THE CONNECTED CAR: WHO IS IN THE DRIVER’S SEAT?

A study on privacy and onboard vehicle telematics technology
THE CONNECTED CAR: WHO IS IN THE DRIVER’S SEAT?

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC). The views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

Published by the British Columbia Freedom of Information and Privacy Association #103-1093 West Broadway Vancouver BC V6H 1E2

604 739 9788 • fipa@vcn.bc.ca • fipa.bc.ca • @bcfipa

This work is licensed to the public through a Creative Commons Attribution NonCommercial 2.5 Canada license (CC BY-NC 2.5 CA).
For more information visit: creativecommons.org/licenses/by-nc/2.5/ca/

This report was researched and written by Philippa Lawson, with the assistance of Brenda McPhail (Usage-Based Insurance) and Eric Lawton (Privacy by Design and Tools for Compliance). Thanks to Melissa Keeshan for able research assistance in the initial months of the project. Design and production by Marianela Ramos Capelo. Special thanks to the following sites for providing royalty-free or CC photography: getrefe.com • gratisography.com • picjumbo.com • littlevisuals.co • unsplash.com
# TABLE OF CONTENTS

## 5 EXECUTIVE SUMMARY

## 7 CHAPTER 1: CONTEXT

### 8 Cars are not a luxury

### 8 Cars as Private Places

### 8 The Automobile Marketplace

#### 8 Limited Choice; Multiple Considerations

#### 9 A Proliferation of Terms, Conditions and Privacy Policies

#### 10 Automobile Industry Regulation in Canada

### 11 The Technology Imperative

#### 12 Big Data

#### 13 Internet of Things

#### 14 Contextual Awareness

#### 14 Smartphones and the App Environment

### 15 Public Mandates

#### 15 Intelligent Transportation Systems

#### 16 Vehicle-based E-911

### 16 Expressions of Concern

#### 16 Public Polling

#### 18 Statements by Public Authorities

#### 18 Industry Awareness of Privacy Concerns

## 21 CHAPTER 2: CONNECTED CAR TECHNOLOGY

### 22 Vehicle Electronics

### 24 Navigation Systems

### 24 Infotainment Systems

### 24 Approaches to Voice and Infotainment Connectivity

### 25 Automaker Telematics System Architecture

### 28 Aftermarket Telematics Systems

### 28 Wireless Communications Technologies

### 28 Cloud Computing and Data Analytics

### 29 Intelligent Transportation Systems

## 31 CHAPTER 3: CONNECTED CAR APPLICATIONS

### 32 Live Agent Assistance

#### 32 Automatic Collision Notification and Emergency Assistance

#### 32 Roadside Assistance

#### 32 Concierge Services

### 33 Remote Monitoring and Control

#### 33 Remote Vehicle Diagnostics

#### 33 Remote Software Updates

#### 33 Fleet Management

### 33 Usage-Based Insurance (“UBI”)

### 34 Automotive Financing

### 35 Car Sharing

### 35 Electric Vehicles

### 35 Convenience applications

## 36 Location-Based Services

### 37 Enhanced Navigation

### 37 Geo-fencing

### 37 Destination Finding and Local Search services

### 38 Location-based Advertising

### 38 Stolen Vehicle Recovery

## 39 Personal Connectedness and Infotainment

### 39 Hands-free Communications

### 39 Contacts and Calendars

### 39 Infotainment

### 40 Wi-Fi Hotspot

### 40 Health and Wellness Applications

## 41 Enhanced Safety

### 41 Advanced Driver Assistance Systems

### 41 Driver Monitoring

### 42 Autonomous Cars

### 42 Intelligent Transportation Systems

## 43 Taxation and Tolls

### 43 Distance-based Road Taxation

### 43 Electronic Tolling

## 43 Connected Car Applications

## 46 CHAPTER 4: THE CONNECTED CAR INDUSTRY ECOSYSTEM

### 47 The Production Layer: Automakers, the Aftermarket and Insurance Providers

#### 47 Automakers

#### 50 Aftermarket

#### 50 Insurance Companies

### 51 Intermediaries

#### 51 Automobile Dealers

#### 51 Automotive Financing Companies

#### 52 Insurance Brokers

#### 52 Car Rental Agencies and Car Sharing Providers

#### 52 Comprehensive Telematics System Providers

### 53 The Supplier Layer

#### 53 Telematics Operating System Providers

#### 54 Infotainment Platform Providers

#### 55 Mobile Telecommunications Network Operators

#### 56 Data Analytics

## 57 Third party interests

## 57 Conclusion
EXEcutiVe SuMMAry

Our vehicles are changing.

Telematics and wireless connectivity have transformed what used to be purely mechanical vehicles into electronically-controlled transportation and mobile communications devices. Vehicle performance data is now transmitted over the air to external computers where it is analyzed and used to monitor vehicle health and driver behaviour. Navigation systems allow for monitoring of vehicle location and route history. Drivers and passengers can now use on-board infotainment systems for voice and data communications, on-demand entertainment, web browsing and a growing range of convenience-related applications. Increasingly, cars are capable of recognizing individuals and customizing settings accordingly. There is no question that Connected Cars offer a growing range of services to car owners and drivers.

But what is the cost to our privacy? All of this data can be linked to the vehicle owner or registered user. The same technologies that allow for safer, more convenient and entertaining vehicles are also capable of amassing vast databases of information about drivers and analyzing that data in order to generate “actionable insights.” These insights can be used not only to improve vehicle systems and features, but also to track and profile customers for targeted marketing and other purposes. With connectivity, cars are becoming highly efficient data harvesting machines and a major element of the evolving Internet of Things. Customer data generated by the Connected Car is now seen as a major new source of revenue for automakers and their many partners. In fact there is so much competition for access to this data that some automakers are now publicly pushing back.

The data generated by telematics and vehicle infotainment systems is highly revealing of personal lifestyles, habits and preferences. In addition to customer account data and vehicle performance data, it includes driver behaviour data, biometrics and health data, location data, personal communications (voice, text, email, social networking), web browsing data, personal contacts and schedules, use of features and applications, and choice of music, radio and other streamed audio or video content. The breadth and depth of personal data that can be culled from Connected Cars is enormous and goes significantly beyond that already available via mobile devices, both in quality and in quantity.

Telematics is also now being used by automobile insurers to offer “usage-based insurance” (“UBI”) programs, under which insurance premiums are determined based on driving behaviour - where, when and how one drives. UBI is relatively new in Canada and subject to regulation at the provincial level. Current regulations require that it be offered on a voluntary basis and be used to provide discounts only (not to impose penalties), but that could change over time if UBI becomes more prevalent in the insurance marketplace.

Governments are working with the private sector to develop Intelligent Transportation Systems that involve automatic, ongoing communications between vehicles, as well as between vehicles and infrastructure, in order to alert drivers to impending dangers and reduce the number of traffic accidents. Such “Connected Vehicle” systems are also being promoted to improve traffic efficiency and lower carbon emissions. But they also involve the sharing of vast amounts of data that could, if not properly limited and secured, create an architecture of surveillance that would be ripe for exploitation by governments, corporations and cybercriminals alike if not properly protected.

Especially when tracked, combined or linked with other available data, the information generated by telematics devices can reveal intensely private details of a person’s life and is therefore highly sensitive and vulnerable to abuse. The monitoring of a person’s vehicle use, driving routes and destinations alone, for example, can reveal a great deal about that person – information that is useful not just for marketers and insurance companies but also to thieves, stalkers, and others with malicious intent. The security risks created by this unnecessary and inappropriate collection and retention of personal data is concerning, while the potential for hacking of electronic car systems that could interfere with control of the vehicle raises additional safety and security concerns.

The privacy risks are amplified in an industry ecosystem characterized by multiple players (who often play multiple roles) vying for a piece of the data pie. In order to offer infotainment services, for example, automakers must partner with telecommunications and applications providers. Key players include telecommunications and information technology giants such as Verizon, AT&T, Apple and
Google, who already have a strong position in the market for consumer data and analytics. Similarly, insurers rely upon third party telematics service providers to deliver usage-based insurance. Other aftermarket providers are also taking part in this 21st Century “data rush”, offering telematics products that can turn existing unconnected vehicles into Connected Cars.

Cars are a necessity for many if not most Canadian households. Doing without a vehicle is simply not an option for most families. But as vehicles are increasingly outfitted with telematics systems, purchasers of new vehicles have little choice in the extent to which their cars are capable of monitoring their driving behaviour and location. Laws and policies have been put in place limiting access to accident data collected by Event Data Recorders, but the same data is now being collected and transmitted wirelessly by vehicle telematics systems.

Of even greater concern is the limited choice consumers are being offered when it comes to the use and disclosure of their personal data collected by the Connected Car. Our review of several Connected Car privacy policies and terms of service indicates that the industry is violating Canadian data protection laws. In addition to lack of consent and forced agreement to unnecessary and arguably inappropriate uses such as marketing, Connected Car service providers are failing to meet the standards of Canadian law in respect of openness, accountability, individual access and limiting collection, retention, use and disclosure of customer data. Even the highly publicized “Consumer Privacy Protection Principles for Vehicle Technologies and Services” issued by automakers in November 2014 fail to meet the standards of Canadian data protection law in numerous respects.

The time for action is now, while Connected Car systems are still being designed.

Canadians are demanding that the privacy of their personal information be respected by Connected Car service providers and that they be given control over the data collected about them and their vehicles. Policy-makers have to provide the guidance that the automotive industry desperately needs on how general principles of data protection apply in their sector. Just as detailed safety standards were established for the industry and are enforced by regulation, a set of data protection standards should be developed collaboratively and enforced via regulation. This will have the beneficial effect of providing a baseline of privacy protection and clear guidance to the industry, while ensuring a level playing field for domestic manufacturers and importers alike.

**RECOMMENDATIONS:**

1. **Establish data protection regulations for the Connected Car industry.**

2. **Develop national data protection standards for usage-based insurance.**

3. **Involve privacy experts in the design stage of Intelligent Transportation Systems, including Connected Vehicle research projects.**

4. **Adopt “Privacy by Design” Principles and Related Tools**
   4a – **Establish a Privacy Management Program**
   4b – **Identify and Avoid Unintended Uses**
   4c – **Be Open and Transparent**
   4d – **Respect for User Privacy: Keep it User-Centric**
   4e – **Work with device manufacturers, OS/Platform Developers, Network Providers, Application Developers, Data Processors to integrate controls and data minimization techniques.**
“There’s plenty of people out there saying ‘Give us all the data you’ve got and we can tell you what we can do with it.’” (Ian Robertson, BMW board member for sales and marketing)
CARS ARE NOT A LUXURY

Canadians love their cars. More importantly, they depend on their cars. According to Statistics Canada’s Survey of Household Spending, 80% of Canadian households own at least one vehicle, and a further 5% lease at least one vehicle.¹ There were over 23 million on-road motor vehicle registrations in Canada in 2013, with an adult population of roughly 27 million.² In 2011, roughly 15.4 million Canadians commuted to work, and the vast majority of commuters (app.80%) used private vehicles.³

Increasing urbanization has not affected the reliance of Canadians on private vehicles; indeed, the proportion of adults who went everywhere by car actually rose together with urbanization between 1992 and 2005, likely reflecting the heavy dependence of suburban households on private automobiles.⁴ As researchers point out, access to a private motor vehicle is not only convenient but sometimes essential, especially for families with young children and those living in sparsely populated residential areas a significant distance away from shopping, work, school, meetings, medical appointments, sports activities and other community activities. Many people working in the trades and business need to stay connected in their cars and use it as an extension of their office.

Not surprisingly, Canadians spend a large proportion of their household budgets on our vehicles: 13.7% of average household expenditure goes to vehicle expenses including acquisition, maintenance and repair, fuel, and insurance. This is more than what we spend on food, non-alcoholic beverages, clothing and footwear combined.⁵ Expenses on private vehicle transportation accounts for approximately 90% of total household expenditures on transportation, and has done so based on surveys going back to 1982.⁶

For most Canadians, therefore, cars are not a luxury – they are needed for essential daily tasks.

CARS AS PRIVATE PLACES

To a large degree, cars function as an extension of our homes and in many cases, our offices. Cars provide a physical environment that envelopes the individual and offers a zone of privacy much like the home – a zone in which individuals can and do engage in intimate conversations and activities. Almost everything that we do at home, we can do in cars: talk, eat, listen to music, work, engage in transactions, watch movies, have sex, entertain our friends. The Connected Car extends that zone to include digital communications and online activities, but does not alter the fundamental nature of the car as a private space in which we engage in often intensely private activities.

THE AUTOMOBILE MARKETPLACE

Limited Choice; Multiple Considerations

There is healthy competition among carmakers and Canadian consumers have many options when it comes to purchasing a vehicle. However, automakers can afford to manufacture only a limited number of different models each year and must make decisions about what features to include in each model; they cannot customize each vehicle to the particular needs of each consumer.

At the same time, each vehicle purchaser has certain needs, priorities and budgetary constraints that limit the selection of vehicles appropriate for them. There are many factors for consumers to consider when choosing among different automakers and models: safety ratings, fuel efficiency, repair costs, reliability ratings, passenger and cargo capacity, functionality for particular uses, interior and exterior design. Connectivity and telematics features are merely one of many considerations for the automobile purchaser. In addition, consumers have limited time and ability to shop around and compare options, and are often subject to pressure from salespersons once they view or test a vehicle in person.

Given these supply-side and demand-side limitations, the reality for most consumers looking to purchase a vehicle is that their options are limited.

The number of choices among advertised features, consumers’ likely time constraints and the pressurized nature of the sales process all make it unrealistic to

---

expect the average automobile purchaser to take into account detailed terms and conditions regarding the collection, retention, use and disclosure ("processing") of their personal data. Yet, this data will be a key component in the connected car infrastructure. As the Automobile Association of America ("AAA") points out:

"Even the smoothest automobile transaction involves copious amounts of paperwork. A buyer signs 30 to 40 sets of signatures and initials on as many as 20 documents. He/she has been at the dealership for hours, is tired and is in no frame of mind to read every word about the specifics involved in the electronics of his/her automobile. Somewhere along the line, he/she is likely to sign or initial a piece of paper giving the manufacturer permission to do whatever it wants to do with the data the vehicle will transmit."

