manufacturers (e.g., GM, Ford, Toyota and Honda) launching their own models (e.g., Lyft, Maven, Chariot, etc.).[137] One privacy consultant stated: "The move towards shared vehicles dilutes personal ownership of data." Many companies (e.g., Lyft, Uber) will include specific provisions in their terms and conditions around personal information collection, use and sharing with third parties, in line with regulations. Greater adoption of ride sourcing and parallel shifts to shared ownership may bring about a fundamental shift in how data storage, processing, and sharing is viewed, with the potential for new risks: the personal information of all owners, drivers and riders is at stake. There is increased vulnerability as mobile ride sourcing, car sharing, social media, and other applications provide access to

---

[135] Privacy by Design primer. (2013). Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf
[136] Communication on Building a European Data Economy. (March 2017). European Commission. https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy
[137] The Future of Shared Mobility. (2017). MaRS TA14.5. https://www.toronto.ca/legdocs/mmis/2017/ta/bgrd/backgroundfile-101335.pdf

information on drivers' and riders' smart devices as well as if shared vehicles store data on a previous operator's journey or mobility preferences.

Many experts emphasized that third party vendor management will be key to ensuring personal information protection and data privacy. Under PIPEDA, the organization that collects and controls personal information is accountable for ensuring its use, storage, and disclosure comply with legislative requirements and protect personal privacy.[138] When outsourcing to a third party, the organization remains accountable for ensuring that the third party's processes meet legislative and organization requirements and reliably protect personal information. Ontario firms are exposed to legal liability if third party providers do not adhere to contract terms or experience a data breach. This differs from GDPR provisions, wherein data processors (i.e., third parties) as well as data controllers are newly accountable for noncompliance in ensuring that all data processing meets GDPR requirements and that the rights of the data subject are protected.[139]

One privacy expert pointed out that many organizations collect more data than what is required for their business purposes in case new use cases are identified at a later date. This increases the risk that a third party might use that data for purposes without consumer consent. The Society of Motor Manufacturers and Traders in the UK emphasizes that data protection must be observed throughout the automotive supply chain and that consumers should be provided proactively with options regarding the processing and use of their personal information.[140] Data sharing should only occur for the fulfilment of consumer services and with consent. This consent may be rescinded at any time.[141] The Senate Standing Committee recommended empowering privacy commissioners to "proactively investigate and enforce industry compliance" with existing legislation and to continue monitoring the need for further regulation related specifically to connected and autonomous cars.[142]

[138] Guidelines for Identification and Authentication. (2016). Office of the Privacy Commissioner of Canada.
[139] Article 28(1). Generation Data Protection Regulation. https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/
[140] Connected and Autonomous Vehicles: Position Paper. (2017). Society of Motor Manufacturers and Traders Ltd.
[141] Ibid.
[142] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication

Implications for Ontario: At the current pace, technological capabilities to aggregate, analyze, and use personal and other sensitive information will outpace attempts to develop standards or regulation related to meaningful consent and data ownership specific to connected and autonomous vehicles. Ontario might consider whether a provincial government-led regulatory approach or government, industry, or cross-sector consortium-led standards will best balance privacy with growth and innovation.

Areas for further research

9. Ownership of personal and non-personal information specifically generated or transferred by connected and autonomous vehicle data has not been clearly defined. The provincial government or other body (e.g., a standards-setting organization) might convene stakeholders from other levels of government, academia, and industry to study potential models, including a rules-based framework (focused on outcomes) or definitive standards by data type.
10. As part of the study of ownership issues, regulators and provincial/federal governments might assess standards for anonymization and pseudonymization, use cases on risks to de-identification, and the appropriate timing and level of individual consent specific to connected and autonomous vehicles.
11. Academic and research institutions might conduct further modelling of future scenarios for ownership and consent depending on the pace and scale of transition to shared ownership or mobility subscription models.

Cyber security risks

Risk vectors

Cyber security is an increasingly important topic of interest for industry stakeholders, researchers, and policymakers alike, particularly how these risks will increase in scope and scale as cars become increasingly connected and reliant on sensors or other automation.[143] Five key threats are associated with connected and autonomous vehicles:[144]

"This is no longer, 'My laptop crashed'. Human lives matter."

- Connected infrastructure provider

- *Theft of property*: Hackers might steal vehicles for personal or financial gain. Cargo in theft in Canada amounts to $5 billion CAD in economic losses per year and would be facilitated if hackers can access a vehicle's location, route, or password

[143] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication; The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.
[144] Securing the networked vehicle: Threat Study (2016). Deloitte.

- *Theft of data:* Connected vehicles may capture and store a range of personal information, including transaction and payment information, user credentials, and communications, as well as information on OEM's proprietary systems
- *Physical destruction and sabotage:* If remote control of a vehicle or access to its location and route is possible, a hacker might seriously damage the vehicle or surrounding property
- *Invasion of privacy:* Personal information (PI), metadata, home and work address, and communications via mobile phone could all be captured through connected and autonomous vehicles and accessed without permission
- *Fraud:* Vehicle insurance fraud could be a significant issue as insurance estimates increasingly rely on vehicle data and vehicle sharing increases in prevalence

The Organization for Economic Cooperation and Development (OECD) has highlighted "increased cyber security risks, especially when network-based systems interact directly or indirectly with primary control systems of vehicles" as a particular area of focus.[145]

As highlighted in Figure 16, the nature and scope of these privacy risks varies in each of the four future states of mobility.[146] The first state is similar to today. Though many vehicles rely heavily on proprietary, potentially vulnerable, software, an increase in connectivity as well as the quantity of code will drive risk. In the second state, the scale of risk increases with growing adoption of shared mobility and increased access to mobile devices, location, and navigation information. In the third state, increased automation and V2X exchange of data exposes vehicles to security breaches which could cause serious collisions. In the fourth state, the scale and level of severity of risks is exponential.[147]

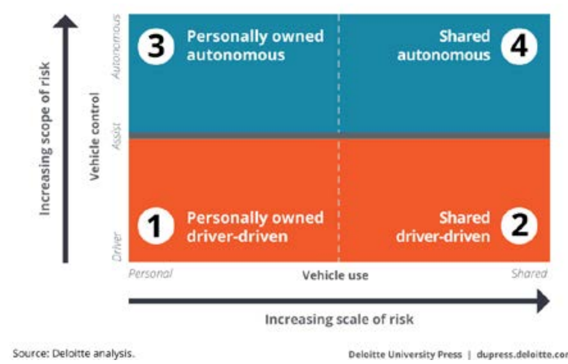


Figure 16 - Scope and scale of risk in the future states of mobility

[145] Canadian Council of Motor Transport Administrators. (2016). White Paper: Automated Vehicles in Canada.
[146] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html.
[147] Ibid.

Cyber security experts in the automotive space emphasized the growing need for safe and secure software in connected and autonomous vehicles. Figure 17 outlines some of the key risks from a passenger vehicle alone.[148]

