Enterprise Holdings' Submission to
Canadian Senate Standing Committee on Transport & Communication

"Data is to this century what oil was to the last one: a driver of growth and change. Flows of data have created new infrastructure, new businesses, new monopolies, new politics and – crucially – new economics. Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators. Many a battle will be fought over who should own, and benefit from, data."
Fuel of the Future, The Economist, May 6, 2017

Family-owned Enterprise Holdings – founded in 1957 – owns and operates the Enterprise Rent-A-Car, National Car Rental and Alamo Rent A Car brands.

- **FY2017 Revenue: $22.3 Billion US**
- **Global fleet: 1.9 million vehicles**
- **Total transportation service provider: car rental truck rental, retail car sales, ridesharing/vanpooling, hourly car sharing and mid-size fleet leasing and management**
- **Largest car rental company in Canada:**
  - **5,200 employees**
  - **More than 750 airport and neighbourhood locations**
  - **92,000 vehicles**
- **$3.8 Billion Annual Economic Impact in Canada:**
  - **$486 million – payroll and business related expenses**
  - **Exceeds $2.2 billion in vehicle purchases in Canada**
  - **More than $4 billion in Canadian manufactured vehicle purchases**
  - **$102 million – federal and provincial taxes**
- **More than $3.7 million donated to local charities**
- **Member of Canadian Aboriginal and Minority Supplier Council, WEConnect International and the Canadian Centre for Diversity and Inclusion**
- **Enterprise Rent-A-Car is Official Corporate Partner of the NHL**

Introduction:

Enterprise Holdings believes connected and fully autonomous vehicles will be transformative and that they are inevitable. There is much to debate about how and when fully autonomous vehicles will be significantly deployed in the market, but there is no debating that connected vehicles are already a reality. And regardless of when autonomous vehicles represent a significant portion of the transportation system, the decisions about how the connected flow of vehicle-generated data will enable them to function are being made today.

In some places around the world, those decisions are being made with the influence of government; and in some places those decisions are being dominated by the interested parties. We are here today to discuss how the competitive landscape for autonomous vehicles, their suppliers and the entire mobility ecosystem of service companies will be reduced or increased by the decisions that Government makes about who controls, and has access to, the data generated by connected, and autonomous, vehicles.

The competitive issues around data control and access have not been addressed, to any degree, by witnesses before the Committee. We believe this is a significant omission. Our brief addresses this issue, along with a few others that specifically concern the car rental industry.

The rental industry can continue to play a significant role in providing mobility options available to consumers – as long as equitable competition remains in the market. Enterprise Holdings' goal is to draw attention to some of the potential threats to competition that we believe would negatively impact mobility-related industries, including but not limited to car rental, and ultimately consumers. If steps are not taken to ensure a robust, competitive transportation – or mobility – market in the future, businesses and consumers alike will be detrimentally affected.

ENTERPRISEHOLDINGS.

The Rental Car Industry and Autonomous Vehicles:

Numerous vehicle manufacturers have declared their intent to not only build these vehicles, but to be the fleet operators providing mobility as a service directly to consumers – some even indicating they will exclusively own their autonomous vehicle fleets. As a result, much of the discussion around autonomous vehicles automatically assumes that there will be a decline of individual ownership to be replaced by fleet operators who offer mobility as a service directly to consumers.

In general, vehicle manufacturers have limited experience [and mixed track records?] in fleet management. However, existing fleet operators – and car rental companies, in particular – bring significant experience and resources to the marketplace for autonomous vehicles:

- The rental car industry purchases nearly one out of nine new vehicles sold in North America.
- The rental car industry collectively owns and operates the largest fleet of passenger vehicles in Canada.
- With thousands of locations across Canada, rental car companies are uniquely positioned with the geographic footprint to facilitate the charging, fueling, cleaning, parking, toll/citation management, and customer services issues that relate to the deployment of autonomous vehicles.
- As autonomous vehicles are deployed in the coming years, many of those vehicles will be owned and operated by rental car companies and rented to their customers.
- Convenience and affordability will drive the adoption rate of autonomous vehicles – both will depend on the logistics and economics of financing, deploying, managing, maintaining and resale of large, widely-distributed fleets.
- The first interaction many individuals will have with autonomous vehicles most likely will be through a rental. The rental industry, with millions of the newest vehicles in its fleets and a customer base accustomed to experiencing new vehicles through rentals, will provide valuable perspective as policy makers consider how to best integrate autonomous vehicles into existing fleets.
- It is critical that consumers fully understand the capabilities and limitations of autonomous vehicles. Consumer-facing organizations like rental car companies can play their part in educating the public about the use of these vehicles.
- While much attention is given to how autonomous vehicles will benefit urban areas, rural areas stand to benefit greatly from increased mobility for under-served populations such as the elderly and physically disabled. Because of the distributed footprint of our offices, rental car companies can be the channel through which autonomous vehicles penetrate the vast expanses of rural Canada.

Competition and the Future Mobility Ecosystem:

Technology is poised to dramatically alter today's transportation systems. The regulatory work underway in the areas of connected cars, data security, and autonomous vehicles will shape the entire ecosystem of future mobility options. Connectivity in vehicles, whether autonomous or not, constitutes a major opportunity regarding innovative mobility services – provided there are no unfair restrictions in place to limit access to in-vehicle data.

Because the global car rental industry operates millions of cars and trucks, it is imperative that it – as a strategic mobility stakeholder – is able to continue accessing vehicle-generated data, while also ensuring customer privacy. In-vehicle data adds value for consumers by making current and future mobility services efficient and effective, today and tomorrow.

The future mobility ecosystem offers significant downstream business development potential for all stakeholders in the automotive sector and could lead to a robust market for consumer services. However, this requires the right legal framework, enabling all players involved (vehicle manufacturers, parts suppliers, car

repairers, car rental companies, and others) to access the data generated by vehicles for appropriate, specified uses, and with appropriate permission, from users and owners, when the data is personally identifiable.

Service Providers in the Mobility Ecosystem – Today and Future

- Telematics – predictive analytics, business travel solutions, safety management
- Navigation – real-time localized traffic information, congestion mitigation
- Infotainment – access to online movies, music, shopping
- Maintenance and Repair – fleet management, remote diagnostics, vehicle recovery
- Insurance – pay-as-you-drive
- Public Services – emergency notifications, roadside assistance, eCall

The question of competition centers around who will be able to participate in this market:

- Will current service providers be able to continue to offer the services they currently offer?
- Will new, innovative business be sparked by increased opportunities to provide valuable services?

The manner in which vehicle-generated data is controlled and accessed will be the core determinant of whether competition will drive a robust mobility market or, whether alternatively, the market will become vertically integrated, with vehicle manufacturers controlling the entire scope of mobility services.

Data is critical for a wide variety of non-manufacturer participants in the transportation service market, including car rental. For example, real-time access to in-vehicle data is essential to our ability to provide safe and affordable transportation options to our customers; it will enable us to operate, maintain and repair our connected, and eventually autonomous, fleet. We currently see two main challenges to providing the most innovative connected services to our customers:

- A **danger of reduced consumer choice** due to a limited number of market players being able to access vehicle-generated data.
- An inherent **risk of abuse of dominant position by the vehicle manufacturers** if the vehicle-generated data is restricted for their sole use, or is not made accessible, in real-time, to other market players.

Lest we seem overly alarmist, we are reacting to the positions that vehicle manufacturers have already publicly taken in a submission made to the European Commission.[1]

> *"Repair and maintenance information that is made available to the vehicle manufacturers network of authorized repairers will be made available to independent aftermarket operators on non-discriminatory conditions (type, amount, and quality of data, delivery time, price). Other Service Providers will have access to a defined dataset to offer their services in accordance with the B2B agreement concluded with the vehicle manufacturers…*
>
> *Data access must occur through offboard means.*
>
> *Service providers who use vehicle data for commercial purposes shall compensate vehicle manufacturers for all costs incurred, for example, in generating the data, and in developing, operating and maintaining the access facility and, where appropriate, for the market value of the data."*

Most people assume that autonomous vehicles are about replacing current automobiles with safer and more environmentally friendly vehicles. However, sophisticated industry experts recognize that autonomous vehicles

[1] European Automobile Manufacturers Association Position Paper, Access to vehicle data for third-party service, December 2016

represent the opportunity to create a platform to collect, analyze and monetize data. Some would argue that there will be more profit in the data generated by autonomous vehicles than in the sale of the actual vehicles[2].