To pretend that car buyers are factoring detailed terms and conditions, let alone privacy policies, into their purchasing decisions is especially unrealistic when companies do not compete on privacy, detailed privacy policies are not provided to consumers up front prior to purchase, dealers don't know what the customer is talking about when they ask about privacy policies, and consumers are presented with non-negotiable terms and conditions of purchase that are unlikely to vary significantly among automakers. But even if these barriers were overcome, it would remain unrealistic to expect the average car purchaser to be able to review and compare the privacy policies of various carmakers, dealers and other relevant service providers, let alone to factor that into their purchasing decision (for more on this, see chapter 7).

The reality is that automobile consumers purchase vehicles that come with features they do not necessarily want and that are subject to detailed terms and conditions over which they have no choice and which they are not expected to review or treat as deal-breakers.

As a result, it cannot be reasonably suggested that automobile consumers have any meaningful say in the detailed contractual terms imposed on them with respect to the processing of their personal data by the various corporate entities in the chain of sale and ongoing service provision of connected vehicles. Greater transparency, notice and choice can improve this situation, but it is unlikely to change the fundamental reality that automakers, dealers and other retail providers of Connected Car services are the ones that set the terms when it comes to consumer privacy.

A Proliferation of Terms, Conditions and Privacy Policies

An individual purchasing a new Connected Car begins at the dealership – a completely independent entity from the automaker. She signs a contract there to purchase the vehicle. The terms of contract may include certain collection, retention, use and disclosure of her personal data by the dealer. The customer may also be required at this time to consent to the terms and conditions (including a privacy policy) of the automaker. Alternatively, the automaker may simply impose its privacy policy, along with other terms and conditions, on the new vehicle owners by virtue of their use of the vehicle.

If the customer is purchasing a Connected Car with infotainment services (e.g., OnStar, SYNC or Uconnect), she will need to register with the automaker (or its agent) for those services. In doing so, she will be required to agree to a detailed set of terms and conditions which incorporate a special privacy policy setting out how her personal data will be collected, used and disclosed by the automaker and/or its agents in the course of providing the Connected Car services.

The automaker may have a third privacy policy for optional additional services such as remote control options involving the use of the customer’s smartphone, a special key fob or other remote device.

If the customer reads the terms and conditions of her new connected service, she may discover that the automaker has partnered with a mobile network provider in order to provide the necessary connectivity for the services. She will then be referred to the privacy policy of that entity (who is not necessarily the mobile network operator she uses for her

---

7 AAA Clubs of New Jersey, “The Connected Car: It’s your vehicle, but is it your data?”, brochure giving results of 2014 public opinion polling on vehicle data, access and privacy, undated.

8 It is not known what proportion of dealerships address the issue of customer data in their dealing with customers. The website of the Canadian Automobile Dealers Association ("CADA"), http://www.cada.ca, had no privacy policy or related information when accessed on Feb.7, 2015, and the CADA Code of Ethics does not address protection of customer data. A survey of three dealerships in Whitehorse, Yukon in February 2014 found that none of them had privacy policies nor did their standard purchase agreements include any term about collection, retention, use or disclosure of the customer’s personal data.
telecommunications needs) to find out how it treats the personal information it collects about her. If the connected services operate over the customer’s existing mobile plan instead, the customer will be referred to the privacy policy of her own mobile network provider.

Assuming that the connected services involve the use of the customer’s smartphone, she will be expected to be aware of and have agreed to the privacy policies of her smartphone device system provider.

When she starts using her Connected Car and wishes to take advantage of particular applications, the customer will find that another, completely different, privacy policy applies to each third party application even though it operates through the vehicle. Depending on the automaker, any number of third party applications may be offered through the vehicle’s infotainment system.

At this point, the Connected Car consumer has been expected to read, understand, and agree to multiple different privacy policies in order to use the connected features of her vehicle, even if such policies were not brought to her attention or provided to her.

But it doesn’t end there: if she needs financing, the customer will be subject to a separate privacy policy applicable to the financing company’s processing of her information (which could involve the use of a telematics device to enforce payment). And another privacy policy will apply to her insurer’s use of her personal data, including data gathered from a telematics device if she agrees to have one installed in the vehicle for the purposes of usage-based insurance.

Because of the variety of stakeholders involved in providing Connected Car services and the unwillingness of automakers to take responsibility for the related data processing practices of their dealers, mobile network providers, third party application providers and other partners, individuals purchasing Connected Car services are expected to be aware of and agree to multiple different privacy policies, any one of which may be unacceptable to them. This is a major change from the unconnected car, where the only relevant policies were those of the automaker and the dealer. Needless to say, it raises serious questions about the appropriateness of relying on consumer consent as the basis for data protection in such an environment.

Automobile Industry Regulation in Canada

While the rules of the road are set by provinces and territories in Canada, the federal government, through Transport Canada, is responsible for safety and emissions-related standards for all vehicles manufactured and imported into Canada. The Motor Vehicle Safety Act sets out over 200 pages of detailed safety-related regulations, referred to as the Canada Motor Vehicle Safety Standards. The standards set out specific requirements for everything from seatbelts and child restraints to such things as location of controls and displays, tire selection and rims, and window glazing materials. In addition, s.18 of the Act requires that each vehicle include an owner’s manual containing the information required by the regulations, and that if the manual is provided only in electronic or optical form, it be capable of use inside the vehicle with a device installed in or supplied with the vehicle.

By setting out these regulations in copious detail, the government can ensure that a certain minimum standard of vehicle safety is being maintained in Canada. For example, rather than simply requiring that controls be visible to drivers in all driving conditions, and leaving it up to carmakers to determine how to achieve that standard, the regulations require that:

“101(10) The indicators referred to in paragraphs (9)(e) to (h), (k) and (l) and the indicator for the automatic transmission control position shall (a) be illuminated whenever the headlamps are activated; and (b) when illuminated, emit light at one of at least two levels of intensity, one of which is so low as to be barely discernible to a driver whose eyes have adapted to dark ambient road conditions.”

By establishing highly specific, detailed standards for every component of the car that has implications for driver and traffic safety, the government assures Canadians that the vehicles they purchase and the roadways they travel on are reasonably safe. There is little if any room for argument over how a given standard is to be interpreted.

In addition to fulfilling its mandate of transportation

---

9 S.C. 1993, c.16.
10 see <http://laws-lois.justice.gc.ca/eng/regulations/C.R.C.,_c._1038/index.html>
11 see <http://laws-lois.justice.gc.ca/eng/regulations/C.R.C.,_c._1038/page-16.html#h-33>
safety for all those travelling on Canadian highways, this approach recognizes that market forces cannot be relied upon to deliver an adequate and reliable level of vehicle safety for individual Canadians. It recognizes that individual Canadian consumers do not have the time or ability to compare and assess the merits of different approaches to vehicle safety when they make purchasing decisions.

Similarly, the government has seen fit to enact laws and regulations governing vehicle emissions: the *Canadian Environmental Protection Act 1999*, Division 5, governs vehicle emissions and establishes the *On-Road Vehicle and Engine Emission Regulations*, almost 50 pages of detailed regulations designed to ensure that every vehicle sold in Canada meets current standards for minimizing air pollution.

These standards have been largely harmonized with those of the US, recognizing that the auto industry operates in a relatively integrated North American market and that automobiles are driven across the border between Canada and the US on a regular basis.

In contrast, data protection standards applicable to the automobile industry in Canada are neither industry-specific nor harmonized with applicable laws and regulations in the US. Automakers, dealers and aftermarket providers selling or leasing vehicles in Canada are subject to broad-based data protection legislation for which there is no comparable legislation in the US. Except in British Columbia, Alberta and Quebec where substantially similar provincial legislation applies, the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to carmakers and other businesses in respect of all "personal information" that they collect, use or disclose in the course of commercial activities.

As set out in more detail in chapter 6, infra, PIPEDA incorporates the Canadian Standards Association Model Privacy Code as the set of data protection standards that must be met by all organizations in the course of their commercial activities. However, the CSA Code, now legal standards set out in PIPEDA and related legislation, is a set of broadly worded, general principles that were originally meant to form the basis of more detailed sector-specific standards. The automobile sector lacks a corollary set of detailed, operational guidelines for data protection akin to the safety and emissions standards referred to above.

**The Technology Imperative**

Over the past decade, computer and telecommunications technologies have continued to advance in unprecedented ways. Microprocessors, microcontrollers, sensors, short range and long range networking communications have all become far more powerful even as they get smaller and less expensive to produce.

As the technology develops, so do the potential applications of it. In a competitive market environment, there is pressure on businesses to take advantage of the technology – if not to be ahead of competitors, at least not to be left behind. This is what we refer to as "the technology imperative."

While there continue to be many publicly-funded initiatives underway to develop non-commercial applications of new technologies (the internet itself being a prime example), commercial interests are major drivers behind both the development of technology and its applications. Recognizing the importance of market forces in technological advancement, governments are generally reluctant to impose regulations that may impede innovation. As a result, there is typically a lag between the emergence of socially undesirable or indeed dangerous applications and the development of regulations to constrain them.

This is the challenge for privacy and data protection in the increasingly digital world we live in. Technology and market forces are always ahead of the law, creating challenges not just for enforcement of existing laws but also for the articulation of legal and social norms that were previously unnecessary. While governments must be careful not to stifle positive innovation through over-regulation, they must also be careful not to let technology and commercial interests determine social results. After all, a key purpose of law – and privacy law in particular – is to establish limits on both state and private sector actions in accordance with social norms.

---

sS.C. 1999, c.33.
Personal Information Protection Act, S.B.C. 2003, c.63.
Personal Information Protection Act, S.A. 2003, c.P-6.5.
An Act respecting the protection of personal information in the private sector, R.S.Q., c.P-39.1.
S.C. 2000, c.5.
As noted by one major industry player, “New technology often carries the potential for misuse and mischief, and it’s vital to address the problem before it hinders personal privacy and security, innovation or economic growth.”

Big Data

A major technological advancement underlying the development of Connected Cars is the phenomenon known as “Big Data”: the use of sophisticated computer and telecommunications technologies to gather, co-relate, analyze and make use of high volumes of data from a variety of sources, on a scale previously only imagined.

Large specialized companies and smaller niche companies have been created to capitalize on this market opportunity; they analyze vast amounts of data for a variety of clients, for a wide range of purposes, often without the knowledge or consent of data subjects.

Big Data allows organizations to combine their data (e.g., on customer behaviour) with data from other sources, public and private, to produce useful insights. The technology behind Big Data is qualitatively different from previous data analytics technology insofar as it can operate on vastly larger amounts of data, can tap data from any number of sources, public and private (including social media, for example), and can do so in real time, as the data is produced or recorded. The hallmarks of Big Data are therefore often referred to as Volume, Variety and Velocity. The emergence of Big Data has been compared, from a scientific perspective, to the invention of the microscope.

Big Data is used in the public and private sector and has proven its value in numerous applications including public health, fraud detection, cost reduction, service improvement and transportation efficiency. It is already being used in the Connected Car environment to deliver real time traffic and weather information to drivers, thereby improving traffic efficiency. It is seen by industry experts as a key element of the Connected Car ecosystem moving forward, offering the potential for significant annual savings as well as new revenue streams.

Big Data raises big privacy concerns, and these have not gone unnoticed. As Privacy International points out, the benefits of Big Data have become “a justification for amassing vast amounts of information, processing the information for multiple and often unforeseen reasons beyond what the individuals who may have shared that information intended it for, and using that information to glean intelligence about individuals, groups, and even whole societies.” The US Federal Trade Commission has expressed concerns about the use of Big Data to further marginalize low income and underserved communities.

Because of their power to identify individuals from supposedly anonymous datasets, Big Data tools threaten to undo de-identification measures that were designed to protect individual privacy while allowing for the benefits of data analytics.

At their 2014 international conference, Data Protection and Privacy Commissioners from several countries passed a Resolution on Big Data expressing concern about privacy as well as discriminatory outcomes, and calling on all parties making use of Big Data to respect fundamental principles of data protection including purpose limitation and data minimization. In their Resolution, the Commissioners noted that:

“Big Data entails a new way of looking at data, revealing information which may have been previously difficult to extract or otherwise obscured. To a large extent, Big Data involves the reuse of data. The value of the data may be linked to its ability to make predictions about future actions or events. Big Data can be perceived to challenge key privacy principles, in particular the principles of purpose limitation and data minimisation.”

Among other points, they urged parties “to exercise great care, and act in compliance with applicable data protection legislation, when sharing or publishing

---

23 <www.privacyinternational.org>
25 Please see chapter 7 for more details.
pseudonymised, or otherwise indirectly identifiable, data sets. If the data contains sufficient detail that is, may be linked to other data sets or, contains personal data, access should be limited and carefully controlled.”26

Internet of Things

Another significant technological development in recent years is the embedding of computing and communications capacity in physical infrastructure, appliances and other devices so as to make possible an “Internet of Things” that can interact with each other, exchange data and perform useful tasks without human intervention. While machine-to-machine (“M2M”) communications and related technologies have been in place for some time, they are now experiencing accelerated growth given the proliferation of affordable wireless communications. Despite a highly fragmented market and low levels of standardization, work is underway to develop security and other standards that will eventually allow the interconnection of billions of devices in order to achieve “Smart Cities” and Intelligent Transportation Systems, among other applications.