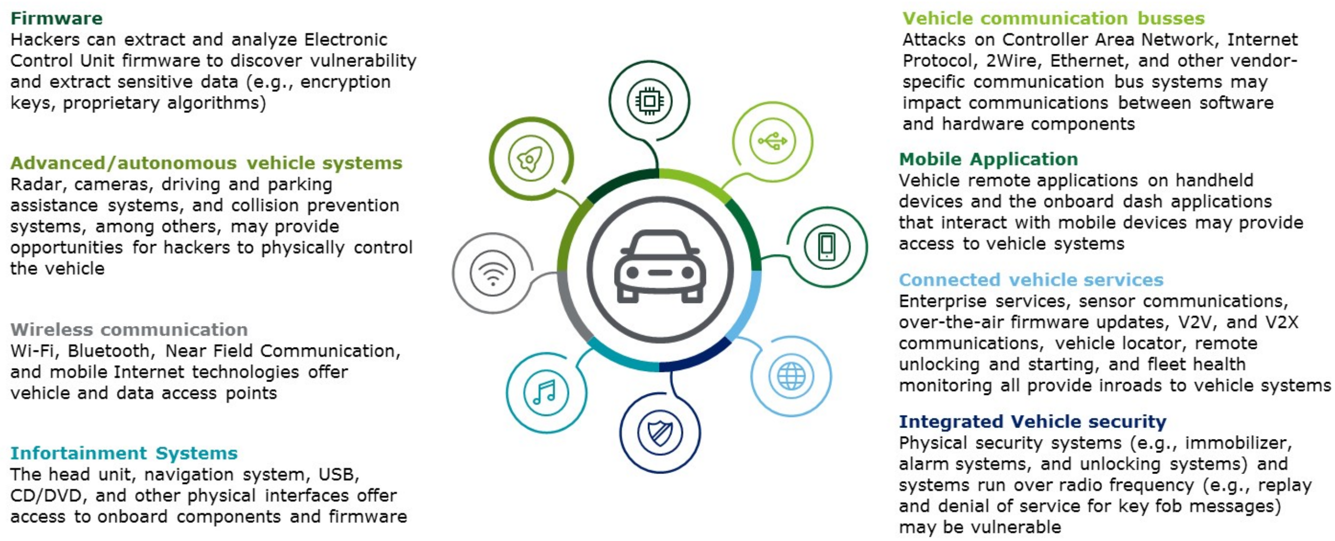


Figure 17 - Security vulnerabilities for connected vehicles

Each of these points of connection transmit data, likely to a cloud storage platform. Cyber security experts highlighted that attacks on data storage platforms or breaches in the capture or transmission of data may also compromise the security, integrity, and, importantly, safety of vehicle data.

Best practices

Various ecosystem players are at different levels of maturity in terms of cyber security capabilities, characterized by the level of knowledge and internal skills capacity on the topic of cyber security. A recent Gartner report found that the global industrial manufacturing sector spent the lowest percentage of total IT budget on cyber security at 4.3%. Cyber security FTEs represented 3.7% of total FTEs in the transportation sector and an average 5.9% of total FTEs in the industrial manufacturing sector (the average across 12 major global industries), compared with 8.3% in banking and financial services.[149] An automotive consultant echoed these findings, indicating that most OEMs share two central challenges: lack of budget to develop autonomous vehicle capabilities and talent gaps in cyber security and data protection.

[148] Ibid.
[149] IT Key Metrics Data 2018: Key IT Security Measures: by Industry. (2017). Gartner Research. ID G00341804. Note that data was collected from a global sample of organizations. Typically, these numbers do not consistently include all cyber services (e.g., Policies and Exceptions Management, Business Resilience & Recovery, Security Operations Center, Threat Intelligence, Cloud Security, Third Party Risk Management) in their estimates, hence actual cyber spend and headcount numbers are expected to be higher than reported.

This may shift as connected and autonomous technologies advance, and an overall increase in firms recognizing the importance of cyber security. An International Data Corporation (IDC) survey found that 60% of Canadian businesses rank security as the top technology priority for 2017.[150] The CIO of Canada has stated: "If you're spending a dollar on a digital service, you should spend a dollar on cyber security".[151] If followed, this industry practice has significant implications for organizational investment: according to the IDC, the global transportation industry will devote nearly half of its spending to connectivity services in 2017.[152]

Privacy experts suggested that traditional industries facing the most risk will be the first to innovate: "OEMs bear the most significant risk [in the case of a cyber attack]. The public is less concerned or focused on where parts come from." These experts identified three key leading practices that might serve as a model for organizations not traditionally focused on cyber security:

- *Follow international best practice and ensure defensive depth:* Take a layered approach to vehicle cyber security (e.g., in line with the National Institute of Standards and Technology's documented Cyber security Framework, which is structured around the five principal functions: Identify, Protect, Detect, Respond, and Recover). Consider the information technology (IT) security suite of industry standards (e.g., ISO 27000 series standards) and best practices, such as the Center for Internet Security's (CIS) cyber defense standards or Blackberry's Seven Pillars Recommendation for Automotive Cyber security.[153]
- *Build security into the Software Development Life Cycle:* Include security as a key factor in the product requirement phase and prominently identify security as a KPI to measure software quality. Consideration for security should cover planning, requirements and analysis, architecture and design, development, testing, deployment and implementation, and maintenance phases.[154]
- *Operate by "Privacy by default" and "Privacy by design" principles as the basis for products and services:* Privacy by default requires that data owners or handlers "implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed," taking into account "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity."[155] Privacy by design operates according to seven principles: proactive not reactive; preventative not remedial, privacy as the default setting, privacy embedded

[150] Wong, C. (2016). IDC says Canadian IT spending set to rebound, mobile device sales to stall in 2017. IT Business.
[151] Change and innovation in the public sector: Episode 6(2018). Shift Podcast.
[152] IDC Forecasts $1.2 Trillion in Worldwide Spending on Digital Transformation Technologies in 2017. (2017). Insurance Canada.
[153] Vehicle Cyber security. (2018). National Highway Traffic and Safety Administration. https://www.nhtsa.gov/technology-innovation/vehicle-cyber security; Blackberry's 7-pillar Recommendation for Automotive Cybersecurity. (2017). White Paper.
[154] How to Secure the 7 Stages of the SDLC. (2018). Security Innovation Europe. https://www.securityinnovationeurope.com/blog/page/how-to-secure-the-7-stages-of-the-sdlc
[155] Article 25, General Data Protection Regulation. (2018). https://gdpr-info.eu/art-25-gdpr/

into design, full functionality, end-to-end security, visibility and transparency, and respect for user privacy.[156]

Data and cyber security experts highlighted a few key best practices, based on leading industries (e.g., credit reporting, financial services):

- Strong self-regulation
- Established data management practices
- Good communication of the process, structures, and controls
- Visibility and clear guidance on how data would be collected and stored

Cyber security experts emphasized that securing connected and autonomous vehicle data and systems need not be complicated but does require a commitment to security and a holistic view. Group VP of Research at IDC Canada, Tony Olvet, recently stated: "Most Canadian organizations don't view cloud security holistically."157 Focusing on the cloud, he emphasized looking at end-to-end encryption, considering the same security factors for cloud as for an on premise data centre, and clearly defining the security responsibilities of all parties involved. Others interviewed for this report recommended establishing risk-focused controls around the most sensitive assets, vigilance by integrating threat, IT and business data for context-rich monitoring and alerts, and resilience throughout the data lifecycle from all parties impacted.158

Physical data storage

Public sector entities are likely to face unprecedented requirements for the secure storage, processing, and transmission of data. To date, public sector entities in the United States and Canada have looked to traditional cloud providers for support, including Amazon Cloud, Google Cloud, and IBM.

The format, infrastructure, and skills and investment required to support new data needs, as well as the supporting policies including retention schedules, metadata structures, and access policies, will be a key piece of further research, including modelling which types and volumes of data will be captured and retained by different levels of government and what security measures are required.

Issues of data residency, protection, and security will also become increasingly important as a number of organizations (public and private) working across jurisdictions handle connected and autonomous vehicle data, particularly with respect to personal information. Currently, PIPEDA specifies that organizations are responsible for personal information in their custody or control, including

[156] Privacy by Design primer. (2013). Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf
[157] Wong, C. (2016). IDC says Canadian IT spending set to rebound, mobile device sales to stall in 2017. IT Business.
[158] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html.

information transferred to a third party acting on their behalf for processing.[159] Organizations transferring data are required to use "contractual or other means to provide a comparable level of protection while the information is being processed by a third party."[160] PIPEDA does not, however, require personal information to be stored in Canada, nor is there any legal prohibition in Ontario against outsourcing data processing and storage to third party providers in other jurisdictions.[161] The IPC's guidance on cloud computing security for public sector organizations states:

> One of the primary concerns with outsourcing to cloud providers is the risk that the data and/ or applications offered by the cloud provider may be physically located and housed outside of the institution's legal jurisdiction. In addition, information stored and processed with a cloud service provider may leave the jurisdiction when in transit from your institution to the cloud provider. Information transmitted or stored outside of the country or managed by a foreign owned provider could be subject to the laws of the country housing the data or that of the provider. These laws may be substantially different from Ontario laws.[162]

The IPC emphasizes that organizations are accountable for meeting legislative requirements regardless of where data resides or is processed. Further study of provincial, municipal, or private sector business requirements related to the storage, transmission, and processing of connected and autonomous vehicle data should include careful consideration of the whole handling supply chain.