Direct, Real-time Access to Vehicle-generated Data is Essential to a Competitive Mobility Market:

A world of autonomous vehicles may well be one in which fewer cars are needed and those that are built may require fewer parts and service. Declining demand for vehicles and service may challenge vehicle manufacturers, and therefore vehicle manufacturers are likely to seek new and diverse revenue streams from vehicles. The car rental industry intuitively understands and supports this strategy – as long as it does not monopolize and control the flow of vehicle-generated data when, as fleet operators, we would be the owner of the vehicles.

However, if vehicle manufacturers are allowed to close down real-time, direct access to vehicle-generated data, and limit third parties' ability to interface with autonomous vehicles, the worst-case scenario could be a vertical monopoly. The reality would be that non-manufacturer participants in mobility services would be unable to compete against the same services provided directly by vehicle manufacturers who would have direct access to data.

If these conditions prevailed, auto manufacturers would have critical competitive intelligence about competitors' fleet operations. Such a scenario could lead not only to higher costs, but also fewer service options:

- Vehicle manufacturers could refuse to provide useful data needed to efficiently operate a fleet;
- They could limit the usefulness of the data by creating a lag, or removing in-vehicle access; or
- They could charge vehicle owners for the right to access the data their own vehicles generate, distorting the competitiveness of the mobility market.

Maintaining competition in the mobility service market is in the best interest of consumers, particularly in light of the expected uptake of self-driving cars. And, maintaining ownership and control of the data generated by our vehicles is critical for all mobility-related businesses to improve customer safety and to ensure proper fleet maintenance, damage repairs, and effective operation of our businesses.

For example, as the vehicle owner, a rental car company would need to:

- Locate a vehicle to determine where to deploy next;
- Identify the safety condition of the vehicles;
- Determine if the vehicle requires refueling or other maintenance;
- Seamlessly coordinate fleet logistics between vehicles from multiple manufacturers; and
- With the informed consent of the user, optimize customer experience by relying on personal information such as geolocation and driving behaviour information.

Even if consumers decide to access transportation services directly from vehicle manufacturers in the future, it would not be in their best long-term interest to regulate data in a way that makes that their only option. The complexities of the future market will necessitate Government taking steps to protect consumers.

---

[2] A good illustration of the potential value is suggested in the descriptor of a patent filing of a few years back.
Advertising-integrated car US 20150262239 A1ABSTRACT
A vehicle with an integrated advertising system. The vehicle can include a computer, at least one receiver, and a driving control. At least one receiver may be configured to communicate wirelessly, for example with an antenna or satellite. The receiver may receive advertising or retail information pertaining to a good or service, also including housing, a menu, or entertainment opportunities. The advertising or retail information may be communicated to a user within the vehicle, and the user may indicate a desire to purchase the good or service. The user may instruct the computer to drive the vehicle to the location of the good or service autonomously or the user may instruct the computer to purchase the good or service, or both.

Cyber-security:

There is nothing more important than safety and security when discussing connected and autonomous vehicles. Unfortunately, cyber-security as it relates to these vehicles is often viewed through the narrow lens of existing vehicle architecture. It is absolutely correct that today's vehicles have cyber-security vulnerabilities. What is not correct is that those vulnerabilities can be eliminated by simply shutting down access to the existing On Board Diagnostic ports (OBD II) in today's vehicles. In June of 2016, leaders from the Society of Auto Engineers (SAE) gave a presentation which included a diagram that identified more than 20 "vehicle attack surfaces" including key fobs, info-tainment systems, USB ports, and many others that are in vehicles today. That means that critical safety functions of vehicles can be accessed and controlled through those various "surfaces."

It is widely recognized that no system is "unhackable" but that robust electronic architecture which follows "safety by design" principles can provide the safest devices in our growing Internet of Things (IoT). Connected, and eventually autonomous, vehicles are one of the many machines that will be part of our future IoT.