Automobiles are key components in the envisaged Internet of Things. Indeed, they are the largest and most sophisticated component of a vast network of interconnected objects, with a potential range of functions and services exceeding those of other mobile devices including the now ubiquitous smartphone. Efforts to connect vehicles could in fact lead development of the Internet of Things, especially given the strong public interest leveraging technology to improve traffic safety, efficiency, and emissions reduction. As one industry commentator noted:

“There is a common refrain heard from nearly everyone gathered in Detroit to attend the World Congress on Intelligent Transport Systems [in fall 2014]: Connected cars will be the ultimate Internet of Things. They will collect and make sense of massive amounts of data from a huge array of sources. Cars will talk to other cars, exchanging data and alerting drivers to potential collisions. They’ll talk to sensors on signs on stoplights, bus stops, even ones embedded in the roads to get traffic updates and rerouting alerts. And they’ll communicate with your house, office, and smart devices, acting as an digital assistant, gathering information you need to go about your day.”27

The privacy implications of the Internet of Things, like Big Data, have not escaped notice. In November 2013, the US Federal Trade Commission held a public workshop entitled “Internet of Things – Privacy and Security in a Connected World”, in which one of the four panels focused on privacy and security issues arising from Connected Cars.28 Further, at their 2014 conference, Data Protection and Privacy Commissioners issued a Declaration on the Internet of Things, noting that:

“Self determination is an inalienable right for all human beings. Personal development should not be defined by what business and government know about you. The proliferation of the internet of things increases the risk that this will happen.”

More specifically, the Declaration states:

“Internet of things’ sensor data is high in quantity, quality and sensitivity. This means the inferences that can be drawn are much bigger and more sensitive, and identifiability becomes more likely than not. Considering that the identifiability and protection of big data already is a major challenge, it is clear that big data derived from internet of things devices makes this challenge many times larger. Therefore, such data should be regarded and treated as personal data.”

It calls upon those who offer Internet of Things devices to:

“be clear about what data they collect, for what purposes and how long this data is retained. They should eliminate the out-of-context surprises for customers. When purchasing an internet of things device or application, proper, sufficient and understandable information should be provided. Current privacy policies do not always provide information in a clear, understandable manner. Consent on the basis of such policies can hardly be considered to be informed consent. Companies need a mind shift to ensure privacy policies are no longer primarily about protecting them from litigation.”29

26 Resolution on Big Data, 36th International Conference of Data Protection and Privacy Commissioners, accessible at <https://www.priv.gc.ca/resource/int/conf_14_e.asp>.
29 See footnote labeled “29” on the next page.
Contextual Awareness

Building on Big Data and the Internet of Things, a growing trend in data analytics for service provision and targeted marketing is “contextual awareness,” or the use of data to make inferences about an individual’s intent or state of mind and to customize services or advertising accordingly. Led by Google and Amazon, contextual targeting of advertisements based on data about the individual target has become standard in the online and mobile environments, and is becoming ever more refined through the use of new data sources such as the Connected Car.

WATERLOO COMPANY UNVEILS EXPERIMENTAL CAR THAT MONITORS YOUR BODY FOR SIGNS OF TROUBLE

Metro News (Sept. 9, 2014)
http://metronews.ca/drive/1150022/waterloo-company-unveils-experimental-car-that-monitors-your-body-for-signs-of-trouble/

... The company says insight gained from the wearable technology is then transformed into anticipated driver behaviour. For example, it says sleep patterns, glucose levels and abnormal heart rates can be used to predict driver drowsiness.

So, before a journey when these conditions are present, and after looking at the intended route and the current weather and traffic conditions, it might warn the driver to be extra cautious, to hand off the wheel to someone else, or even to stay home. This information is relayed to the driver by a tablet or screen inside the vehicle.

In a December 2013 interview with the UK-based trade journal Telematics Update, the director of developer ecosystem and application development for GM's Global Connected Consumer business unit, Steve Schwinke, noted that automakers were barely “scratching the surface” when it comes to context-aware apps. He forecast that 4G connectivity, proliferation of in-car camera technology, Big Data and wearables would all be used to personalize the “in-car app experience”.30 Indeed, some OEMs such as Mercedes-Benz are looking to be leaders in this area by offering an increasingly “predictive user experience” based on in-car cameras and sensors that recognize individuals and adjust settings and preferences accordingly. The goal, according to Johann Jungwirth, president and CEO of Mercedes-Benz Research & Development North America, is to “create a passionate relationship between customer and car, and immerse the customer in a personalized Mercedes-Benz experience that follows him from one car to another.”31

Smartphones and the App Environment

Connected Cars are operating in an already mature market for mobile communications devices, in which over 56% of Canadians now own a smartphone and 58% of Canadians connect to the internet via a mobile device.32 Apple and Google dominate the market for smartphone operating systems in Canada, with Blackberry a distant third.33 Through these mobile devices, consumers have access to a growing array of third party applications as well as applications proprietary to the device operating system. This has a number of implications for Connected Cars.

First, consumers have become accustomed to being connected while on the move and want to remain connected in the car, especially during long commutes and for work purposes. This, together with laws restricting cell phone use by drivers, has provided automakers with an opportunity for a new value-added service to drivers: hands-free connectivity. Moreover, telematics technology allows automakers to communicate directly with their car drivers through vehicle systems.

Second, there is a mature, competitive and highly creative market for mobile application development which automakers and aftermarket providers are tapping into, whether to develop their own proprietary applications or to offer popular third party applications via their platforms.

Many existing mobile applications involve the collection and use of large amounts of personal information, yet are not always clear about this with consumers: a sweep of over 1200 mobile apps by

33 In 2013, Google’s Android operating system claimed 43% market share, Apple’s iOS was at 35%, Blackberry at 19%, and Microsoft WindowsPhone at 2%; <http://o.canada.com/technology/personal-tech/android-has-43-per-cent-of-canadas-mobile-smartphone-market>.
privacy enforcement authorities across the globe in May 2014 found that many were seeking access to personal data without adequately explaining how they would use the information. This prompted Canada’s Privacy Commissioner, along with 22 other authorities, to call on app marketplaces to make it mandatory for mobile app developers to post links to privacy policies prior to download if they are going to collect any personal information.

Third, it is up to carmakers to decide not only which mobile apps to make available in their vehicles but how to do so. The extent to which carmakers integrate mobile apps - and infotainment services more generally - with their telematics services has implications for consumer privacy: the more data that can be associated with an identifiable individual, the greater the privacy risk and corollary responsibilities of data custodians.

PUBLIC MANDATES

Technology, commercial interests and expected consumer demand are not the only forces behind development of the Connected Car: public policy is also playing a role, with governments starting to mandate telematics for public safety purposes. While no Canadian jurisdictions have yet done so, it is likely that some form of safety-related telematics will be required in new vehicles, in the near future.

Intelligent Transportation Systems

At the same time as industry players are taking advantage of evolving information and communications technology to develop telematics and infotainment systems for commercial benefit, governments are working with standards bodies and industry stakeholders to develop Intelligent Transportation Systems” (“ITS”) that use telematics to allow for automatic communications among vehicles, infrastructure and pedestrians to improve traffic safety and efficiency. Vehicle-to-vehicle (“V2V”) or “Connected Vehicles” systems are a key component of ITS, focusing on surface transportation. First generation V2V systems involve the transmission of a “Basic Safety Message” (a defined set of data including speed, acceleration and position) between vehicles so as to provide warn drivers of imminent collisions. Second generation systems are expected to use vehicle sensors to trigger automatic safety-related actions.

In addition to the promise of improved road safety, V2V and, more broadly, intelligent transportation systems are touted as easing traffic congestion and lowering overall carbon emissions. By directing drivers to less congested routes, helping to eliminate unnecessary stops, and providing drivers with real-time information on traffic, weather and alternative transportation options, such systems are expected to reduce commute times, cut traffic emissions and help people make greener and more efficient transportation choices.

ITS can also be used by the state to identify and track vehicles for purposes of law enforcement. For example, Brazil is moving ahead with a mandatory electronic tag-based vehicle identification program aimed at ensuring that drivers pay vehicle registration fees and taxes, road tolls and parking fees. The system will also be used for police identification of vehicles involved in crimes or stolen or unregistered vehicles. It is expected that all vehicles will be tagged and roadside infrastructure for automatic monitoring of vehicles will be in place across the country by 2017.

Following the lead of the US, Canada launched a national ITS strategic plan in 1999 (“En Route to Intelligent Mobility”) and in 2010 released version 2.0 of the “National ITS Architecture for Canada”. This document provides a basis for stakeholders to work together on standardization of ITS technologies and ensuring interoperability of technologies used at Canada-US border crossings. There are now over 200 ITS-related projects underway across Canada, including two Connected Vehicle “test beds” at the Universities of British Columbia and Alberta. Similar Connected Vehicle research and development initiatives are underway elsewhere.

In addition to funding ITS projects such as these test beds, Transport Canada is working with the Ministries of Transportation

---

24 See <https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp>.
25 See <https://www.priv.gc.ca/media/nr-c/2014/nr-c_141210_e.asp>.
26 We contend that notice will not solve the problem - focusing on transparency alone does little more than legitimize over-collection and unnecessary uses of personal data.)
30 e.g., “The Intelligent Car Initiative” in Europe, “The Smartway Project” in Japan, and “The Connected Vehicle Initiative” in the USA.
in Ontario and Quebec to develop a “Smart Corridor” for more efficient multi-modal commercial movement of goods. The City of Toronto, Canada’s largest city, recently adopted a Congestion Management Strategy that involves ITS projects and the potential for Big Data analytics.\(^41\)

Meanwhile, the U.S. Department of Transportation (“DOT”) and National Highway Transportation Safety Administration (“NHTSA”) announced in February 2014 that it will begin taking steps to enable V2V technology in light vehicles with a view primarily toward improving traffic safety. In August 2014, the NHTSA issued an “advance notice of proposed rulemaking” in which it invited comment from the public and stakeholders on various issues, including privacy and security of V2V systems, as it works to deliver a Notice of Proposed Rulemaking by 2016. It is expected that the US will soon mandate the provision of V2V telematics technology in new vehicles. Canada is collaborating in the development of V2V systems standards for use in North America and is expected to follow suit once the NHTSA determines that a V2V system is ready for implementation.\(^42\)

These inter-vehicle communications are variously referred to as “V2V” systems, “Vehicular Communications Systems”, “VANETs” and “Connected Vehicles” among other technology-specific terms.

**Vehicle-based E-911**

While Canada has not yet required vehicle manufacturers to build emergency calling capability into cars, there is a good chance that it eventually will do so, following the lead of the European Union (EU) and Russia. The European Union has established standards for pan-European in-vehicle emergency service known as “eCall” that will detect collisions and automatically call public emergency services, providing GPS-based location of the vehicle, time of the accident, direction of driving, number of occupants and vehicle identification number. Manual emergency calling must also be facilitated. All cars must be equipped with eCall compliant technology by October 1, 2017.\(^43\) Russia has moved forward with a similar initiative, referred to as “ERA-GLONASS”, under which all new passenger vehicles as of January 2015 must be equipped with a special device that can detect collisions and call emergency services automatically, relaying the location, speed and other vehicle information.\(^44\)

While the EU and Russian mandatory vehicle emergency call regimes are broadly similar in terms of the service provided, they differ markedly when it comes to the collection, retention, use and disclosure of data collected by the system. The EU has designed its eCall system with privacy as a key principle: the system does not collect data unless triggered by an accident, only a minimal defined set of data is sent to emergency services, and the data is neither retained nor used for secondary purposes. In contrast, the Russian approach (as of September 2014) was to collect, store and make the data available for analysis and use by other state bodies (including state insurance agencies), local governments, vehicle owners, and others.

**EXPRESSIONS OF CONCERN**

**Public Polling**

Annual polling conducted on behalf of the Office of the Privacy Commissioner of Canada (“OPCC”) shows consistently high levels of concern among Canadians about privacy, with over a third saying they are extremely concerned about personal privacy (up from 25% in 2012). Over half (56%) think they do not have enough information to understand how new technologies are affecting their personal privacy. Of particular relevance to Connected Cars are the high levels of concern expressed about mobile devices, with three-quarters of mobile device users worried about what might happen to the personal information stored on the device if it is lost or stolen. Location privacy is a particular concern, with 58% saying they had (at some point) turned off the location tracking feature on their mobile device (up from 38% in 2012).\(^45\)

There has been little polling of Canadians on the data collection, use and disclosure entailed with the delivery of automotive telematics and infotainment services. However, the 2014 OPCC poll did ask

---

\(^41\) City of Toronto Council meeting, October 28, 2013. See http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2013.PW2712

\(^42\) Interview with Ryan Klomp, Manager and Senior Advisor, Environmental Initiatives, Environmental amd Transportation Programs, Transport Canada, Jan.26, 2015.


one question about insurance telematics: 75% of respondents expressed concern (38% strong concern) about the risks to their personal privacy from “black boxes used by auto insurance companies to record your driving habits for the purpose of setting the cost of your insurance”.

A more extensive survey of Canadians about their awareness of and attitudes towards usage-based auto insurance was conducted by Kanetix Ltd. in 2014, using LegerWeb’s online survey tool: 75% of the 1555 respondents said they were concerned that their personal information could be stolen, and 73% were afraid that the collected information might be used to deny an accident claim or cancel their policy. The survey also indicates that seven out of 10 Canadians worry about who owns the information, or whether that information might be shared with other insurers. And about 60% were concerned that the telematics device would capture too much, and might report accidents that the driver does not want to claim.46

A very recent (March 2015) poll conducted for the Canadian Automobile Association found that nationally about 37% of respondents would agree to monitoring in exchange for an insurance discount, while 53% would not.47

The CAA poll also asked questions about Connected Cars generally. When asked who should control access to data collected by Connected Cars, 82% said consumers should have exclusive rights. Only 4% thought automakers should. Comparing the privacy risks versus the benefits of the new technology, 28% said they thought benefits outweighed the privacy risks, while 50% thought these technologies put their privacy at risk while offering little benefit to consumers. On the question of whether car makers should be required to design technology that would mean consumers wouldn’t have to choose between the benefits of technology and protecting privacy, 74% of respondents agreed, 37% strongly.