Role of advanced technologies

Stakeholders and researchers have begun to explore how advanced technologies might be used to manage and secure data generated by connected and autonomous vehicles. Start-up financing for automotive technology companies surpassed $1 billion worldwide in 2016; Canadian start-ups had the second largest share.[163] Large automakers including Ford, GM, and Toyota interact with these start-ups on a daily basis at some of Ontario's autotech hubs, including in Kitchener-Waterloo, the GTHA, and Ottawa, seeking solutions for distracted driving, capturing biometrics, and wearable tech. Traditional automotive companies are also increasingly looking to partnerships or affiliations to explore emerging technologies and their applications.

---

[159] The international Comparative Legal Guide to: Data Protection 2017. (2017). Global Legal Group. https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Canada-2017.pdf
[160] When Your Data Must Stay in Canada. (2017). Server Cloud Canada. https://www.servercloudcanada.com/2017/10/privacy-law-canada/
[161] Locke, J. (2015). Canadian Privacy Laws and the Canadian Cloud: A Primer for Canadian Businesses. https://www.servercloudcanada.com/2015/09/canadian-privacy-laws-canadian-cloud-primer-canadian-businesses/
[162] Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions. (2016). Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2016/08/Thinking-About-Clouds-1.pdf
[163] Lindzon, J. (2017). For Canada's auto start-up companies, financing is all relative. Driving. http://driving.ca/auto-news/news/for-canadas-auto-startup-companies-financing-is-all-relative

One such emerging technology is blockchain. Blockchain is a "digital, decentralized, distributed ledger that provides a way for information to be recorded, shared and maintained by a community".[164] It is a way of storing data securely while providing access to all previous transactions for any user with permission. Four characteristics are critical for understanding blockchain:

- *It functions on Smart Contract logic:* smart contracts define the rules of engagement between ecosystem partners, determining control over or automatically executing transactions of data (information, currency, etc.)
- *It is based on cryptography:* entries are chained together through cryptography and, once entered, very difficult to change without detection. This allows information to be trusted by the network
- *It is distributed:* no one owner or organization holds the record of transactions or the data, meaning there is no single point of failure
- *It is fundamentally a ledger:* the same as has been used in banking for centuries, the ledger logs a double entry when transferring value or a single entry when recording a fact

The key value of blockchain is its reliability, immutability, irreversibility, transparency, and near-real time processing.[165]

The automotive sector is a strong candidate for blockchain due the following characteristics:[166]

- Consumer behaviours are changing to embrace digital, on-demand services, ride sourcing and vehicle sharing services, and electric vehicles, generating the need to share data and connect with digital infrastructure
- Mobility and logistics services will generate significant amounts of data that might be monetized for insights (e.g., car usage, experience analytics)
- Disjointed or fragmented supporting systems can result in a complex and slow vehicle purchase and delivery process
- Vehicles can be underutilized or expensive
- Regulation and new competition (e.g., open banking, peer-to-peer lending) will impact consumer expectations of automotive products

In the automotive sector, Volkswagen has announced a partnership with IOTA, a scalable, modular, decentralized platform based on distributed ledger technology, while Daimler AG recently completed a pilot project using blockchain technology to execute a financial transaction.[167] In the broader mobility ecosystem, researchers

---

[164] Accelerating Technology Disruption in the Automotive Industry: Blockchain in the automotive industry. (2018). Deloitte.
[165] Accelerating Technology Disruption in the Automotive Industry: Blockchain in the automotive industry. (2018). Deloitte.
[166] Pon, B. (2017). How Automakers Can Use Blockchain. BigChain. https://blog.bigchaindb.com/how-automakers-can-use-blockchain-adab79a6505f
[167] Munford, M. (2018). Volkswagen's Chief Digital Officer Joins Blockchain Non-Profit Iota Foundation. Forbes; Successful utilization of blockchain. (2018). Daimler. https://www.daimler.com/investors/refinancing/blockchain.html

across Ontario universities and companies in the province's key autotech clusters are investigating use cases for blockchain in cyber security and financial transactions. The Government of British Columbia is piloting a distributed ledger to manage business information shared across provincial borders.[168] The Government of Ontario-funded Ontario Centres of Excellence recently awarded funding to a blockchain technology company (Nuco) to develop a distributed ledger that integrates a person's records held across multiple siloed government agencies. The ledger would store and synchronize user data in real time across agencies, protecting the integrity and privacy of the information with smart contracts and permissioned access.[169]

Use cases might fall into three categories, with varying degrees of value and complexity/ease of implementation:[170]

- *Verification and process improvements* (e.g., provenance/trace and verify parts including cyber security components and sensors, event data recorders, etc.): A blockchain-based solution that identifies vehicles with defective parts and issues an automatic recall through lines of connectivity, improving customer safety and experience
- *Vehicle management and incentives* (e.g., dealer and customer incentives, odometer fraud, ride sourcing and on-demand mobility services): Users and providers of ride sourcing services (including connected and autonomous vehicles) could register on the blockchain and exchange information such as car key location, payment information, insurance, cost per kilometer, with users maintaining control and visibility into who accesses their data and how it is applied
- *Finance, payments and insurance* (e.g., insurance contracts, auto leasing, connected services for purchasing infotainment, connecting to in-home devices, payment services): License and credit checks, leasing agreements, and payment could all be completed and stored via the blockchain, enabling secure transaction of personal and other information while maintaining customer control and transparency.

This is a nascent area of research and development and will be monitored over the coming years as connected and autonomous technology also evolves and further use cases are identified.

Implications for Ontario: Cyber security should be an increasingly central part of private and public sector organizational strategies in Ontario, following international standards to harmonize with other jurisdictions and to set up

[168] Smart, A. (2017). B.C. experimenting with 'blockchain' to store and share crucial data. The Times Colonist.
[169] Allison, I. (2017). Blockchain technology: Nuco selected by the Ontario government for digital identity tech. International Business Times.
[170] Accelerating Technology Disruption in the Automotive Industry: Blockchain in the automotive industry. (2018). Deloitte.

security infrastructure from the start, before threats become realities. In particular, the readiness of various organizations and suitability of existing regulation to support secure storage, transmission, and processing of Ontario data should be assessed in order to capture business requirements and potential roles for advanced technologies in mitigating risks.

Areas for further research

12. The provincial government might create a space for traditional and non-traditional automotive ecosystem players to convene and engage with leading practice industries (e.g., financial services) on cyber security, with the objective of identifying lessons learned that might apply in Ontario.
13. Further study to identify capacity needs, current state gaps, and potential models to fill gaps, to be conducted in parallel with discussion on data ownership and broader data residency frameworks.
14. Further study should be conducted on how blockchain and of other advanced technologies might converge to create opportunities for connected and autonomous vehicles. Recent public sector use cases in British Columbia and Ontario demonstrate an emerging role for government in this space.

Harmonization and interoperability

The WEF's recent manifesto on the need for a seamless integrated mobility system (SIMSystem) positions interoperability (between modes of transportation and between modes and infrastructure across borders) as critical to the success of future mobility. The WEF writes: "The full realization of the SIMSystem vision includes all modes of transport and the functionality to use and deploy those modes as well as the infrastructure on which they operate, across geographies, for the movement of people and goods, globally." While the report acknowledges that the feasibility of a single global, national, or even regional SIMSystem for movement of people and goods is questionable, the organization urges mobility ecosystem players to consider how benefits for users will be enhanced the more systems can be integrated. Particularly as mobility continues to function cross-border, governments and industry may increasingly find that they need to coordinate to establish common standards and interoperability protocols in safety, security, privacy, service levels, accessibility and other key areas.