Today's vehicles have an electronic architecture that was designed long before connectivity was contemplated. In layman's terms, most vehicles operate on a system of sensors and processors that are connected by a single communications "party line." Because of this, if an ill-intentioned party gains access anywhere, they have access everywhere – to everything, including critical safety components. The engineering principle of "safety by design" will require a vehicle architecture that ensures critical safety functionality is separated and layered into the electronic architecture, thus increasing the vehicle's defenses against hacking or even accidental disruption.

There are literally hundreds, if not thousands, of academics, technology start-ups, and long-standing automotive experts working on solutions to securing connected and autonomous vehicles. And as is the case with most technology concerns, there is no single solution that accommodates everyone's interests perfectly. What we believe is important to recognize is that there are multiple solutions; some are costly, some require a longer timeframe for implementation, and some create problematic market distortions. Three of those solutions were studied by the Transportation Research Laboratory (TRL) at the request of the European Commission. The TRL Final Report titled "Access to In-vehicle Data and Resources" was released in May of 2017 and rendered its independent evaluation of the 1.) Data Server Platform solution; 2.) In-vehicle Interface solution; and 3.) On-board Application Platform solution.

- **The Data Server Platform** solution is the solution proposed by the European Auto Manufacturer's Alliance (ACEA) which is the vehicle manufacturer's industry association in Europe and increasingly being cited by North American manufacturers as their intended path forward. It proposes to close down OBD II access for all but diagnostic purposes and have all vehicle-generated data communicated and maintained on the manufacturers' own servers. Another variation has the data hosted on an independent server. In either version, the vehicle manufacturers act as gatekeepers and allow third parties (including vehicle owners) to access the data through negotiated contracts or subscriptions, essentially monetizing the data for the vehicle manufacturers' benefit.

- **The In-vehicle Interface** solution is envisioned as a "hardened" OBD port that would require any application using data to run outside the vehicle system either on an external device or on a layer of the interface itself. The benefits here are that real-time, direct access to vehicle data is maintained in a similar manner as today.

- **The On-board Application Platform** solution would allow access to vehicle data and execution of applications inside the vehicle environment through a type of "hyper-visor" which would require any system that interfaces with the vehicle to be authenticated and approved before the "hyper-visor" would allow the interaction.

ENTERPRISEHOLDINGS.

TRL evaluated how well each of these three solutions achieves the core principles the European Commission has established. The principles are: data provision conditions and consent; fair and undistorted competition, data privacy and protection, tamper proof access, and the ability to achieve the EU's desired "data economy". ***The only solution to receive an "incompatible" rating in any category was the Data Server – Extended Vehicle proposed by the vehicle manufacturer; it was deemed incompatible with the principle of fair and undistorted competition.***[3]

Enterprise readily acknowledges the complexity, and importance, of the issue. Technology and market competitive interests ensure that public policy issues such as consumer privacy, cyber security, and competition policy interests will overlap and collide. In this regard, we recommend the Canadian Government take note of the balanced approach taken by the European Commission in its recent Communication on 'Building a European data economy' regarding data ownership of manufacturers and service providers. We share the Commission's assessment that "*a de facto control of data*" could "*be a source of differentiation and competitive advantage for manufacturers*" and that "*any future solution should foster effective access to data, taking into account, for example, possible differences in bargaining power between market players*."

Much of the debate between vehicle manufacturers and non-manufacturer transportation interests has centered on which technically viable solutions should be pursued. Unfortunately, most of the solutions offered to date do not provide optimal solutions for protecting broad consumers' interests.

For this reason, we believe the Government can play an essential role in this process.

The government has the opportunity to clearly establish principles and standards for data access, privacy and cyber-security as they each pertain to vehicle-generated data. Although this would set the bar for vehicle manufacturers, it would not stifle the innovation they can employ to achieve the standards. There has rarely been a one-size-fits-all approach to technology that yields optimal consumer protection and benefit. However, clearly establishing the principles that consumers should expect is a way for government to protect consumers and support innovation simultaneously.