Polls of consumers in other western countries consistently show significant consumer concern about privacy in the context of Connected Cars.

Respondents to a 2014 industry-funded survey of over 5,000 adult drivers in the US, UK, Spain, Germany and Brazil in January 2014 were generally, and in some cases overwhelmingly, reluctant to trade various kinds of personal information gathered by telematics and infotainment systems for benefits such as “special offers”, reduced insurance costs and competitive bids from repair shops. Close to a third of respondents agreed with the statement “My car is a private space. I wouldn’t be willing to share any information.”48

Another 2014 international consumer survey of new car buyers found high levels of concern about data privacy in the context of Connected Cars: 51% of German and 45% of American respondents agreed, some strongly, with the statement “I am reluctant to use car-related connected services because I want to keep my privacy.” Similar proportions (59% in Germany, 43% in the US) expressed concern about hacking of connected cars via the internet.49

An online poll of readers of a story posted in August 2014 on the autoblog.com website asked “Are you concerned about privacy/data security in your car?” Of the 551 respondents, 58% were “very concerned”, 25% were “somewhat concerned”, and only 15% were “not very concerned”.50

Also in 2014, the Automobile Association of America (“AAA”) conducted a poll of New Jersey motorists about “Vehicle Data, Access & Privacy”. Over half of respondents said that motor vehicles generating information about how, when and where they drive – as well as having the ability to store emails, text messages, phone numbers and navigational searches – would cause them to be “very concerned”, with two-thirds saying they would be at least “concerned”. Particularly high levels of concern were expressed about automakers having access to texts, emails, telephone numbers called, when and where your car is driven, and smartphone use. The vast majority of those surveyed agree that “consumers should always be able to decide if information generated by their car can be shared and with whom.”51

---

47 www.caa.ca/telematics
48 Telefonica, Connected Car Industry Report 2104, p.28.
Statements by Public Authorities

Public concern about the impact on individual privacy of vastly increasing data gathering and analytics in the private and public sectors is reflected in numerous news and journal articles, legislative initiatives and statements made by public authorities. As noted above, Data Protection Commissioners from around the world have expressed great concern about the privacy implications of Big Data and the Internet of Things, generally. These concerns apply, a fortiori, to Connected Cars.

In October 2014, German Federal and State Data Protection Authorities issued a Resolution on Connected Cars, calling on automobile manufacturers, distributors, retailers, repair shops and other Connected Car service providers to ensure the informational self-determination of drivers by:

1. Observing the principles of “Privacy by Design” and “Privacy by Default” in the development of new vehicles and services;
2. Observing the principles of data avoidance and data minimization, deleting data when no longer needed;
3. Ensuring that data subjects (e.g., drivers and owners) are able to recognize, control and stop transfers of personal data to service providers;
4. Establishing privacy-friendly system settings that provide data subjects with choices regarding processing of their data, including the ability to delete; and
5. Ensuring data security via appropriate technical and organizational measures, particularly with respect to data communications from cars.

In the U.S., privacy issues arising from Event Data Recorders and in-car location-based services have been a focus of legislative attention in recent years (see next Chapter for more on U.S. legislative initiatives).

In 2013, the U.S. Government Accountability Office (“GAO”) conducted a study of industry practices with respect to location data that it had been asked to conduct by a U.S. Senate Committee. The GAO found that:

• Company disclosures explaining why they collect location data are so broadly worded as to be unclear
• Customers were not given the option of deleting their data,
• There was significant variation in methods used to de-identify customer data,
• There was significant variation in the length of time personal data was retained, and that
• Companies did not disclose how they hold themselves and their employees accountable for compliance with their own privacy policies.

In December 2013, U.S. Senator Edward Markey sent letters to 20 automakers expressing concern about the potential for both hacking and corporate surveillance of Connected Cars, and asking a set of detailed questions about the carmakers’ policies and practices. His scathing report, “Tracking & Hacking: Security & Privacy Gaps put American Drivers at Risk”, released in February 2015, identifies serious deficiencies in both security and driver privacy measures, finding among other things that:

“Manufacturers use personal vehicle data in various ways, often vaguely to ‘improve the customer experience’ and usually involving third parties, and retention policies - how long they store information about drivers - vary considerably between manufacturers.”

“Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features such as navigation.”

Industry Awareness of Privacy Concerns

Automakers are well aware of the privacy risks they face moving forward with Connected Car systems. In 2011, GM was taken to task for attempting to change the OnStar terms and conditions to allow it to use and share customer data even after the customer’s OnStar

---

53 GAO, In-Car Location-Based Services: Companies are taking steps to protect privacy, but some risks may not be clear to consumers, GAO-14-81, December 2013.
subscription had ended. Only after a New York senator asked the FTC to investigate the matter did GM back down.  

After a Ford VP’s public statements in January 2014 (about the extent of personal data now available to Ford) raised eyebrows, the company quickly reacted by reassuring the public that Ford does not actually engage in individual customer monitoring. The following week, Ford’s CEO called for privacy legislation to protect drivers’ privacy needs. Later that year, Ford created a new position for a Global Privacy Policy Attorney to work with its already established legal group, implicitly acknowledging the need to pay more attention to privacy issues.

One year later, at the Detroit auto show in January 2015, BMW publicly expressed concerns about the pressure it and other automakers are facing from technology and advertising companies to surrender data gathered, or capable of being gathered, by telematics systems. According to Ian Robertson, BMW’s board member for sales and marketing:

“There’s plenty of people out there saying ‘Give us all the data you’ve got and we can tell you what we can do with it.’ And we’re saying ‘No thank you…’ Several companies have said, ‘We’d like to know that data because then we will know whether it’s an adult or a child sitting in the car. If you also tell us how long the engine’s been running, then we know…from the navigation system, they’re about to pass a McDonald’s, the car’s been running for three hours, and the child’s probably hungry.’”

BMW claims to have put a firewall in place between to protect its vehicle telematics data from unauthorized access. Other automakers appear to be making similar design decisions for customer privacy as well as corporate security and proprietary commercial reasons. According to an Audi executive, “We are separating the vehicle-related functions from the infotainment features, thereby securing the data against unauthorized access. The customer has to give express consent for the use of data generated in the vehicle.”

But not all industry players appear to appreciate fully the privacy issues arising from Connected Cars. In its 2013 report on Connected Cars, the organization representing mobile operators worldwide, GSMA, listed various categories of Connected Car services and rated the importance of various considerations including privacy with respect to choice of cellular network technologies, for each service. While treated as “important” for various telematics services (e.g., insurance, fleet management, remote diagnostics, breakdown services) and for “multimedia, internet services and more”, privacy was considered to be “very important” only for “payment/ticketing”, and was not treated as even “important” for navigation services, travel and traffic assistance, remote control of vehicle environment, or on-demand radio, video or other content.

This failure to appreciate privacy issues is surprising as privacy is not a new issue for the telematics industry: as early as 2008, key players recognized the privacy issues created by telematics systems that not only track where people go, how fast they are driving and what emails they just received, but can also shut off engines and lock doors remotely. Erik Goldman, then President of Hughes Telematics (now Group President, Verizon Telematics, after Verizon’s acquisition of Hughes), is quoted as saying at that time: “We are hyper-sensitive to the privacy issue. The car owner owns the information gathered by the system, and the owner controls access to that info.” Although Mr. Goldman’s sensitivity to privacy issues no doubt remains, it is unclear whether he would stick to his statement about the car owner owning vehicle data.

Also of relevance to Connected Car privacy is that, in 2008, according to the article, “any aspect of the [Hughes telematics] system can be turned off or opted out by the user.” If this was true at that time, it no longer appears to be the case. Car users typically have few options to disable discrete aspects of the telematics system in their vehicles. More often than not, the telematics service is an “all or nothing” proposition: with minor exceptions (such as receiving marketing offers or permitting disclosure to third parties for marketing purposes), if you don’t want your data to be collected or used in the way that the company’s policy permits, your only option is to disable the entire system.

58 “BMW sounds alarm over tech companies seeking connected car data”, irishtimes.com, Jan.14, 2015.
“Within the automotive industry, times are changing. Data is the new horsepower and connectivity is the new chassis.”  

In order to understand the privacy implications of Connected Cars, one needs to understand the underlying technology. This chapter provides an overview of the relevant technologies used to provide telematics and infotainment services in automobiles.

Telematics and other Connected Car services are delivered using a combination of technologies including on-board vehicle electronics, global positioning system (“GPS”) satellite communications, short-range and wide-range wireless telecommunications systems, data analytics, cloud computing and the internet.

Because of the lack of standardization in both vehicle electronics and connectivity, telematics systems vary. Indeed, the sheer variety of components, platforms, formats and systems, while allowing for product differentiation, is a major challenge facing all parties involved in the telematics landscape. Each manufacturer has many options and there are significant variations among components and systems. There are a number of common elements, however, so it is possible to describe a representative automaker system which we have set out below.

---

1 Jack Palmer, Project Director, Telematics Update
(email news, Nov.5/14)
Vehicle Electronics

Almost every component of today’s vehicles has an electronic aspect – indeed, it is not an exaggeration to say that modern cars are, effectively, computers on wheels. Sensors throughout the vehicle measure such things as speed, acceleration, braking, orientation, steering angle, and wheel rotation, constantly capturing and communicating information about vehicle operation. Microprocessing modules known as electronic control units (“ECUs”) form the core of the system. Each ECU controls a specific set of functions – e.g., engine (the largest), transmission, automatic braking, air bags, power windows, air conditioning, etc. Individually programmed to respond to specific packets of data within specific parameters, each ECU gathers data from sensors and, based on that data, sends instructions to actuators that perform particular vehicle operations. Sensors, ECUs and actuators constantly exchange data in order to make the vehicle operate as designed. Modern vehicles contain as many as 70 ECUs, thousands of data points, and millions of lines of software code, reflecting the growing number of electronic vehicle operations. A special ECU, the Telematics Control Unit (“TCU”), typically provides the platform for the delivery of telematics services. Details on the TCU are provided below.

This modular communications network is referred to as a “bus.” There can be more than one “bus” network in a given vehicle. For example, Volkswagen has separate networks for drive train, climate control, and infotainment, reflecting different needs in terms of speed and bandwidth. Data generated and communicated via the vehicle bus system(s) covers virtually all aspects of vehicle operation including engine temperature, engine RPM, throttle position, vehicle speed and orientation, distance travelled, fuel levels and consumption, door open/close, tire pressure, ignition, headlights/tail-lights, battery status, cumulative idling, odometer, trip distance, braking activity, and much more. With the addition of GPS modules, the vehicle bus data also includes vehicle location information. ECUs communicate with each other using a standard protocol, of which there are several. The protocol most commonly used in light vehicle applications is the Controller Area Network or “CAN” standard. The CAN bus standard operates without a host computer; instead, each ECU (a miniature computer itself) communicates with other ECUs as necessary over the CAN bus. There is no central hub in the CAN bus system; there is just a constant flow of data signals among sensors, actuators and ECUs within the vehicle, ensuring that several ECUs are able to process data from a given sensor and control their actuators accordingly.

Prior to telematics, there was no storage of data within the CAN bus system other than via Event Data Recorders (“EDRs”), which store a limited amount of data and only during the seconds preceding and during a vehicle crash. However, TCUs or separate GPS modules now typically store a limited amount of data (e.g., maps, routes, contacts, phone numbers) in order to deliver navigation and other telematics services.

The system of electronic communications within each vehicle, while generally similar, varies by manufacturer and is invariably treated as proprietary: automakers apply strong technical security measures to prevent unauthorized access to their vehicle networks, and assert intellectual property rights to telematics software and the data it generates. There is, however, one exception to this rule: vehicle data made available via the On-Board Diagnostic port.

All vehicles now include an On Board Diagnostic (“OBD”) port, a standardized hardware interface located within two feet of the steering wheel, typically

---


4 See http://en.wikipedia.org/wiki/CAN_bus
**EVENT DATA RECORDERS**

Event Data Recorders ("EDRs") predate modern telematics. It is estimated that 96% of recent model cars are now equipped with EDR capability and the U.S. National Highway Transportation Safety Administration ("NHTSA") has proposed that they be made mandatory on all light passenger vehicles.\(^5\) EDRs are triggered by deployment of airbags or other safety restraint systems and record certain information in the seconds before and during a crash. This information is stored in the device and cannot be accessed other than directly by someone with physical access to the vehicle. EDRs collect crash-related data such as vehicle speed, engine throttle, brake activation, crash forces, air bag deployment and seat belt use. Unlike "black boxes" used in airplanes, EDRs in automobiles do not record audio, video or location information. EDR data is used to assess the effectiveness of safety systems as well as to reconstruct accident scenarios (e.g., in litigation).

In response to public concern about driver privacy and the potential for unintended uses of EDR data, several US states have enacted laws restricting access to EDRs. Most such laws require that data collected from an EDR cannot be downloaded without consent of the vehicle owner.\(^6\) This is the approach taken by Canadian OEMs as well.

---

**M2M CONNECTIVITY**

Telematics is a form of machine-to-machine ("M2M") communication: the flow of data between network connected devices, without the need for human interaction. "The basic M2M operation is that remote sensors gather data and send it (wirelessly or wired) to a network, where it gets routed, through the Internet or cellular network, to a centralized server. On the server, the data gets analyzed and acted upon according to specific software in place. Data collected could include device identity, location, status, condition and so on. Data could be uni-directional or bi-directional. The transactions are primarily useful for improved decision making, better business processes and enhanced operational efficiencies. The scope is far reaching because it is not only about smart devices having an IP address but being able to link even passive objects on the network." Source: TATA Consultancy Services, "Technology Review and Trends in M2M Communication", White Paper, undated.

---

internal networks can now be sent via the TCU over the air to off-board computers where it can be stored, processed, and converted into usable information. It can then be employed for all kinds of purposes including enhanced safety, remote monitoring, customer relationship management and a host of other applications (see next chapter).