Mobility experts echoed that interoperability was critical to realizing benefits from connected and autonomous vehicles. If services and technology are introduced in silos, functioning on different systems (much like today), traffic could become worse, connected vehicles could become stranded, and the cost of manufacturing could be prohibitive as vehicles would need to connect with everything at all times.

The WEF speaks to three layers of interoperability: digital, physical, and rules (or regulations and standards; see Figure 21):[171]

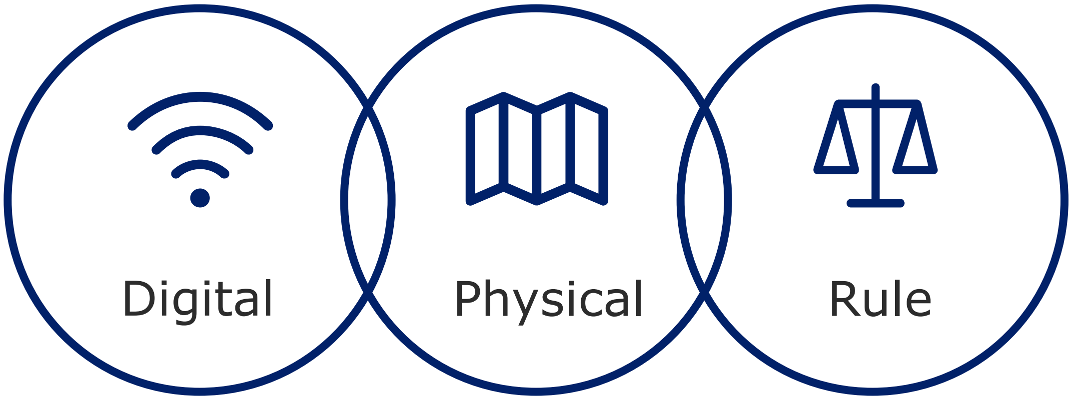


Figure 21 - The three layers of interoperability

The extent to which harmonization is feasible and desirable across these three layers may shift depending on the scale of the mobility system (i.e., cross-provincial, national, international) and the pace of transition to greater levels of autonomy and connectedness.

Digital interoperability

While there have been industry-driven movements to create uniform data structures or data layers across manufacturers, the complexity and number of sectors and industries that would need to be involved as well as the drive to stay competitive rather than partnering may mean that total digital interoperability is not feasible. According to a number of experts consulted, however, this is not a technological hurdle, but rather a challenge to build complex relationships.

In its recent report, the WEF urged the whole ecosystem of actors to "collaborate, define standards for the exchange of data, and participate in a platform that enables users to access integrated trip functionality."172 The WEF sees technological collaboration and knowledge sharing as key to establishing common priorities, accelerating technology development, and sharing information across levels of government and borders, as has been effective in other sectors (e.g., energy) such as space exploration and energy.

The WEF emphasizes that availability and standardization of data will be critical to optimizing mobility in real time, with that data available in some form for consumers and operators to access. Players across the data lifecycle will need to coordinate as information is created, captured, acquired, standardized and stored

[171] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem).
[172] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem).

in ways that are reliable and meaningful for a variety of players, and analysis will be needed to “extract meaning, gain insights and make decisions”.

Stakeholders from across industries suggested that the Ontario government might play a convenor role, creating a space for different sectors to work together for common benefit. There is evidence of this working already with the Autonomous Vehicle Innovation Network and other innovation hubs across the province. While some saw inherent conflict in public and private sector motivations (e.g., governments would like to manage congestion and enhance accessibility, the private sector would like financial gain), there might be room for common ground in sharing data and skills that benefit all actors. Some saw potential to use the visibility of developing connected and autonomous technologies to spur further investment in the overall transportation system, informed by new data that has historically been difficult to access.

Physical interoperability

The WEF also speaks to the need for physical interoperability, through energy networks, infrastructure and transport modes. If the fleet of vehicles operating in Ontario becomes increasingly electric and automated, charging and fueling across the province and potentially the country must become commonplace and standardized.[173] This might be especially important as freight or carrier vehicles become increasingly automated. Some carriers are already building connected fleets and are beginning to experiment with autonomous, electric, or shared fleets. The Ontario government committed to achieving 5% electric vehicles out of the total vehicle fleet by 2020.[174] Data will be critical to understanding the mobility patterns and ranges of these trucks, while connectedness will allow for remote routing, recharging, and diagnostics.[175]

Interoperability across infrastructure also means “physically connecting modes that might otherwise be isolated and dispersed” and plugging some of the nearly $5 billion infrastructure gap in Ontario alone.[176] Data sharing across modes may help provide infrastructure operators (e.g., different levels of government) with the ability to prioritize and proactively address infrastructure needs to support the whole system. Finally, interoperability across transport modes will allow integrated mobility, personalized to each individual passenger. The WEF encourages consideration of innovative business models to fund infrastructure

[173] Ibid.
[174] Expert analysts predict this goal will be achieved closer to 2030 or 2040. Jones, A. (2017). Ontario will miss its 2020 electric vehicle target, experts say. Toronto Star. https://www.thestar.com/business/2017/12/03/ontario-will-miss-its-2020-electric-vehicle-target-experts-say.html
[175] Choe, T., Rosenberger, S.A., Garza, M., & Woolfolk, J. (2017). The Future of Freight: How new technology and new thinking can transform how goods are moved. Deloitte. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/future-of-freight-simplifying-last-mile-logistics.html
[176] Trenton, K. (2017). AMO Report Shows Municipal Share of Provincial Deficit. https://www.myhaliburtonnow.com/21598/m-o-report-shows-local-share-provincial-infrastructure-deficit/

gaps and cross-border systems, including innovation tenders or public-private, revenue-sharing agreements.

In most government literature, technical interoperability is less explored than interoperability of rules or physical assets. Recent announcements of investments in 5G technologies are a positive step forward. Beyond the recent federal investment in ENCQOR (discussed above), Ontario has invested $63 million in the Next-generation Network Program, in partnership with the Centre of Excellence in Next Generation Networks (CENGN) and the OCE (as well as a consortium of industry, academic, and research leaders) to expand CENGN's Cloud Expansion Project, to connect 18 innovation centres across Ontario and provide advanced networking capabilities. Progress across these initiatives, required investment, and legislative barriers will need to be monitored and explored further.

Harmonization of regulation and standards

The WEF claims that connected mobility relies on having harmonized regulations, standards, protocols, and other policy elements across modes, geographies, and functionalities. While ecosystem players in Ontario thought it unlikely that such harmonization could be achieved internationally, many emphasized the value of national frameworks for data access, ownership, privacy and security as connected and autonomous vehicles evolve. This could rely on what the WEF calls a rules-based framework, taking into account leading practices from other jurisdictions and harmonizing where effective and efficient (e.g., in the case of shared borders). Private sector companies will be instrumental in informing and leading the development of national standards, particularly in areas of expertise around technology and data.[177] As one automotive supplier said: "It is important for the government to tell us what to do, but not to be prescriptive on how to do it."

"Auto-manufacturing is a global ecosystem. It would be very hard for governing bodies to decide what needs to be followed in a unanimous way."

- Automotive Industry Expert

As such, many see the need for a national policy and regulatory framework for connected and autonomous vehicles. The Council of Ministers and Deputy Ministers Responsible for Transportation and Highway Safety writes that a national framework would promote the standardization and harmonization of AV technology across the country" and encourages the federal government to also act as a facilitator for international harmonization.[178] Witnesses to the House of Commons Standing Committee on Transport, Infrastructure, and Communities stated that the federal government should act as a catalyst, "bringing together various public and private stakeholders to develop a vision for the future of Canadian communities", as well as improving R & D capacity across the country.[179] Participants from industry testified to the importance of standardization on connected and autonomous vehicle policies between provinces and with the United States to maximize clarity and minimize regulatory burden.[180]

While protection of personal information is regulated at the national level, the wealth of data being generated by CVs and AVs as well as data from the sensors interacting with vehicles (e.g., from smart roads, connected transportation systems, etc.) may require policies and regulation at the provincial and territorial level. Expert witnesses to the Senate Standing Committee on Transport and

[177] World Economic Forum. (Jan. 2018). Designing a Seamless Integrated Mobility System (SIMSystem).
[178] Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle.
[179] An Interim Report: Infrastructure and Smart Communities. (Dec. 2017). Report of the Standing Committee on Transport, Infrastructure, and Communities.
[180] Ibid.