Enterprise, has worked with other rental industry members, as well as numerous industry associations across North America and Europe whose members are currently part of the transportation ecosystem (and see themselves as an important contributor in the future mobility ecosystem) to draft principles for data access, data interoperability, and command and control functionality that balance the interests of consumers, vehicle owners, third-party providers, public agencies, and vehicle manufacturers. We have provided those principles and the proposed framework on the following page. We put it forward for the Committee's consideration.

[3] TRL – Access to In-Vehicle Data and Resources, Final Report, May 2017, page 12.

Connected - Autonomous Vehicles
Proposed Principles for Data, Interoperability and Control

Vehicle Owners' Rights Regarding Vehicle-Generated Data / Interoperability / Vehicle Control:
Vehicle ownership should convey the following rights of access and control for the vehicle owner, and owner's designee(s):

- Direct, real-time access to vehicle-generated data;
- A secure means of interfacing directly with the vehicle for both request and respond capabilities; and
- Authenticated, remote command and control of the vehicle (excluding in-motion control)

Vehicle-Generated Data – Control, Access and Authorized Use Cases:

- Vehicle Owner
  - Control of vehicle-generated data produced by an owned vehicle
  - Access to, and use of:
    - Aggregated and/or anonymized data of any user, for any purpose
    - Data, which may be personally attributable or identifiable, of non-owner user with appropriate notice and disclosures of use
- Non-Owner User
  - Access to, and use of, data which may be personally attributable or identifiable
  - Right to grant, or limit, access to and use of data, which may be personally attributable or identifiable, by third parties, including owner
- OEM
  - Access to, and use of, safety and performance data for authorized use cases
  - Access to, and use of, aggregated and/or anonymized data with express permission of owner
  - Access to, and use of, data which may be personally attributable or identifiable:
    - Data of owner - Requires express permission of owner, with appropriate notice and disclosure of use
    - Data of non-owner user - Requires express permission of both user and owner, with appropriate notice and disclosure of use
- Third-Party Service Provider
  - Access to, and use of, designated data according to authorized use cases and standards of use
  - Access to, and use of, aggregated and/or anonymized data subject to standards of use, and with express permission of owner
  - Access to, and use of, data which may be personally attributable or identifiable:
    - Data of owner - Requires express permission of owner, with appropriate notice and disclosure of use
    - Data of non-owner user - Requires express permission of both user and owner, with appropriate notice and disclosure of use
- Government / Public Interest Entity
  - Access to, and use of, designated data according to authorized use cases and standards of use
  - Access to, and use of, aggregated and/or anonymized data according to authorized use cases and standards of use
  - Access to personal data which may be personally attributable or identifiable:
    - Data of owner – Requires express permission of owner, with appropriate notice and disclosure of use
    - Data of non-owner user – Requires express permission of both user and owner, with appropriate notice and disclosure of use

Personally Identifiable Data Input by User (i.e., Infotainment Data) – Control, Access and Authorized Use Cases:

- Vehicle owner
  - Control of data
  - Access to, and use of, non-owner user data with express permission
- All other parties may access, and use, data with express permission from both user and owner

ENTERPRISEHOLDINGS.

Other Issues and Concerns

Cleaning Personal Information from Autonomous Vehicles:
Our customers routinely adjust vehicle settings. Owners of autonomous vehicles must have a readily accessible method of cleaning the personal information from the Autonomous vehicle, much as the car rental company today 'clean' a vehicle in preparation for the next customer. Currently, it is difficult, if not impossible, to purge a user's information from a rental vehicle without rebooting or resetting the vehicle's entire information system. We believe that we can improve safety by requiring manufacturers to equip vehicles with clear indicators that vehicles settings have been altered from factory defaults and then a process to have them easily restored. A signaling and cleaning method for personal information in autonomous vehicles with multiple users – perhaps a different user each hour – can only be developed by the manufacturers of these vehicles. This is a necessary standard to protect the privacy of the users and the safety of the vehicles. We note that this was also a recommendation of Philippa Lawson and the BC Freedom of Information & Privacy Association.