Wireless transmission of vehicle data makes it readily and constantly available to the automaker. OEMs continue to treat much, if not most, of the vehicle data as proprietary, blocking access to it with strong security measures and assertions of legal rights. Car owners and independent repair technicians therefore remain unable (without hacking) to access telematics data that they cannot access via the OBD-II port. They can however now use wireless communications technology to collect non-proprietary vehicle data over the air via aftermarket telematics devices (“dongles”) attached to the OBD-II port.

Navigation Systems

Most of today’s Connected Cars include a navigation system, whether built-in or brought-in. Built-in navigation systems may be stand-alone (i.e., based on their own control unit) or integrated with the telematics system. Regardless, they require a GPS antenna, a computer processor and a user display. The antenna receives signals from the GPS satellites orbiting around earth, and the computer uses these signals to determine the vehicle’s location to within a few meters, displaying it on a digital screen that is embedded in or mounted on the dashboard (also referred to as the “head unit”). Using this constantly updated information on vehicle location, together with digital maps stored in the system, the computer calculates the vehicle’s route, and compares the calculated route with the vehicle’s current location throughout the journey. Built-in systems may also use data from wheel speed and/or other sensors in the vehicle to enhance route calculation, in which case they must be linked to the vehicle bus.

Vehicle-based navigation systems increasingly incorporate external traffic, weather and road condition data from various sources in order to detect problems ahead and suggest alternative routes. They can also access information on local businesses and points of interest, allowing drivers to search using the vehicle system. Past routes can usually be stored in the system and retrieved later.

Infotainment Systems

Infotainment systems, like navigation systems, can be stand-alone or integrated with the vehicle bus in order to make use of location data or other vehicle data. Either way, they typically involve their own operating systems to organize and manage their many functions and features. These include a dashboard interface, a system for connecting the vehicle to the internet so as to enable various private and/or public cloud-based services and applications, and voice recognition systems that allow drivers to engage in hands-free communications and operation of the infotainment system.

Once “paired” with the car’s internal system, the user’s phone connects with the car system each time it enters the vehicle. Calls can then be automatically transferred between the phone and the vehicle seamlessly, downloading or uploading preferences, contacts, calendar data and other content from the phone. Voice commands can be used to make calls, play music, and operate the system in other ways.9

Finally, modern cars are increasingly equipped with interior microphones and video cameras for hands-free communication as well as monitoring purposes.10

Approaches to Voice and Infotainment Connectivity

In order to transfer data wirelessly, a modem is required to modulate and demodulate signals. For voice and other human-generated wireless communications, a Subscriber Identity Module (“SIM”) is required to authenticate and authorize the end-user. Each SIM has a unique serial number, international mobile subscriber identity and authentication codes.11 SIM cards also hold the subscriber’s phone contacts and network-specific data, and can be programmed to display custom menus on the user’s device.

---

10 Remotely controlled interior cameras are also available via the aftermarket: www.brickhousesecurity.com/category/video+surveillance+security+cameras/car+cameras.do
EMBEDDED SIM CARDS

Until recently, SIM cards could not be remotely programmed; they had to be manually swapped and updated in order to switch carriers, e.g., when the customer travelled to a different geographic region. However, in late 2013 the GSMA issued an “Embedded SIM Specification” standard that allows for the remote provisioning and management of network operator subscriptions. This facilitates embedded connectivity in vehicles, by allowing carmakers (or vehicle owners, if the carrier’s contract is with the owner) to change carriers over the life of a connected vehicle without having to physically replace the SIM card.

There are three broad approaches to connecting cars to mobile networks for the purpose of infotainment and voice communications, each involving different levels of reliance on smartphones or other connected devices that can be brought in to the vehicle. In all cases, the vehicle dashboard provides the interface (typically, a computer screen) for users to access content and to communicate while driving. The three approaches are not mutually exclusive and most automakers use more than one approach, depending on the application.

• Under the embedded approach, both connectivity (SIM card and modem) and intelligence are built into the vehicle without the need for other devices. Mobile devices may be used to monitor or control the vehicle environment remotely. All data is transmitted via the OEM. This approach is typically used for vehicle-centric applications and services such as emergency assistance that require high reliability and availability. GM’s OnStar service is an example of a largely embedded approach.

• Integrated solutions rely upon the owner’s mobile device for both connectivity and intelligence and are not connected to the vehicle CAN bus. All that the vehicle provides is the port into which the phone or device is plugged and an interface screen that mirrors the owner’s smartphone interface. Integrated solutions are typically used for high bandwidth and personalized applications such as voice and on-demand music, video and social networking. They require a simpler TCU and eliminate the need for the OEM to manage mobile network operator subscriptions. Toyota’s “EnTune” service and Jaguar/LandRover’s “InControl Apps” service are examples of this approach, under which all data can remain in the owner’s device.

• Under hybrid approaches, connectivity is provided through an external modem and/or SIM card (via smartphone or other device), while intelligence is embedded in the vehicle. Hybrid approaches make sense for connected navigation and internet-based infotainment, where reliability is not critical. Ford SYNC’s system is an example of this approach.

One global carmaker CEO was quoted as saying, “soon you will not be able to make money anymore with cars that don’t integrate customers’ smartphones.” On the other hand, embedding connectivity in the vehicle is more reliable than depending on the user’s smartphone. In practice, automakers are taking a mix of approaches depending on the type of service or application in question.

Automaker Telematics System Architecture

Although OEM telematics systems can be designed in many different ways, a typical design includes the following key components:

• A Telematics Control Unit (“TCU”) located in the vehicle and connected to the vehicle bus;
• A GPS receiver that is attached to or forms part of the TCU;
• A network operations hub (“Telematics Operations Centre”), located outside the vehicle, where data from the TCU is processed, other data is gathered, and telematics services are delivered;
• A wireless communications system over which data and voice communications are exchanged between the TCU and the network operations centre;
• A call centre where customer service representatives can communicate with vehicle occupants; and
• Service and content providers who provide information, entertainment, and other services (e.g., traffic feeds, music, video, on-demand streaming of data) to the network operations hub for use in various telematics and infotainment applications.

14 Ernst & Young, The quest for Telematics 4.0: Creating sustainable value propositions supporting car-web integration, 07 Jan 2013, Executive Summary, p.1.
*This model represents a typical system. Not all OEM telematics systems are the same.
Telematics Control Units
A special ECU is now commonly installed in vehicles to control the operation of telematics systems. Telematics Control Units (“TCUs”) control such applications as remote vehicle diagnostics, remote operations (e.g., start/stop, door lock/unlock) and alerts, automatic crash notification, emergency calling, vehicle locating and monitoring, and geo-fencing. Like other ECUs, TCUs monitor data flowing throughout the bus system; they gather, interpret and disperse it as necessary to operate telematics functions.

Unlike other ECUs, however, TCUs include (or are linked to) GPS receivers that calculate and provide precise vehicle location and timing information to the TCU. They can be designed to store location data as necessary for delivery of the service – e.g., during periods during which satellite communications are lost.

TCUs are further distinct in that they include a wireless interface module that allows for the communication of vehicle data and voice communications to and from points outside the vehicle – typically to and from a central computer system (e.g., “Telematics Operations Centre”) from where the telematics system is managed. The TCU’s wireless interface allows for two-way communications between occupants and the system’s call centre, as well as for the delivery of on-demand and interactive infotainment services. It can further act as a data modem for other devices in the car. TCUs can provide connectivity for telematics and infotainment applications whether they are delivered via applications embedded in the vehicle or accessed from a smartphone or desktop.15

TCUs can also house the software interface required for hands-free communications and operation of in-vehicle features by vehicle occupants. They can be designed to store a limited amount of personal data such as contact lists, calendars, playlists, and favourite websites for easy access by vehicle users.

Telematics Operations Centre
Each Connected Car manufacturer has a network operations hub, which is a computerized system that oversees operation of the vehicle’s telematics services and operations. It is often managed by a third party (see Telematics System Providers, under The Connected Car Ecosystem, below). In a typical set up, the Telematics Operations Centre receives and processes data from the TCU, links it with information gathered from other sources, and delivers telematics service either back to the vehicle via the TCU (e.g., remote door lock/unlock, Wi-Fi connection, automatic crash assistance), directly to the end-user (e.g., monitoring reports or alerts sent to a desktop or mobile device), or to applications providers who use the data to deliver their applications. The Operations Centre therefore communicates constantly with the TCU as well as with other information sources and devices.

The Operations Centre performs network security, fault management, configuration, and other functions necessary for the telematics system to operate. One such function is billing – i.e., a customer relationship management system involving acquisition and analysis of customer profiles, subscriptions and telematics service usage. Telematics Operations Centres are typically scalable and can be designed to collect, store and analyze as much data as desired.

Call Centre
The Call Centre, usually operated by a third party service provider, provides real-time voice-based assistance to vehicle occupants for emergency and other purposes. Customer service representatives are able to access customer and vehicle information from the Telematics Operations Centre in order to provide the requested assistance. They can link to emergency services, assist drivers with system operation, and provide callers with destination information.

Service and Content Providers
Telematics technology provides a platform for a growing array of possible services, content and applications. Although some carmakers offer their own proprietary telematics applications, they are not in the business of content or entertainment. Infotainment systems therefore invariably include the provision of popular content and services from third party sources and providers such as Pandora and Spotify, and integration of popular systems such as Apple’s iOS and Android.16 Such content and services are delivered via the Telematics Operations Centre to the TCU (or possibly a separate infotainment module) where they are then delivered to end-users via the dashboard display unit.

---

Aftermarket Telematics Systems

There are two primary differences between automaker and aftermarket telematics/infotainment systems:

First, while automaker systems are internal to the car, aftermarket systems rely upon a device (“dongle”) that attaches to the OBD-II port and thereby provides access to vehicle data. The device also includes a built-in modem permitting it to communicate with both the customer and the service provider. It may also include a GPS unit, or may instead rely upon the customer’s mobile device for location information.

Second, the interface for automaker infotainment systems is typically a screen or other unit built into the vehicle dashboard. Aftermarket providers do not have access to this interface, and must either rely upon the user’s mobile device or provide their own separate interface device that can be mounted on the car dashboard.

Aftermarket telematics service providers have their own back-end systems, including in some cases Call Centres and networks of vehicle repair technicians for roadside assistance, as well as third party application providers for such services as remote home appliance control.

Wireless Communications Technologies

Telematics uses a variety of wireless communications technologies depending on the application. Different functions require different distance ranges, speeds and reliability of communication and therefore call for different communication technologies. For example, safety-critical vehicle-based applications require high reliability but not high bandwidth, while internet-streamed radio and video require high bandwidth but not high reliability.

Short-range wireless communications within the vehicle, such as those connecting user smartphones to the car’s dashboard display or to the aftermarket dongle, are typically handled by Personal Area Network systems such as Bluetooth or Wireless USB. Aftermarket products such as Mojio and Dash also use short range wireless communications to link customer smartphones with their OBD-II device.

Dedicated Short Range Communication, suitable for safety-critical applications in the 300m - 500m range, is being promoted for use in public safety-related Intelligent Transportation Systems.17

Communication of data between the TCU and the Operations Centre is typically handled by cellular communications. Cellular communications are rapidly evolving from second generation (2G) networks offering download speeds of 140 kbps, to 3G with speeds of up to 14 mbps, and now 4G LTE (Long Term Evolution) offering 173 mbps, making it possible for carmakers to offer high bandwidth services such as internet access. Wireless Local Area Network technology, known as Wi-Fi, is also used together with high speed cellular communications to turn cars into moving internet “hotspots” with the capacity to link several devices within the car to the internet at a given time.

Cloud Computing and Data Analytics

“Cloud computing” and data analytics are important tools used by telematics systems providers to process and use the increasing amount of data generated by telematics systems. Cloud computing is the distribution of computing tasks over several servers and other computer equipment so as to make efficient use of computing resources. Rather than each company using its own server to store and analyze data, several companies can pool server resources so as to provide faster and more reliable access to stored data. These pooled resources are referred to as a “cloud.” They must be managed to ensure that they have the necessary power, scalability, security, data storage and other capacities required by their users. Cloud services are offered by specialized cloud service providers or managed internally by large companies.

As one industry insider noted,

“...connected cars need data. Lots of data. ...But as connected cars before were sophisticated rolling wired devices, the amount of information flowing back and forth from them will skyrocket. And so they will demand for [sic] the cloud’s scalability and storage capabilities. The cloud also provides sophisticated processing and analytical capabilities. The cloud is the central hub where

all of this quickly changing, far-flung information will pass through. It will provide the platform for making sense of this data. And the cloud is also the home for building and developing the apps and programs used by cars on the road.18

Data analytics involves the application of mathematical and statistical modeling of data in order to discover meaningful patterns and draw conclusions about the data. Advances in data analytics technology and techniques, together with cloud computing and the availability of ever more data to analyze, allow companies to better understand their products and their customers. Carmakers can use data generated by their telematics systems, for instance, to track performance problems by location and/or user behaviour, generating “actionable insights” that can drive product and service improvements. They can also personalize services based on individual user profile and categorize customers for target marketing purposes. External sources of data, whether purchased through data brokers or obtained directly from publicly available sources, can be mined for additional relevant data that, when combined with the carmaker’s own data set, can help generate additional revenues through a better understanding of the customer.

**Intelligent Transportation Systems**

Intelligent Transportation Systems involve the development of interoperable, networked wireless communications among vehicles and roadside infrastructure, as well as pedestrians, cyclists and other physical things on or near the roadway. The systems use a variety of mobile sensors (e.g., radar, GPS, laser, video, light and thermal) and fixed sensors (e.g., traffic counters, cameras and weather instruments), together with wireless communications (Dedicated Short Range Communication), backend computing and information management (cloud computing) to allow vehicles, other mobile devices and roadside infrastructure to communicate with each other. ITS are only possible if a representative amount of data can be collected, processed and made available, all in real time.