Communications cautioned that provincial and territorial jurisdiction over connected and autonomous vehicles may lead to a “patchwork of requirements”. Given that vehicles, particularly commercial or freight, will need to function across provincial, territorial, and Canada-US borders, this was seen as an area of particular importance. Witnesses felt existing venues such as the COMT or RCC would be appropriate to continue collaboration on this point.

Automotive industry experts consulted for this report emphasized Canada’s position as a follower in terms of automotive technology innovation and regulation, while acknowledging Ontario as a leader. Decisions on data ownership and privacy as well as cyber security often follow NHTSA or the European Union, perhaps because those jurisdictions house a large number of OEMs. Many emphasized that it was positive for the government to look for industry best practices and international standards to avoid “re-inventing the wheel” and to better harmonize with other jurisdictions. For companies operating across borders, automotive experts saw most seeking to comply with the most stringent sub-national or international regulations to ensure compliance.

While European member states are working to introduce voluntary guidelines, regulation, or legislation to ensure compliance with the new GDPR, North American auto manufacturers have been less proactive.[181] Automotive industry experts and researchers suggested that without a single regulatory body or governance structure, the patchwork of legislation, regulation, and technological advancement across states and provinces did not allow for a uniform approach to harmonization.

Voluntary and regulatory approaches

As discussed above, Ontario will likely seek to learn from and complement approaches in the other jurisdictions to the protection, ownership, and security of data generated and transferred by connected and autonomous vehicles. As jurisdictions transition to greater levels of vehicle connectedness and automation and different models of ownership, different regions have taken different approaches. Several countries have developed codes of practice on data collection, protection, cyber security, and software management, taking a more voluntary approach.[182] By contrast, several Canadian privacy experts and the Privacy Commissioner of British Columbia have recommended that data protection regulations be established for the Connected Car Industry in particular, complemented by a robust national regulatory framework to address privacy concerns, including national data protection regulations, national standards for

[181] For instance, the French Data Protection Authority (CNIL) published a compliance package in 2018 to help stakeholders comply with the GDPR.
[182] Canadian Council of Motor Transport Administrators. (2016). White Paper: Automated Vehicles in Canada.

insurance, and formal adoption of Privacy by Design principles and related tools.[183]

Auto manufacturers in the US and globally have adopted a number of voluntary principles-based frameworks, including the National Highway Traffic Safety Administration's Cyber security Best Practices for Modern Vehicles and the Association of Global Automakers' Framework for Automotive Cyber security.[184,185] Cyber security Best Practices for Modern Vehicles, is intended to help protect vehicles over their lifetime and to emphasize the importance of cyber security for automotive leaders.[186] The United States Department of Transportation (DoT) released its *Automated Driving Systems 2.0: A Vision for Safety* in 2017, updating the policy released in 2016 to take a more voluntary approach. The Policy focuses on automation levels 3 to 5 and provides voluntary guidance on 12 safety elements for the design of cars. The DoT has taken a voluntary approach to regulation in order to encourage innovation and regional policymaking. To this end, they have drafted a Model State Policy for state governments to use in their AV legislation. Transport Canada and the Canadian Council of Motor Transport Administrators (CCMTA) are in the process of developing a report on guidance to support the harmonization of AV testing and deployment regiments across Canadian jurisdictions and voluntary guidelines for industry testing.[187] 21 states and Washington, D.C. have passed AV legislation related to vehicle safety and testing, with varying degrees of rigour. 11 states have introduced executive orders, typically related to the testing or study of autonomous vehicles at Level 3 and above.

The *Drivers' Privacy Protection Act* and other federal statutes, as well as state laws in 47 states and the Washington, D.C. provide various protections for personal information. According to legal experts, depending on the type of data, the way it is collected, and the entity collecting it, these protections apply more or less directly to data generated by connected and autonomous vehicles.[188]

North Dakota is notable in its autonomous vehicle legislation as it includes particular provisions related to the collection, management, and storage of data. HB 1202, enacted in 2017:

[183] The Connected Car: Who is in the driver's seat? A study on privacy and onboard vehicle telematics technology. (2015). BC Freedom of Information and Privacy Association and Office of the Privacy Commissioner of Canada.
[184] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html.
[185] See the Framework for Automotive Cyber security published in January 2016 by the Alliance of Automobile Manufacturers and the Association of Global Automakers. http://www.globalautomakers.org/OldSiteContentAssets/press-release/Automakers-Develop-Framework-for-Automotive-Cyber security-Best-Practices-assets/framework-autocyberbestpractices-14jan20161-pdf.
[186] Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2017). Securing the future of mobility. Deloitte University Press. https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cyber security-challenges-connected-car-security.html
[187] Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle.
[188] Autonomous vehicles: The legal landscape in the US and Germany. (2016). Norton Rose Fulbright.

> Requires the department of transportation to study the use of vehicles equipped with automated driving systems on the highways in this state and the data or information stored or gathered by the use of those vehicles. Also requires that the study include a review of current laws dealing with licensing, registration, insurance, data ownership and use, and inspection and how they should apply to vehicles equipped with automated driving systems.[189]

In its recommendations for Canada in preparing for the future of mobility, the Senate Standing Committee on Transport and Communications recommended that Transport Canada work with the Communications Security Establishment (CSE) and Public Safety Canada and industry stakeholders to address issues and establish a "real-time crisis connect network". Industry associations such as the Canadian Advanced Technology Alliance and the Canadian Automated Vehicle Centre for Excellence are already coordinating industry efforts that might be built on. The National Cyber Security Strategy announced in Budget 2018 (discussed in further detail below) is a significant commitment in this space from the federal government. The Standing Senate Committee also recommended that Transport Canada, the Communications Security Establishment and Public Safety Canada develop cyber security guidance based on best practices and recognized cyber security principles.

This is in line with the United Kingdom's approach, where cyber security initiatives have largely been focused on education through the National Cyber Security Strategy. Currently, the electricity sector is the only critical infrastructure sector with mandatory and enforceable cyber security standards in Ontario today.[190]

The Committee did not recommend further privacy regulation at this time as it believed further observation of the industry's evolution was required to determine whether regulation was necessary or whether guidance (e.g., a code of practice) would suffice.[191] This is in line with the approach in the US, where the Alliance for Automobile Manufacturers' seven voluntary principles for customer privacy are accepted as best practice guidance: transparency, choice, respect for context, data minimization, de-identification, and retention, data security, integrity and access, and accountability.[192]

The Committee did recommend strengthening the privacy commissioner's ability to proactively investigate and enforce the law. The Committee heard that the

[189] North Dakota Legislative Branch. Bill Versions of HB 1202. http://www.legis.nd.gov/assembly/65-2017/bill-index/bi1202.html.
[190] Statements from Minister of Energy on the 2017 Auditor General's Report. (2017). Government of Ontario. https://news.ontario.ca/mei/en/2017/12/the-industrial-conservation-initiative-cyber security-ieso-market-programs.html.
[191] Ibid.
[192] Letter to the U.S. Federal Trade Commission Re: Consumer Privacy Protection Principles for Vehicle Technologies and Services. (Nov. 12, 2014). Alliance of Automobile Manufacturers, Inc. & Association of Global Automakers. http://www.globalautomakers.org/Global-s%20and%20the%20Alliance-s%20FTC%20Letter%20Committment%20and%20Privacy%20Principles%20-2-.pdf.

Office of the Privacy Commissioner of Canada has the ability to start an investigation in response to a privacy complaint and has a number of enforcement tools at its disposal that may be applied based on the outcome of that investigation.[193] That said, the current framework does not allow proactive investigation, limiting the effectiveness of current enforcement mechanisms.[194]

Finally, the Senate Standing Committee on Transport and Communications recommended the development of a Connected Car Framework, with a focus on data protection and privacy, and continued monitoring and review of the issue. This approach will also ensure implicated industries and governments at all levels are able to remain flexible during the transition time while a mix of vehicles at different levels of automation and operating under various ownership models are on public roads.