Build in Anti-Theft Technology & Tracking from the Beginning:
According to the Insurance Bureau of Canada, automobile theft, each year, auto theft costs Canadians close to $1 billion, including $542 million for insurers to fix or replace stolen vehicles, $250 million in police, health care and court system costs and millions more for correctional services. As a rental car company with operations in every province, we deal with these issues on almost a weekly basis. In addition to the loss or damage to property, the administrative efforts required of our employees on each of these cases are daunting. Vehicle theft results in higher insurance rates for law-abiding consumers; and, certainly represents upward cost pressure on the rental industry.

There is growing evidence of the involvement of organized crime, including sophisticated smuggling rings. However, our direct experience has been that auto theft is treated as a less serious crime by authorities. We have not found enforcement and prosecution efforts particularly comprehensive or aggressive. Since autonomous vehicles are a 'greenfield' area for new technologies, there is an opportunity to get this right from the start. Recognizing the ingenuity and adaptability of car thieves, we would encourage law enforcement, insurers, and vehicle manufacturers to work on a set of robust standards to create multiple ways to prevent, and, when required, track stolen vehicles.

Liability:
Federal and provincial liability statutes generally hold the driver of a motor vehicle liable for injuries and property damage caused by that driver's negligence. With autonomous vehicles, there is no "driver" per se, and thus responsibility for injuries and harm become problematic. Policymakers should consider assigning liability for accidents caused by autonomous vehicles to the entities most capable addressing design and functionality shortcomings in autonomous vehicles – in most cases, the vehicle designer or manufacturer.

Regulatory Harmonization:
As a company that deals with regulatory differences when we operate in fifty states and ten provinces in North America and other parts of the world, we can testify to the accumulated costs that they add to the operation of any business, and ultimately get passed on to consumers. Our customers cross provincial lines in their current rental cars without restrictions and likely will anticipate the ability to do the same with rented autonomous vehicles. As a result, a myriad of complex and perhaps contradictory provincial laws or regulations on technical, safety or operational standards for autonomous vehicles should be avoided wherever possible.

Continued provincial regulation of autonomous vehicles in traditional areas such as licensing, registration and insurance requirements should not pose impediments to the introduction of autonomous vehicles, but they should be standardized as much as possible. We note several witnesses before the Committee, cited the importance of harmonizing laws and regulations. In fact, it would be a surprise to us if the Committee did not endorse those recommendations and Canadian Federal and Provincial Ministers did not also support

harmonization. However, discrepancies in laws and regulations occur despite best intentions. They occur because different departments operate within their sometimes narrow mandates; some interests have more sway in some jurisdictions than others; and, in some cases, it just comes down to idiosyncratic or unintended consequences.

We believe you can reduce the incidence by having governments work from agreed 'model' legislation and regulations. You can also mitigate the impact by having officials track and regularly report on such discrepancies to the Federal and Provincial Ministers, charged with oversight on these files. We believe the tracking and reporting on any discrepancies should be public to keep the pressure on the system to make the law and regulations as frictionless as possible.

Summary of Recommendations to Senate Standing Committee on Transport & Communication

1. The car rental industry and other fleet management operators should be formally identified as key stakeholders in the development of federal and provincial policies.

2. Competition policy, particularly around the issues of data interoperability and control needs to be a more important factor in the formulation of federal policies, laws, and regulations on autonomous vehicles.

3. A principle-based approach based on fair access should be part of federal policy with the regards to the rights to access and control of vehicle-generated data by consumers, manufacturers, vehicle owners, non-owner users, third-party service providers, and government/public interest entities.

4. Vehicle manufacturers should be urged to equip vehicles with clear indicators that vehicles settings have been altered from factory defaults and provide a means to easily restore them to a default setting.

5. Auto manufacturers should work with law enforcement and insurers to create robust standards to prevent, and, when required, track stolen vehicles.

6. Liability for accidents caused by autonomous vehicles should be assigned to the entities most capable of addressing design and functionality shortcomings in autonomous vehicles – in most cases, the vehicle designer or manufacturer.

7. To support statute, regulation and policy harmonization, the provincial governments should work from model legislation and regulations.

8. Discrepancies in statute and regulation should be tracked and reported to the appropriate federal and provincial ministers. Such reports should also be made available to the public.

ENTERPRISEHOLDINGS.