As explained in the previous chapter under “Public Mandates”, Intelligent Transportation Systems are being developed by the public sector with the participation of the private sector, for public interest purposes.

---

CHAPTER 3
CONNECTED CAR APPLICATIONS

“The race is on for automakers to compete for customers globally through connected car solutions.”¹

“We need to look at the data we can get out of cars and ask how we can leverage this intangible.”²

As telematics and infotainment services merge, there is virtually no limit to the applications that will be developed to take advantage of the increasingly connected car. Ford, for example, has 11,000 developers working on innovative uses of technology using its Smart Device Link platform.³ Open platforms such as Google’s Android Auto and Canadian aftermarket provider Mojio create competition among developers for the next most popular car-related application. According to Jay Giraud, CEO of Mojio: “There are eight million software developers in the world and there’s at least eight million ways that the connected car and connected world is going to grow.”⁴

The following section describes Connected Car applications currently in use in North America and/or Europe.⁵ Not all described applications may yet be available in cars sold in Canada. The purpose of these descriptions and examples is to provide a sense of the range of uses to which telematics technology is being or may be put, as a foundation for the privacy analysis later in this report. Chapter Five examines the data extracted from these applications and its implications for individual privacy.

¹ Chris Penrose, Senior VP, Emerging Devices, AT&T Mobility, quoted in “AT&T Drive Studio and Ericsson release global study on Connected Car buyer”, Ericsson Press Release, Sept.10, 2014.
² Quote from participant in EY business leaders roundtable, EY, The quest for telematics 4.0: Dialogue with the value chain; Detroit executive roundtable summary, 2013, p.17.
⁴ Jay Giraud speaking on same panel.
⁵ Information is derived from automaker and aftermarket provider websites, accessed between December 2014 and February 2015, unless otherwise noted.
A common telematics application offered by both OEMs and some aftermarket providers is automatic collision notification, along with live agent assistance in the event of emergencies. When a crash occurs, connected cars are typically equipped with a feature that automatically sends data about the crash to the OEM or other Call Centre, or directly to the local 911 emergency response centre. In addition to location, such data may include model and colour of the vehicle, type of crash (front, side, rear or rollover), number of safety belts detected in use, number of airbags deployed, or other information that could help assess risk of injury. Emergency assistance systems typically activate hands-free voice systems, allowing passengers to communicate with rescuers directly, but they can also be activated manually with the push of a button.

Telematics enhances roadside assistance services offered by automakers or aftermarket providers by automatically communicating vehicle diagnostic information as well as location information to the service provider. In addition to faster service, technicians can guide drivers through repairs from a distance.

Live agent assistance can also be offered for non-emergency purposes such as destination finding, ticketing and reservations. Originally offered on high-end models, this service is now becoming mainstream with OnStar and Verizon both offering versions of it in 2015.
REMOTE MONITORING AND CONTROL

Remote Vehicle Diagnostics

With the ability to access vehicle bus data remotely, carmakers are able to engage in remote diagnostics, assessing the health of every vehicle they produce. Combining this with in-car voice communications, OEMs or their dealers can notify customers directly when service is required or recommended. Aftermarket products offer similar remote diagnostic services to consumers. Although limited to vehicle data that is made available to them via the OBD-II port, aftermarket providers are able to access enough diagnostic data to offer significant monitoring and diagnostic capability.

Some services allow customers to schedule appointments with the dealer from their vehicle without the need for a phone call. With access to the customer’s personal calendar, the service provider can even schedule the appointment itself. Customers can be provided with vehicle health reports by email or mobile app, and tools by which to monitor vehicle health or remotely check such things as tire pressure and fuel levels. Telematics also allows service providers to log driving records (e.g., locations, distances) for a given vehicle so as to understand the vehicle’s use pattern and therefore be better able to maintain and repair that particular vehicle.

Remote Software Updates

Telematics also allows for over-the-air system software updates, with potentially significant savings for OEMs in terms of avoided recalls and warranty costs. According to one expert, “60 to 70 percent of vehicle recalls in major automotive markets in North America and Europe are due to software glitches”, a proportion that will grow as automobiles become more dependent on software coding. Some OEMs are already using wireless telecommunications to update software. For example, Tesla used an “over-the-air software update” to direct its Model S electric car to maintain greater clearance after determining that battery fires were likely caused by debris kicked up from the ground.

Fleet Management

Whether delivery trucks, taxis, rental cars, or company cars, telematics have become a standard tool by which businesses and others manage their automotive fleets. Telematics systems that remotely access OBD data along with data from GPS receivers allow fleet owners to keep track of their vehicles – where, when and how they are being driven. Telematics allows for detailed monitoring of employees using company vehicles, as well as monitoring of vehicle health and performance, both real-time and historical. Fleet managers can see at any given time where each vehicle is, whether it is moving or stationary and the status of equipment such as the snow blade (up or down) or sand spreader (on or off). Using any number of methods by which to verify driver ID (e.g., RFID-enabled ID cards, coded keys or fobs, biometrics), they can also verify who is driving the vehicle. They can monitor speed, driving direction, ignition status, driving violations and see a trail of where the vehicle has been. Telematics also allow fleets to determine the most efficient routes, saving them costs related to personnel, gas, and maintenance.

Usage-Based Insurance ("UBI")

While telematics-based insurance programs are relatively new in the Canadian market, insurance companies in Europe and the US have been using the technology for a number of years to track driver behaviour and thereby tailor insurance rates to the individual customer. This is referred to as Usage-Based Insurance ("UBI") or Pay-as-you-drive ("PAYD") insurance. Premiums can be based on where, when and/or how the vehicle is driven, with lower rates or discounts offered to drivers who drive less, only in daylight hours, only on safer routes, and who do not engage in hard braking, fast acceleration or other tracked behaviours that suggest higher risk driving. Similar systems are used for safe driver programs, allowing drivers and others to monitor their own driving and even the actual or possible effect of it on their insurance rates.

UBI systems can also allow insurers to refine their risk assessment metrics, to receive automatic notice

---

7 e.g., Hyundai BlueLink Connected Car Service Link. 8 e.g., OnStar, Hyundai BlueLink Connected Care. 9 E.g., OnStar RemoteLink mobile app.
12 e.g., see www.mixtelematics.com
of accidents, to more accurately estimate accident damages, and to reduce fraud by analyzing driving data (such as hard braking, speed, and time) during an accident. In addition, UBI devices can be used to track and recover stolen vehicles and thereby reduce costs related to vehicle theft.

Most UBI products in Canada involve the installation of an aftermarket telematics device in the vehicle’s OBD port to measure distance driven, time of day driven, as well as acceleration, braking, speed and cornering. Data is sent wirelessly to the insurer (or more typically, a third party service provider) who stores and processes it. Discounts of up to 30% are typically offered for drivers who drive less overall, who do not drive between midnight and 5am, and who refrain from sudden braking and acceleration. UBI telematics devices also monitor location, which may be used to deduce additional driver behavior such as lane changes that goes into the risk calculation.

Another approach, used in some applications in the US and the UK and likely to become more common as the technology becomes more pervasive and mature, uses an app on a policy-holder’s smartphone to assess driving behaviour. Smartphone-based technology has the advantage of being familiar to consumers, and reduces initial expenses for an insurer who need only supply an app, not a device, to the consumer. However, it also requires considerable ongoing effort by the consumer: the phone must be in the car, charged and on; and for optimal effectiveness, it needs to be tethered to the vehicle – e.g., placed in a mounting bracket before driving. While there are doubtless ways to make this easy for drivers, no amount of programming can affect the need for the driver’s participation. Security, intellectual property and data portability, and the difficulty of determining whether the phone’s owner is in fact driving or is instead a passenger in another vehicle, are also ongoing challenges for insurers wishing to implement UBI using a smartphone platform.

UBI can also be offered by OEMs using embedded telematics systems, as GM is now doing. Such systems obviate the need for a separate device, and can include smartphone-based functionality. The service, regardless of technological platform, often includes a personalized dashboard application that may be viewed on a personal computer or other device, that displays data collected about drivers’ behavior and how it is affecting their insurance premium. One program (Mobiliz) that is targeted to 16-24 year old drivers, is marketed as a method of encouraging safe and responsible driving. It assesses driver behavior on a monthly basis and adjusts monthly premiums upward or downward, accordingly. Other programs only offer discounts. Because the insurance industry is regulated provincially in Canada, the permitted uses of telematics data for insurance purposes varies across the county.

Automotive Financing

Using similar technology, automobile creditors can manage their loans by reminding borrowers of overdue payments and, if necessary, locating, disabling and repossessing vehicles. iMetrik, a Canadian company that supplies GPS-based tracking systems for insurance as well as financing purposes, claims to be “the only GPS global provider serving the subprime industry with 3.5G technology...”, with over 800,000 vehicles connected and over 10 billion kilobytes of data. iMetrik markets its tracking solutions to “Buy-Here Pay-Here (BHPH) car dealers, car credit companies and lenders wishing to experience more on-time payments, fewer repossessions and greater profits”. Lenders can require that customers agree to have the device installed in order to obtain the loan. The device alerts delinquent drivers with an audible alarm every time they start the car, disables the car starter after a payment is missed (the lender can determine the grace period if provincial consumer protection laws do not do so), enables it when payment is made, and locates the vehicle for repossession if warnings and disabling commands are ignored. Similar services are offered to North American dealers and lenders by US-based companies Skypatrol and PassTime. Their GPS-based systems allow lenders to set geo-fence boundaries, as well as to locate vehicles, view vehicle location history, alert drivers to unpaid bills and enable or disable the vehicle’s starter. PassTime’s “automated collection technology” is notorious for the annoying beeps that are used to

13 AllState in the US is offering smartphone-based UBI as part of its DriveWise program, although DriveWise also has an OBD2 option. Other companies, including Agero, Cognizant and Deloitte are developing or have developed UBI smartphone apps. The Financial Services Commission of Ontario (“FSCO”) has indicated that a smartphone offering may be ‘in the works’ for Ontario soon.
remind customers that they owe money before the ignition is disabled.

Starter-interrupter devices are controversial, with reports from the US of lenders disabling cars within a few days of the payment due date17 and of a disgruntled employee remotely disabling more than 100 vehicles.18 There are reports of cars being disabled while idling at stoplights and one report of a car being shut down while being driven.19

Car Sharing

Car sharing is increasingly viewed as a realistic alternative to car ownership and is now seen by industry experts as a major disruptive trend that will affect vehicle design and sales in the future. Telematics has made the growing popularity of car sharing possible by providing real time information to customers on the availability and location of cars, facilitating member access to the vehicles and monitoring vehicle use for payment purposes. For example, MoDo, a carsharing cooperative in Vancouver, offers members access to cars using a fob that disables the engine when the vehicle is parked and not in use. Bookings can be made online, using an app that shows the location of available cars.

With a fleet of over 300 SmartCars in both Vancouver and Toronto, Car2Go offers one-way point-to-point rentals. Users are charged by the minute, with hourly and daily rates available. There is no central office, and cars are accessed by members wherever parked using a downloadable smartphone app.

Zipcar.ca also offers a car-sharing service in various locations across North America. Once approved, a new member gets a “Zipcard” that unlocks the reserved vehicle simply by holding the card to the windshield. Zipcars can be reserved, locked and unlocked using a mobile app. Telematics can also be used to monitor and report on vehicle use within pre-defined geographical areas, for example to show the reach of fleet-based advertising.

Electric Vehicles

Telematics allows manufacturers of electric vehicles to provide their customers with real time information on the location of charging stations. Vehicles can then communicate with the stations’ reserve spots and be billed automatically. Navigation services offered by suppliers such as Inrix and HERE Auto to electric carmakers include showing charging locations for electric vehicles on the in-car map, along with relevant data including the type of plug, voltage, and amenities. They can also indicate where services are available and whether they are busy. As well, drivers can check their car’s battery charge and precondition the car remotely, while carmakers can monitor the performance of new battery technologies. In the words of one expert: “Because of the huge importance of battery for electrical cars, remote services for monitoring battery level and usage over lifetime makes the use of connectivity indispensable. As we see it, telematics and electric cars go hand-in-hand.”20

Convenience applications

Common convenience-related applications of telematics offered by OEMs to individual owners include remote door locking and unlocking, car locating, horn and light activation, climate control and engine starting or stopping, all from anywhere with internet access.21 Using a mobile app, the car owner can log into the system and operate the remote controls, even disabling the car unless and until a password is entered into the system. OnStar also offers remote control of the vehicle’s built-in Wi-Fi internet connection. In addition to a “Remote App”, BMW allows its ConnectedDrive customers to call the BMW Call Centre and have an agent activate the remote service for them. Some OEMs are developing remote applications that can be performed using wearables – for example, Hyundai recently showed off a smartwatch that can start or unlock one of its cars.22

As the Internet of Things develops, cars are connecting with other devices, starting with those in the home. Mercedes-Benz and Ford now offer services via

---

18 Kevin Poulsen, “Hacker Disables more than 100 cars remotely”, www.wired.com, March 17, 2010.
20 Rémi Demerlé, Director of Global Partnerships for Telenor Connexion, quoted in “Car telematics enters the mainstream”, 26 July 2012, www.telenor.com
21 e.g., OnStar RemoteLink Mobile App, Hyundai Blue Link Remote Access.
22 Keith Naughton, “Cars are becoming increasingly important to the annual International Consumer Electronics Show”, <driving.ca>, Dec.29, 2014.
Google’s “Nest” through its vehicles, automatically opening and closing the garage door and communicating with home thermostats. Aftermarket provider Vinli offers a similar application called “Home.” U.S. smartphone-based aftermarket provider Automatic offers a growing suite of convenience applications via its “IFTTT” (If This Then That) platform: customers select triggers (e.g., leave home, begin drive home) and actions (e.g., turn off house lights, text spouse to say I’m on the way home) that then occur automatically.