Implications for Ontario: The Ontario government is well-situated to create a space and convene different sectors to collaborate on a rules-based framework or similar protocol for interoperability within provincial borders and with neighbouring jurisdictions (e.g., Michigan, Quebec). As the Canadian leader in this space, Ontario might also play a key role in informing a national policy framework for connected and autonomous vehicles, harmonizing approaches to the extent possible across the country and balancing regulatory rigour with flexibility as the technology evolves.

Areas for further research

15. The balance between voluntary standards and regulation in any eventual Connected and Autonomous Vehicle Framework should be carefully considered.
16. The provincial government might develop a deeper understanding of the current state of interoperability between data structures and platforms across the ecosystem in order to determine requirements for establishing digital and physical interoperability and the feasibility of such an endeavour.

Role of government

Federal

Currently, the federal government's primary role related to vehicles is safety. Transport Canada's *Transportation 2030* strategic plan includes supporting the use of connected and autonomous vehicles on public roads as a key pillar.[195]

[193] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication; Enforcement of PIPEDA. (2017). Office of the Privacy Commissioner of Canada.
[194] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[195] Transportation 2030: A strategic plan for the future of transportation in Canada. (2017). Government of Canada.

Transport Canada is also working across borders, collaborating with the United States through the Regulatory Cooperation Council (RCC), having established CV and motor vehicle safety working groups to monitor the development of CVs and AVs and to develop common standards related to key issues.

The federal government also provides funding for research and development of connected and autonomous vehicles and related technologies:

- Budget 2016 committed to providing $7.3 million over two years to increase inspection capacity and support the development a regulatory framework for emerging technologies such as automated vehicles. Budget 2017 built on this investment with $76.7 million in funding over five years for Transport Canada to “modernize” Canada’s transportation system.
- Transport Canada's Program to Advance Connectivity and Automation in the Transportation System, under the Trade and Transportation Corridors Initiative, provides $1.725 M over four years to fund research, studies and technology evaluations, the development of codes, standards, and guidance materials, and professional capacity building[196]
- Starting in 2017-18, initiatives include developing regulations for the safe adoption of CVs and AVs, working with industry and other levels of government for pilot projects, and increase the ability to establish and provide standards and certifications for industry to use new technologies.[197]
- In 2017, Transport Canada has committed $50 million in funding to update regulations for autonomous vehicles, including issues of data access, ownership, privacy, and security
- In 2018, the Government of Canada announced $400 million investment in a 5G research and testing corridor, working with the Ontario and Quebec governments and a group of industry organizations.[198]
- Transport Canada and Innovation, Science and Economic Development Canada (ISED) also co-sponsor for provincial initiatives and provide matching funding for targeted innovation initiatives.[199] The Automotive Supplier Innovation Program, Automotive Innovation Fund, Innovation Superclusters Initiative, Smart Cities Challenge, CIFAR Pan-Canadian AI Strategy, and individual NSERC and SSHRC grants also provide funding for connected and autonomous related initiatives.

---

[196] Program to Advance Connectivity and Automation in the Transportation System. (2018). Government of Canada.
[197] Growing the Middle Class. Federal Budget 2016 Tabled in the House of Commons by Hon. William Francis Morneau. ISSN 1719-7740.; Building a Strong Middle Class. Federal Budget 2017. Tabled in the House of Commons by Hon. William Francis Morneau. ISSN 1719-7740.
[198] New Canadian partnership in next-generation wireless technology. (2018). Innovation, Science and Economic Development Canada.
[199] For example, Transport Canada’s partnership with ACTIVE-AURORA and ISED’s recent partnership with the Ontario Ministry of Economic Development and Growth and Linamar, matching funding to support Linamar in manufacturing “next generation” vehicles and conducting research through its innovation centre (see: https://news.ontario.ca/medg/en/2018/01/ontario-invests-in-auto-industry-innovation.html).

Budget 2018 specifically included measures related to connected and autonomous vehicles and related data infrastructure:[200]

- *Digital Research Infrastructure:* The Government proposes $572.5 million over five years, with $52 million per year ongoing, to implement a Digital Research Infrastructure Strategy. The objective is to increase access for researchers to essential digital research tools and services – including connectivity, computing power, and storage services and advanced computing and big data resources – resources that will support the development of CVs, AVs, and related infrastructure
- *Regulatory Reform:* Budget 2018 proposes $11.5 million over three years (starting in 2018-19) for the Government to pursue a regulatory reform agenda "focused on supporting innovation and business investment" through increased transparency and efficiency. Reform will involve targeted reviews of regulatory frameworks that act as barriers to innovation, with an initial focus on agri-food and aquaculture, health/bio-sciences, and transportation and infrastructure, including emerging technologies such as autonomous vehicles
- *Cyber security:* The Government proposes $507.7 million investment over five years, and $108.8 million per year ongoing, to fund a new National Cyber Security Strategy, focusing on three goals:

  – Ensure secure and resilient Canadian systems
  – Build an innovative and adaptive cyber ecosystem
  – Support effective leadership and collaboration between different levels of Canadian government, and partners around the world

- *Intellectual Property and Innovation Growth:* The Government proposes $85.3 million over five years, with $10 million per year ongoing, in support of a new Intellectual Property (IP) Strategy, with three central initiatives:

  – To pilot a Patent Collective to increase firms' access to share IP and grow their business
  – To support the development of IP expertise and legal advice, enabling the innovation community (including those working on CV and AV technology)
  – To create an IP marketplace for facilitated licensing or sale of public sector-owned IP

Looking forward, numerous Canadian executives and academics have urged the federal government to establish a national data strategy to enable the most efficient and secure use of each dataset collected across the private and public sector. Some argue this is a precondition to the National Cyber Security Strategy

[200] Equality + Growth: A Strong Middle Class. Federal Budget 2018. Tabled in the House of Commons by Hon. William Francis Morneau. ISSN 1719-7740.

announced in Budget 2018.[201] These advocates emphasize the need for harmonization of "how we collect, store, and access data", with a national strategy offering consistency for private sector companies and mobility ecosystem users.[202]

Provincial

The Council of Ministers and Deputy Ministers Responsible for Transportation and Highway Safety (COMT) understand the primary responsibility of provincial and territorial governments as:

- Creating the legislative framework for AV testing and deployment within their own jurisdictions (incorporating federal vehicle safety requirements)
- Responsible for driver licensing, vehicle registration and insurance, rules of the road and any changes to highway infrastructure that might be needed to support AV deployment[203]

COMT highlights the importance of government as a regulator of data ownership as the transition to greater connectivity and automation occurs. They suggest engaging with regulatory bodies in other sectors (including healthcare) and jurisdictions (including the US and Mexico) to learn best practices and address gaps. The COMT also recommends governments focus on building capacity to store and process data as well as to ensure ownership rights are clear and protected as the provincial government's role shifts to that of data manager.[204]

A number of provincial and territorial initiatives are underway in Canada as governments develop and understand their role in the world of connected and autonomous vehicles.