Blackberry launched its “IoT Platform” in January 2015, focusing initially on automotive applications. Blackberry gives the following example of the value-added services that its platform can deliver:

“a user’s driving preferences like seat position, mirror position, steering wheel tilt, music, and frequently called phone numbers can be stored in the cloud. Vehicles can have an infinite number of custom user profiles. The user profile becomes portable and upon buying, renting, or borrowing another car, the profile can be transferred, which leads to improved brand loyalty and customer satisfaction.”

Other IoT applications include Volvo’s Roam Delivery service, which allows car owners, through digital key technology, to have their online shopping goods delivered to their car. Similarly Toyota’s has partnered with Panasonic to integrate cars with home appliances, and various OEMs are collaborating with electric utility companies to manage energy grid consumption using signals from electric cars.

Using the same technology as for fleet management, both carmakers and aftermarket providers can offer individual car owners the ability to monitor their vehicle activity and location. Geo-fencing can be used to alert owners if their vehicle has been driven out of preset geographical boundaries. Alerts can also be sent if, for example, a preset speed or distance limit is reached. With remote vehicle monitoring services, OEMs can inform owners of where their vehicle is at any given time, if it is sitting idling, what speed it is being driven at, when it was last started and when it was shut down. Hyundai’s BlueLink service, for example, allows parents to monitor and set restrictions on the car’s speed, hours of operation and where it travels. If any of the limits is exceeded, the owner is notified by text or email.

FordSYNC recently introduced an integrated version of the “Life360” smartphone app, allowing connected users to see where one another’s location is on a map, send messages amongst themselves and get help in an emergency. Once the driver connects his or her smartphone to Ford SYNC via Bluetooth, the app automatically sends a message to everyone in the driver’s Life360 circle suggesting they not text the driver. A follow-up message is sent once the driver arrives at his or her destination and turns off the car.

Interior cameras can also be used to record who is in the vehicle and share that information remotely. Brick House Security, for example, offers aftermarket “dash cams” with 120+ degree viewing angles and the ability to record audio that are marketed as:

“a great way to make sure your teen driver or employee is doing the right thing behind the wheel. Dash cams are also great for providing evidence in case of an accident or insurance dispute. Choose from any number of functions, from dual lens car security cameras that face inside and outside to in-car video systems with night visions recording, accident sensors, built-in GPS logging software and more.”

LOCATION-BASED SERVICES

Location information is central to many if not most Connected Car applications, whether for safety, convenience or other purposes. In addition to vehicle monitoring and other location-related services noted above, GPS functionality in Connected Cars allows for destination-finding services, real-time traffic and weather information, estimated commute times, fuel station location and pricing, and parking services that guide drivers to the closest available parking space. Vehicle navigation services have evolved from simple in-car navigation to location-based services that span the entire journey – from planning on a home computer to using a smartphone app to find the final destination.

25 e.g., Mojio Family Connect. e.g., Lexus Enform Remote, Hyundai BlueLink.
Enhanced Navigation

Navigation services offer turn-by-turn directions, often by voice and now using 3-D mapping. OnStar was a pioneer in this area and other carmakers are now following suit. At the same time, a number of independent companies have built strong reputations based on their aftermarket navigation systems for vehicles. Some applications provide drivers with real-time information on traffic conditions, calculating delays and offering detour suggestions. Traffic information is gleaned from a variety of sources including cell phone companies whose networks are being used to deliver navigation services to drivers, GPS data from vehicle fleets, police reports and other drivers. Traffic apps commonly require users to agree to let their (anonymous) speed and location information be tracked and used for the purpose of the app.

TomTom offers aftermarket navigation systems that can be either added to the built-in system of certain vehicles by the dealer or used via a smartphone set on the dash. Not only does TomTom provide detailed map-based directions, it can display a full picture of traffic jams nearby and identify the fastest route or tell drivers the cause and length of the delay of a particular congestion, identifying where it starts and ends.

Nokia’s HERE Auto service, provided to carmakers, offers an in-dash navigation system as well as a smartphone app. According to its website, “what sets HERE Auto apart is our location cloud, a robust engine that provides always-on access to dynamic services”, allowing customers to “save your favourite places, routes and commutes in the HERE Cloud and synchronize them with other HERE products.” HERE customers can get fuel price information on the road, find available parking, see street level images of destinations, and access community-generated content (e.g., ratings, reviews, pictures) about nearby points of interest, among other things. HERE aggregates information from many sources to deliver a complete package to carmakers and through them to drivers.30

Waze, a crowd-sourced app owned by Google, advertises itself as “the world’s largest community-based traffic and navigation app”.31 Information on traffic, road hazards, accidents, police traps and other road-related data is gathered from other app users. “After typing in their destination address, users just drive with the app open on their phone to passively contribute traffic and other road data, but they can also take a more active role by sharing road reports on accidents, police traps, or any other hazards along the way, helping to give other users in the area a ‘heads-up’ about what’s to come.” Waze learns users’ frequent destinations, commuting hours and preferred routes. It allows users to add contacts as “Friends” and to share routes and see their “Friend’s” ETA when driving to the same destination.32

Geo-fencing

As noted above, telematics allows vehicle owners to establish geographical boundaries beyond which they do not wish the car to be driven. If the vehicle does venture out of bounds, the owner receives a notice, such as an, email, text or other notification. Geo-fencing can be used by employers and rental car agencies to detect out-of-bounds driving, and is now being marketed to parents for monitoring their children’s use of the family vehicle.

Destination Finding and Local Search services

Navigation systems are now incorporating information search capabilities designed to assist drivers find particular destinations or services. Lexus offers a service allowing users to search, organize and name up to 200 destinations in 20 separate folders and send them wirelessly to the Lexus Navigation System. Some systems offer the ability to link to a live operator who will assist with destination information and guidance.33 OnStar offers a service called “Destination Download”: drivers can simply push the OnStar button and ask the agent to download directions to the vehicle. Car owners can also send destination addresses, turn-by-turn directions and telephone numbers to their vehicle, so that once in the car, they can call up the information on the dash screen.34

Local search services - for anything from restaurants to gas stations - are also being offered increasingly. Ford SYNC offers “points-of-interest search and expanded recognition of voice commands such as

33 E.g., Mercedes-Benz mbrace Virtual Co-pilot.
34 e.g., OnStar, BMW “My Info/Send to Car”.

‘I’m hungry.’ Higher end services will help drivers narrow their choices by distance or type of cuisine. Many carmakers have embedded the Yelp local search application, or simply enabled its use via the dashboard display.

It is now common for rental car agencies to offer vehicle-based navigation services. Hertz now offers a smartphone app that pairs with its in-car “NeverLost” GPS navigation system, allowing customers to plan their trip in advance, then transfer the details including stopping points to the in-car system. The navigation system pairs with smartphones to store destinations, make calls to points of interest, place reservations, and access the contacts file. Other features include weather and flight information as well as access to a concierge who can help search for destinations, create custom trips and send route information directly to the system.

Location-based Advertising

“Imagine the continuity marketing opportunities that flow from having a continuous, two-way conversation with your drivers.”

Vehicle-to-Retail, or “V2R”, communications are expected to be one of the most dominant segments of the Connected Car market over the next decade or more. The same proximity-based marketing systems used to send SMS advertising messages to mobile devices within a certain range of the business, or to send custom advertising to cell phone subscribers based on their current location, can be applied to connected cars. GM OnStar recently unveiled a new advertising feature that is expected to be available to its North American subscribers in 2015: “AtYourService” allows retailers and merchants to deliver special offers to OnStar subscribers based on their requests for directions to a particular point of interest or location. OnStar currently receives over 35 million requests for directions from its North American users. Already, OnStar has signed up partners such as Dunkin’ Donuts and Priceline.com. “AtYourService” combines popular location-based information and reservations concierge services with local advertising.

Mobile advertising company Kiip has partnered with aftermarket telematics provider Mojo to offer targeted advertising to drivers with the device. Kiip specializes in “moments targeting”: using advertising to reward people at particular moments of their day in relevant ways. Its head of partnerships sees access to data from a car’s engine and safety systems via the Mojo device as providing the basis for profitable new approaches to ad targeting: “It could be you just had a little fender bender, and you need something to lift you up”; “You get to your meeting early and you should get a free coffee from the place around the block”; or “you just logged 100 miles on a road trip; your phone says, ‘Here’s a Red Bull.’”

Stolen Vehicle Recovery

Telematics is now widely used to locate and recover stolen vehicles. This is a common feature offered by OEMs in conjunction with other remote control and monitoring services, but similar services are also offered by aftermarket service providers. One company, Lojack, specializes uses radio signals rather than GPS signals to locate stolen vehicles. Lojack’s Boomerang system requires that the vehicle in question be equipped with a special radio transceiver, which is easily installed in a non-visible location. Once installed, the device and the vehicle VIN are registered in the Lojack system database. When the owner reports a vehicle theft to Lojack or partnering law enforcement agencies, the device is automatically activated and begins emitting radio signals (a 2 millisecond chirp every ten seconds). Lojack’s local recovery team and/or partner police, equipped with signal-receiving devices on their vehicles, are then alerted when they detect the vehicle within 3-5 miles. The tracking units display the approximate direction and distance to the stolen vehicle, as well as a serial number that links to a physical description of the vehicle including licence plate number and VIN. Lojack also offers a stolen vehicle notification service: if the central Lojack system detects that the car has been started by someone without the associated fob, it sends alerts to the car owner.

26 e.g., Lexus “Destination Assist”.
29 “Smart Car Innovation and Value Creation to Shift to the Boundaries between Automotive and other IoT Segments, according to ABI Research”, www.businesswire.com, June 18, 2014.
AUTOMATIC LICENCE PLATE READERS

Law enforcement agencies are increasingly using sophisticated cameras called “Automatic Licence Plate Readers” (ALPRs) to scan and record vehicle licence plates for such purposes as locating stolen cars, tracking suspects and collecting unpaid tickets. Mounted on top of patrol cars or overlooking city streets, these cameras can scan licence plates day or night, from as far as 1500 feet away. They can record hundreds of licence plates per minute and can instantly compare them to enormous databases so as to provide real-time matches to police or repossessors.42 A leading provider of ALPR technology to law enforcement as well as repossessors, MVTrac, operates a system that captures millions of digital reads each week from thousands of static and mobile cameras located worldwide. It archives the intelligence in a centralized database, against which matches can be made. ALPRs can also be used to monitor and enforce vehicle registration.43

PERSONAL CONNECTEDNESS AND INFOTAINMENT

Hands-free Communications

Hands-free operation of infotainment systems through voice recognition technologies is critical in order to minimize driver distraction and comply with local laws. Connected cars typically allow drivers and passengers to make and receive voice-activated phone calls and engage in hands-free texting, tweeting and emailing via the car interface: touch-screen, buttons on the head unit, or steering wheel controls. Ford SYNC’s system allows drivers with synchronized phones to continue telephone conversations uninterrupted as they move from the smartphone to the car-based system and back again. In all systems, hands-free operation is key: voice command systems allow drivers to dial phone numbers, browse contacts and direct-dial locations stored in the navigation system without having to use their hands.

Interior cameras are beginning to be deployed for gesture recognition, to further facilitate driver commands.44 Interior cameras, facial recognition software and data analytics can be further used to authenticate drivers and then personalize the display information (e.g., calendar, music, contacts) specific to that individual.45 Cadillac’s CUE system can detect hands approaching the screen before they actually touch it. Ford has been working with Intel on a project called Mobile Interior Imaging, (“Mobii”). If the driver is not recognized, a photo is sent to the owner’s smartphone. The owner can then set permissions and specify features on the car that should be enabled or disabled (e.g., limiting speed or phone use while driving).

Contacts and Calendars

Connected Car systems commonly store users’ contact lists for easy access in the car. The Buick Intellilink system automatically downloads names and numbers programmed into the user’s Bluetooth-paired smartphone, allowing users easy access to their contacts’ phone numbers from the vehicle. Ford SYNC does likewise, and can also display photos from the user’s phone book on the dash screen when calling, receiving a call or browsing the user’s personal directory. It can also show Caller ID, call waiting, a caller log, and contact list on the display screen.

Personal calendars can also be synchronized and downloaded into car-based systems. BMW Connected includes an app that imports the user’s calendar entries onto the vehicle display and can read out appointments on request.

Infotainment

Connected Cars typically have built-in entertainment systems with the ability not just to receive broadcast radio and play CDs but also to stream music, internet radio, audiobooks and podcasts through such services as SiriusXM, Pandora and Spotify. Some systems allow users to store favourite music and other content in vehicle-based library.46 Whether delivered via an embedded system or simply mirroring the user’s integrated smartphone interface, in-car infotainment systems typically include a dashboard screen that is used not only to access communications and infotainment functions but also for navigation and other telematics-based services.

---

46 E.g., Chevrolet MyLink.
Infotainment systems are generally separate from vehicle operations but can be linked to the vehicle bus for such purposes as automatic adjustment of volume levels according to vehicle operations and related noise. Infotainment systems are however commonly linked with the navigation system and typically offer access to various location-based information services (see above) as well as news, weather, social network updates and web browsing. The possibilities for car-based apps delivered via these systems are almost endless. BMW offers a large number of BMW-specific and third-party applications and services through its ConnectedDrive store, both online and via the car’s on-board system. Both vehicle-based apps and smartphone-based apps are available via BMW Online. U.S. aftermarket provider Dash allows registered users to upload their driving data to a “leaderboard” from which they can compare driving metrics with friends on social networking sites.

Originally planning to introduce its own “AppShop” in 2015, GM has delayed this launch while it develops a system that will support Android Auto and Apple’s CarPlay. Other OEMs are expected to do likewise given that many popular infotainment apps that operate on the Android and Apple platforms are already available via smartphone app stores and can rely on the smartphone for connectivity. To the extent that they merely facilitate the provision of third party Apps over their infotainment systems, automakers are effectively turning their vehicles into one more mobile device for consumers.