- As policymakers and regulators:
  - Ontario is, to date, the only Canadian jurisdiction that has AV testing regulations in place and permits on-road use [205]
  - As of 2018, both Quebec and Manitoba have recently announced plans to make regulatory/legislative amendments to permit AV testing in their jurisdictions

[201] Balsillie, J. (2018). Canada needs a national data strategy. https://www.thestar.com/opinion/contributors/2018/01/30/jim-balsillie-canada-needs-a-national-data-strategy.html.
[202] Blatchford, A. (2018). Canadian CEOs and academics push Ottawa for nation big-data strategy. Globe and Mail. https://www.theglobeandmail.com/news/national/canadian-ceos-and-academics-push-ottawa-for-national-big-data-strategy/article37848737/.
[203] Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle.
[204] Ibid.
[205] O.Reg 306/15: Pilot Project – Automated Vehicles. https://www.ontario.ca/laws/regulation/150306

- The British Columbia Ministry of Transportation and Infrastructure and the Insurance Corporation of British Columbia both have Autonomous Vehicle Working Groups and are monitoring the development of CVs/AVs[206]
- The CCMTA coordinates federal, provincial and territorial matters dealing with the administration, regulation and control of motor vehicle transportation and highway safety. Their AV Working Group released a report on the future of autonomous vehicles in January 2018 and is working on developing guidelines and best practices for the deployment of AVs on public roads[207]

- As researchers/developers:

  - As discussed, Ontario has permitted a number of organizations to test automated vehicles, includingBlackBerry QNX, The University of Waterloo, The Erwin Hymer Grou p, Continental Corporation, X-Matik, Magna, and Uber[208]
  - Ontario is investing $80 million over five years to create the Autonomous Vehicle Innovation Network (AVIN) project, in partnership with the Ontario Centres of Excellence. AVIN will support industry-led R&D projects and attract and grow talent, and also includes a Central Hub that will act as a resource and focal point to conduct research, share information, build connections and raise awareness[209]
  - The Governments of Alberta and British Columbia, City of Edmonton and City of Vancouver, Transport Canada and a number of academic institutions and industry partners are sponsoring the ACTIVE-AURORA affiliated research project, consisting of four test beds and two laboratory test environments to explore the opportunities with connected vehicles.[210]

- As end users:

  - Governments may be the owners of a wealth of data as the operators of infrastructure and vehicle fleets with embedded sensors or connected to other sensors/vehicles

Municipal

Municipalities are the primary owners of intelligent infrastructure and connected transit systems within their region and make key urban planning and land use

---

[206] Driving Change: Technology and the future of the automated vehicle (Jan. 2018). Report of the Standing Senate Committee on Transport and Communication.
[207] Ibid.
[208] Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle
[209] Ontario Centres of Excellence. "How It Works". Connected Vehicle/Automated Vehicle (CVAV) Program. http://www.oce-ontario.org/programs/industry-academic-collaboration/cvav-research-program/how-it-works; Autonomous Vehicle Innovation Network Hub (https://www.avinhub.ca/)
[210] ACTIVE-AURORA Project: Wireless connected vehicle technology now testing a variety of applications. (2016). Transport Canada; Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle

decisions. They are responsible for determining land use, built form, use of public space, and other zoning through Official Plans, driving accessibility, economic development, and socioeconomic equity for citizens, regulating, training, and deploying emergency services, directing waste management services, arranging parking, governing public health, and operating transit fleets. Municipalities are also broadly responsible for "[executing] the legislative and regulatory framework created by provinces and territories, including AV safety enforcement".[211] These regions are therefore in a position to leverage new data to make more effective and efficient allocation decisions.

Municipalities have been active in monitoring technological progress and preparing for the deployment of connected and autonomous vehicles as well as participating in research and innovation. The City of Ottawa was the first Canadian city to launch testing of an autonomous vehicle on public roads, a demonstration developed through partnership with BlackBerry QNX. Ottawa hosts over 70 firms that are collectively known as the Ottawa AV Cluster, including Ford Canada's AV Research Group.[212] The AVIN demonstration zone is located in the City of Stratford.[213] The City of Toronto has partnered with local universities on research papers and has an Interdivisional Working Group to "jointly monitor technological and policy development, share information, and collaborate on cross-divisional initiatives".[214]

Municipalities are also at the centre of the "Smart Cities" movement developing across the globe. In Canada, the federal Smart Cities Challenge has spurred small, medium, and large municipalities to invest in technology that will improve security, accessibility, and liveability for residents.[215] The data generated by connected and autonomous vehicles will form one part of the influx of data received by municipalities.

Implications for Ontario: The provincial government will at once be working with federal counterparts to shape national CV/AV frameworks for data management, data ownership, cyber security, and others, while also creating the conditions for innovation within provincial borders. Other levels of government might learn from municipalities and their experiences becoming Smart Cities, including establishing partnerships, planning for data storage, transmission, and related security, and deploying technology using citizen-centred techniques to accelerate success.

[211] Future of Automated Vehicles in Canada. (Jan. 2018).
Report of the Policy and Planning Support Committee (PPSC) Working Group on Connected and Automated Vehicle
[212] Initiative on Cities and Autonomous Vehicles. Bloomberg Philanthropies, Aspen Institute. https://avsincities.bloomberg.org/
[213] Ontario Creating Opportunity with Cars of the Future (2017). Government of Ontario News Release. https://news.ontario.ca/opo/en/2017/11/ontario-creating-opportunity-with-cars-of-the-future.html.
[214] Preparing the City of Toronto for Automated Vehicles. (2018). PW26.4 Report for Action. Transportation Services. https://www.toronto.ca/legdocs/mmis/2018/pw/bgrd/backgroundfile-110665.pdf.
[215] Smart Cities Challenge. Infrastructure Canada. http://www.infrastructure.gc.ca/plan/cities-villes-eng.html.

Areas for further research

17. Research and development hubs made up of consortia of academic institutions, non-profits, research organizations, community groups and industry associations are emerging as catalysts for technological advancement and cross-sector collaboration. Mapping of these organizations, led by the provincial government or another province-wide body or association would allow a deeper understanding of the current Ontario ecosystem, including an assessment of gaps and needs to compete and lead the future of mobility.

Capacity-building

The collection, storage, management, use, disposition, and regulation of connected and autonomous vehicle data will require specific skillsets across industries, including auto manufacturers, suppliers, associated service providers, and public sector organizations. Commentary on the skills required to further develop the CV/AV ecosystem has focused on engineering and other technical skills, and current gaps related to data management have not been studied in depth.

The Information and Communications Technology Council (ICTC) has analysed the labour market changes and new skills requirements as AVs are deployed: "Our labour market will increasingly witness changes, disruptions, challenges and opportunities as AV technology becomes more developed, commonplace and accepted…the rise of this key technology will also usher in changes to our current labour market needs".[216] The organization indicates that automotive-related occupations and some auxiliary occupations such as emergency services will likely require upskilling and/or retraining while ICT jobs will be in greatest demand. The same may be true for public/city planners, transit operators, and other public sector agencies coping with new volumes and types of data. Interviewees suggested these skills will be critical in supporting connected and autonomous vehicle development and deployment.

Automotive innovation and research experts suggested that some industries may be more prepared than others. Technology companies and financial services firms, for example, likely already have the underlying skillsets and capabilities required to compete in the new data-driven environment. Public sector entities, auto manufacturers, and insurers, on the other hand, may have to shift focus from their traditionally core business to embrace new skillsets. Additionally, greater understanding from government as to the operations and constraints of

[216] Cutean, A. (2017). Autonomous Vehicles and the Future of Work in Canada. Information and Communications Technology Council.

the private sector and vice versa will be critical as further integrated transportation partnerships are formed.

The Canadian Automotive Partnership Council (CAPC) emphasizes that Canada may have an advantage as a hub for talent in key innovation research areas including strong, light-weight materials, mobile communications, sensors, software development, data analytics, artificial intelligence, cyber security, and advanced battery technology, not to mention strong investment in growing STEM education. Budget 2018 contains dedicated funding to researchers and innovators (discussed below). Auto manufacturers including Toyota Motor Manufacturing Canada and Fiat Chrysler and providers including Siemens have also made investments in building skills capacity in Ontario.[217] CAPC urges Canada and Ontario to collaborate on an inventory of national skills and R&D capabilities across the supplier community, universities and other research institutions and map these against the needs of global auto manufacturers and suppliers.[218]

Through its Memorandum of Understanding with the Government of Michigan, the Government of Ontario has committed not only to supporting technology advancement and information sharing but also to sharing best practices on workforce skills development.[219] The Workforce Intelligence Network for Southeast Michigan conducted a CV/AV skills gap analysis and found that greatest demand for workers with CAV skills was for those in IT, information security, and computer systems.[220] They recommended that employers work together to create a common set of requirements for workers in CV/AV industries, that current workers start cross-training now, and that connections between employers and the talent system of educational institutions and workforce associations be strengthened to encourage upskilling and skills matching. This will be particularly important if professions, including professional drivers and repair shop personnel, are displaced by automation. A similar analysis has not been done for Ontario but may inform research and investment in Ontario's strengths and gaps, either reflecting common areas of weakness or indicating complementary areas where Ontario might lend skills.

Implications for Ontario: A comprehensive skills inventory and gap analysis across industries (potentially led by an academic institution, the provincial government, or a neutral third party), with a focus on connected and autonomous vehicle development and deployment, could help inform Ontario's skills development strategy and CV/AV framework.

[217] Wolfe, D. & Goracinova, E. (May 1-3, 2017). Regional Resilience and Ontario's Automotive Cluster: Its Future in the Digital Age. Munk School of Global Affairs, University of Toronto.
[218] CAPC Submission on a Canada Innovation Strategy. (2016). Canadian Automotive Partnership Council.
[219] Ontario and Michigan Partner for Auto Industry Growth and Innovation. (2016). Office of the Premier.
[220] Connected and Automated Vehicles Skills Gap Analysis. (2017). Workforce Intelligence Network for Southeast Michigan.

Areas for further research

18. CV/AV industry representatives, led by either an academic institution, R&D hub or by the provincial government, might create a common set of capabilities for workers in CV/AV industries in order to inform strategies from the provincial government, industry associations, and academic institutions for cross-training and skills development.

3.0 Conclusion

This report provides an overview of considerations related to data access, ownership, privacy, and security as connected and autonomous vehicles become ubiquitous on Ontario roads and as the fleet of vehicles, both passenger and commercial, achieve new levels of automation. Across the literature as well as in speaking to experts, it is clear that this transition is in its nascent stages but very much accelerating. A number of opportunities exist for further research, as outlined: some should be pursued in the near-term to address pressing issues (e.g., safety, security) and to proactively prepare for and enable future success. Some should be explored while organizations monitor the evolution of the connected and autonomous landscape. Finally, some are long-term investments in a deeper understanding of connected and autonomous vehicle technology and its implications for Ontario.

Areas to address now to enable future success

Safety incentives during the transition (Recommendation 1): Provincial and municipal governments could work with industry, public safety organizations, and community organizations to develop policy tools specific to incentivizing safe passenger behaviour and driver responsibility as vehicles transition to Level 3 automation and above.

Opportunities to enhance accessibility and inclusion (Recommendation 5): All mobility ecosystem actors could further study the implications of connected and autonomous vehicles on accessibility and inclusion, with a focus on how data might be used to help maximize these benefits.

Establishing data needs for public interest (Recommendation 7): The provincial government could further consider the need for standards or regulation with respect to data access for specific data types that might contribute to public interest or materially help research and business development across the ecosystem and might be shared for mutual benefit.

Models for connected and autonomous vehicle data ownership (Recommendation 9): Ownership of personal and non-personal information specifically generated or transferred by connected and autonomous vehicle data has not been clearly defined. The provincial government or other body (e.g., a standards-setting organization) might convene stakeholders from other levels of government, academia, and industry to study potential models, including a rules-based framework (focused on outcomes) or definitive standards by data type.

Data ownership and residency capacity needs (Recommendation 13): Regulators and industry might conduct further study to identify capacity needs, current state gaps, and potential models to fill gaps in parallel with discussion on data ownership and broader data residency frameworks.

Requirements for interoperability (Recommendation 16): The provincial government might develop a deeper understanding of the current state of interoperability between data structures and platforms across the ecosystem in order to determine requirements for establishing interoperability and the feasibility of such an endeavour.

Mapping the Ontario ecosystem (Recommendation 17): Research and development hubs made up of consortia of academic institutions, non-profits, research organizations, community groups and industry associations are emerging as catalysts for technological advancement and cross-sector collaboration. Mapping of these organizations, led by the provincial government or another province-wide body or association would allow a deeper understanding of the current Ontario ecosystem, including an assessment of gaps and needs to compete and lead the future of mobility.

Areas to monitor over the near-term as the industry evolves

The need for data ownership regulation (Recommendation 2): The provincial government might monitor decisions made by industry players and partnerships on data ownership and access to determine whether policy or regulatory intervention is needed as use cases for data sharing and monetization become more complex and operate cross-sector. Multiple levels of government will have a significant role in decisions related to data ownership

Mapping of data needs and use cases (Recommendation 3): Academic, industry, and government actors could collaborate to develop a comprehensive taxonomy of datasets and types likely to be generated by connected and autonomous vehicles in order to identify particular data needs and determine best use for each type.

Determination of specific stakeholder data needs (Recommendation 6): As above, academic, industry, and government actors could deepen understanding of the particular data needs of each player and determine which group or partnership is best to collect, store and use different data types.

Data-sharing model pilots (Recommendation 8): Researchers, government actors, and representatives across industries could work together to pilot different data sharing models, developing a deeper knowledge of the benefits of each model for different contexts and use cases.

Exploration of anonymization and pseudonymization standards (Recommendation 10): As part of the study of ownership issues, regulators and provincial/federal governments might assess standards for anonymization and pseudonymization, use cases on risks to de-identification, and the appropriate timing and level of individual consent specific to connected and autonomous vehicles.

Cross-industry information sharing on cyber security (Recommendation 12): The provincial government might create a space for traditional and non-traditional automotive ecosystem players to convene and engage with leading practice industries (e.g., financial services) on cyber security, with the objective of identifying lessons learned that might apply in Ontario.

Balancing of voluntary and regulatory approaches (Recommendation 15): The balance between voluntary standards and regulation in any eventual Connected and Autonomous Vehicle Framework should be carefully considered.

Mobility ecosystem skills gap analysis (Recommendation 18): CV/AV industry representatives, led by either an academic institution, R&D hub or by the provincial government, might create a common set of capabilities for workers in CV/AV industries in order to inform strategies from the provincial government, industry associations, and academic institutions for cross-training and skills development.

Areas for long-term investment

Coordination between parallel innovations (Recommendation 4): Relevant provincial ministries could continue to coordinate on parallel innovations in electric, autonomous, and connected vehicles to identify areas for mutual benefit or complementary research and development.

Future state modelling (Recommendation 11): Academic and research institutions might conduct further modelling of future scenarios for ownership and consent depending on the pace and scale of transition to shared ownership or mobility subscription models.

Convergence of connected and autonomous vehicles and advanced technologies (Recommendation 14): Further study should be conducted on how blockchain and of other advanced technologies might converge to create opportunities for connected and autonomous vehicles. Recent public sector use cases in British

Columbia and Ontario demonstrate an emerging role for government in this space.

In addition to the above, all ecosystem players might consider four foundational actions to plan for the transition to fully connected and autonomous vehicles while accounting for the decades and uneven progress in between:

1. Define the organization's data needs and the channels through which access might be gained
2. Analyze and map the required skills and infrastructure to effectively capture, store, analyze, and use that data
3. Build in privacy and security as the foundation for all activity throughout the data lifecycle
4. Establish discussion and partnership across sectors to share data, knowledge, and capacity

While Ontario may not regularly see vehicles performing all driving functions (Level 4 or 5) for another thirty years, the transition has started and Ontario will need to build the foundations now to compete.

4.0 Acknowledgments

This research has attempted to take a holistic, cross industry view of the future of mobility in Ontario. In order to achieve this level of breadth and depth, the authors engaged leaders from private companies, governments and academia in a variety of disciplines to understand the implications of connected and autonomous vehicles, identify gaps in our collective knowledge, and set paths for further research. This report is the product of extensive research and a range of interviews.

Deloitte extends its sincerest gratitude to the many individuals who contributed through interviews, discussions, and review cycles. Given the breadth of areas impacted by connected and autonomous vehicles and the data generated by new mobility systems, this contribution was invaluable in developing a holistic and comprehensive perspective on the implications of connected and autonomous vehicles in Ontario.

Special thanks to Yvonne Rene de Cotret, Jelle Donga, Michael Parent, Riyaz Nathwani, Sarah Wilson, and Kurtis Sterling for leading the development of the report and well as to the Ontario government for its leadership, direction, commitment and input.