Infotainment systems not only deliver streamed music, content and communications but also allow users to store personal settings, playlists, favourites and selected content. Cadillac’s CUE system stores up to 60 presets from music, addresses, maps, phone numbers or system commands, and displays the most frequently used applications along the top of the screen. Ford SYNC helps users browse music collections and create playlists. It will also index the user’s podcasts and audiobook library, as well as their music. Ford’s new SYNC3 platform will be upgradeable over the internet, “so it can receive updates even at a Starbucks with free WiFi.”

Aftermarket providers of infotainment systems include Navdy, a “head-up display” device that sits on the dash in front of the driver and projects data from the smartphone onto a transparent screen that appears to be floating two metres ahead. Navdy integrates the user’s smartphone into a more driver-friendly device, adding voice and gesture controls, and allowing the user to control which kinds of notifications to display or have read out automatically. The smartphone connects to the device via a Bluetooth-equipped dongle plugged into the OBD port.

**Wi-Fi Hotspot**

Connected Cars can also be turned in to WiFi “hotspots”, allowing occupants to access the internet via personal devices while on the move. OnStar’s new 4G LTE service provides state-of-the-art connectivity that turns the vehicle into a Wi-Fi hotspot as soon as the car is on, and operates without draining a mobile device battery. Aftermarket portable wireless routers are also available: Autonet offers one for cars, called “CarFi”, with monthly data plans. IEEE experts have predicted that 60% of vehicles on the road will be internet-enabled by 2025.

**Health and Wellness Applications**

One of the newer frontiers for Connected Car applications is personal health and wellness. Ford has been working on various ways to integrate mobile health services with its cars: Bluetooth connectivity between the car’s computer and personal medical devices (e.g., glucose monitoring devices), remote access to cloud-based health and wellness services via the car’s computer (e.g., allergy alerts), and syncing with health apps users already have on their smartphones or wearable devices. According to Fact Sheets published by Ford’s “SciLab” in 2011, a diabetic person could connect their glucose monitoring device to the car via Bluetooth and monitor glucose levels and trends through audio alerts and visual displays. As well, “[using] voice commands, Ford SYNC users could access their WellDoc profile to receive real-time patient coaching, behavioral education and medication adherence support based on their historic and current disease information.”

---

45 “Ford In-Car Health and Wellness Solutions” Fact Sheets: “Medical Device Connectivity via Bluetooth”, “Allergy Alert via Ford SYNC AppLink” and “WellDoc® via Ford SYNC Services”, all dated 5/2011. These applications have been stalled apparently because of US Food and Drug Administration regulatory requirements: “Bumps on the road to mHealth in the connected car”, Telematics Update, April 4, 2014.
Although these applications have not yet been marketed, the growing popularity of wearable devices is making this kind of driver health monitoring more realistic. With Bluetooth connectivity, any device can be connected to car systems. This enables carmakers to gather biometric data from drivers and passengers more easily and reliably than via steering wheel or other car-based sensors. For example, heart rate monitors can indicate when drivers are stressed. According to a journalist who visited the Ford Research and Innovation Center in Michigan in June 2014, “Ford vehicles don’t currently offer any integration with any wearable platforms, but clearly it’s coming. [Ford representative] Buczkowski said the company will ultimately work to support all of the different wearable devices that are expected to hit the market in the coming years.”

Nissan’s Nismo Smart Watch, introduced in 2013 and aimed at performance-oriented track drivers, connects to drivers’ smartphones via Bluetooth technology and actively monitors a number of both automotive and bio metrics, including speed averages, fuel consumption habits, and heart rate. The watch also allows users to access weather conditions and share content with social media like Facebook, Twitter, and Instagram.

Fitness tracking company Jawbone and U.S. aftermarket provider Automatic have partnered to offer users of both the Jawbone UP wristband and the Automatic smartphone app a way to integrate their driving data into the Jawbone app so that it appears alongside their physical activity log. If the user doesn’t achieve their target step count for the day, the app might point out when and where they could have walked instead of driven.

**ENHANCED SAFETY**

**Advanced Driver Assistance Systems**

All carmakers are now equipping vehicles with increasingly sophisticated advanced driver assistance systems (“ADAS”) such as blind spot warnings, forward collision warnings, parking assistance, traffic sign detection and cruise control that adapts to the speed of cars ahead. ADAS systems rely on sensors, cameras, laser scanners and radar-emitting devices embedded in the vehicle, together with ECUs that receive, interpret and act on data generated by the sensors and other input units. Some applications are automatic (e.g., braking to avoid a collision) while others issue warnings or other information to the driver (e.g., traffic sign detection). ADAS are increasingly prevalent, especially in high end car models. GM, for example, has stated that the 2017 Cadillac will be able to operate hands-free in certain conditions.

For the most part, ADAS operate without transmitting data outside the vehicle and are therefore are not properly considered “telematics” as we have defined it. However, they can gather and use data from drivers or other sources outside the vehicle and in those respects, can be considered elements of a Connected Car.

**Driver Monitoring**

In addition to external cameras offering 360 degree images to aid parking and recognize pedestrians or other obstacles, carmakers are increasingly looking to inward-facing cameras and biometric sensors to monitor driver alertness and behaviour as part of ADAS. For example, driver monitoring based on eye-tracking and/or other biometric sensing could be employed on semi-autonomous cars to determine whether the driver is ready to assume manual control of the car.

One form of ADAS involves the use of cameras and vehicle sensors to detect driver lack of attention or drowsiness (e.g., if car is drifting out of the lane, together with changes in the driver’s pedal use, steering, speed, etc.) and set off alerts or other vehicle system adjustments designed to wake the driver up or encourage a stop. More advanced systems involve interior cameras that monitor driver attention, vision and/or head pose.
A further refinement of such systems involves the use of biometric sensors.\(^{58}\) Biometric sensors in the steering wheel, seat and seatbelt can monitor drivers’ palms, facial temperature, heart rate and breathing rate. Volvo is reported to be working on sensors that detect driver drowsiness based on head and eye movements.\(^{59}\) Toyota was reported in 2011 as developing a steering wheel with an embedded ECG to detect abnormal heart rhythm through the driver’s hands. Ford has also been developing various health and wellness applications for its cars.\(^{60}\) In 2012, Ford was experimenting with a system it called “driver workload estimation” to use such data, in combination with data on driver use of the throttle, brakes and steering wheel, to adjust warning times for collision alerts and automatically filter out phone calls and messages if drivers seem to be losing attention or getting stressed.\(^{61}\)

IMS, a Canadian-based supplier of usage-based insurance via its “DriveSync” connected car platform, recently showcased technology that would use insights gained from wearable technology to anticipate driver behaviours. In a news release describing its driver health monitoring service, IMS explains: “For example, sleep patterns, glucose monitoring levels and abnormal heart rate detection are used to signal driver drowsiness and potential health risks.”\(^{62}\)

**Autonomous Cars**

The ultimate manifestation of ADAS systems is the fully autonomous car. Nissan has announced plans to have fully autonomous cars ready for sale by 2020, while Audi piloted its prototype autonomous car on public roads in January 2015.\(^{63}\) Google’s well-publicized fleet of autonomous vehicles has been driving safely on public roads in California for years.\(^{64}\) By definition, autonomous cars do not rely upon communication with other vehicles or information sources, and are therefore not generally considered to be “Connected Cars”, nor do they necessarily use personal information. However, autonomous cars will undoubtedly be connected in a number of ways – at a minimum, by receiving data from other vehicles and sources to create and continually update the “maps” on which they rely to navigate safely, and by updating vehicle systems software over the air and relaying information to the vehicle owner. As well, in-vehicle personal communications and infotainment are expected to play a much greater role in autonomous vehicles since occupants need not drive.\(^{65}\) More importantly, autonomous vehicles will undoubtedly be integrated with Intelligent Transportation System, thus becoming “Connected Vehicles”.

**Intelligent Transportation Systems**

At the same time as they are developing and implementing autonomous ADAS, automakers are working with government agencies and researchers to develop Intelligent Transportation Systems (“ITS”) that rely upon constant communications among vehicles (“V2V”) as well as between vehicles and the surrounding infrastructure (“V2I”) to navigate and avoid collisions. (For a brief explanation of ITS systems and the government’s interest in them, see Chapter One, under “Public Mandates”, and Chapter Two, under “Intelligent Transportation Systems”.)

For example, Volvo has announced that its “Drive Me” project (endorsed by the Swedish government) will feature 100 self-driving Volvos on public roads in and near the automaker’s Swedish hometown of Gothenburg in 2017.\(^{66}\) GM is planning to include V2V technology in its 2017 Cadillac, challenging other OEMs to do likewise.\(^{67}\) Although currently focused on assisting human drivers to take appropriate corrective action in the face of danger, the ultimate manifestation of a road-based Intelligent Transportation System is the self-driving car.

Like other ADAS applications, V2V applications include driver warnings about blind spots when changing lanes, imminent forward collision, and unsafe conditions to pass. They can detect the speed and location of approaching and surrounding vehicles, and can take into account road conditions ahead. V2I applications include curve speed warnings, red light violation warnings, and stop sign gap assistance.

\(^{63}\) Tom Maloney, “Technology in place for autonomous cars, but is it meaningful?”, Globe & Mail, Jan.5, 2015.
\(^{67}\) Keith Naughton, op cit.
V2X technology takes autonomous ADAS a step further through its ability to “see” around corners and “through” other vehicles, thus perceiving threats sooner than vehicle-based sensors, cameras or radar can. It is estimated that a system of V2V and V2I communications could, by warning the driver of an impending hazard, prevent a significant number of vehicle crashes involving unimpaired drivers.68

Autonomous vehicle technologies are seen as complementary to V2V technologies and it is expected that the two will merge so as to augment system accuracy and efficiency. Some initiatives are already two-track, developing autonomous ADAS as well as V2V communications systems.69

**TAXATION AND TOLLS**

**Distance-based Road Taxation**

The concept of taxing drivers based on distance travelled is more advanced in Europe but has been promoted in the US as a new model for financing roads as improvements in fuel economy and the growing popularity of electric vehicles reduce revenues for highway maintenance. Drivers can either pay a high flat rate for unlimited driving or allow a GPS-enabled metering device in the vehicle (dongle or smartphone app) to track distance driven, calculate the amount owed and determine the appropriate taxing jurisdiction. Payments can be made via regular billing, gas pump-based systems, or automatic deductions from a prepaid customer account. Various options have been explored to protect the privacy of participants. Oregon was the first state to pass legislation enabling a system of road usage charges for transportation funding. The law, passed in 2013, authorizes the Oregon Department of Transportation to establish a pilot project with 5,000 volunteer motorists beginning July 2015, to test the mileage-based collection system.

**Electronic Tolling**

Electronic toll collection systems typically rely on radio-frequency identification (“RFID”) tag transponders embedded in or applied to vehicles and RFID readers at the toll gate, sometimes in combination with Automatic Licence Plate Readers (“ALPRs”). Satellite-based telematics systems are now being promoted for use in electronic toll systems, reducing delay at toll collection points and managing congestion in dense urban areas. In contrast to older technology RFID beacon systems, telematics-based toll systems allow for detection and recording processes to be performed virtually, without the need to install or expand infrastructures along roads. Computer modules at the operator site or offered via a cloud-based service automatically collect road-usage data and calculate tolls. Each vehicle’s on-board GPS unit transmits data required for calculation and billing of road tolls.

Singapore is developing “smart road” toll technology that would be based on global navigation satellite system (“GNSS”) location monitoring, thus overcoming the constraints of physical entry and exit points and allowing for distance-based pricing. The new system is intended to provide drivers with a range of value-added services, including real-time traffic information tailored to their location and electronic payment for parking. Opposition parties expressed concern about the privacy implications of this move.

**CONNECTED CAR APPLICATIONS – LOOKING AHEAD**

Telematics and infotainment services offered by OEMs have evolved over the past few years from a differentiator to a mainstream offering in new vehicles and they continue to evolve by leaps and bounds each year. Common telematics services now offered by OEMs and aftermarket providers include emergency and roadside assistance, stolen vehicle

---

69 Volvo’s “Drive Me” pilot project is a joint initiative with public sector partners and involves developing a “smarter” infrastructure with which vehicles can communicate. See footnote above.
tracking, remote vehicle diagnostics and remote control features. The number of GPS-based traffic and location-related services continues to grow. Infotainment systems are turning cars into another fully connected mobile device. With the addition of biometric sensors, cameras, and predictive analytics technologies, new applications based on gesture and mood sensing, consumer behaviour analysis and cloud-supported user experiences will result in increasingly personalized services.

It is no longer science fiction to contemplate a car that, while you are preparing to drive to work, checks the weather, your schedule for the day, traffic conditions, and plans your route accordingly, re-routing as necessary to avoid traffic jams, before locating an available parking spot to save you time. Nor is it unrealistic to expect a rental car to recognize you when you enter the car, and to adjust the seat, mirror, calendar and music to your preferences based on the same brand of vehicle that you own. The technology exists now for a car to be able to check your blood pressure, and if it finds it elevated, play soothing music as it drops you off at work and then goes to park itself. With current technologies, cars can not only make restaurant suggestions based on your food preferences (as determined by your previous food purchases) but then make a reservation for a time of arrival taking into account the restaurant’s location, local traffic conditions and your driving style. In the words of industry executives:

“We try to bring the digital life into the car and the car into the digital life... Not only do we want to make the internet accessible from the car, but also the other way around, that is, to make the car accessible from the internet – a truly bi-directional connection.”

“[W]e are .. entering a new era of Connected Car innovation that will integrate all aspects of a person’s life.”

According to Peter Sweatman, Director of the University of Michigan’s Mobility Transformation Center:

“We are on the cusp of a transformation of mobility on a scale we haven’t seen since the introduction of the automobile a century ago.”

Whether from a commercial or public service perspective, the development of Connected Cars is ushering in a completely new concept of transportation, one that centers around the collection of data about vehicles and their occupants on a massive scale - similar to that underlying mobile devices generally, but with more context and even more data.

---

77 http://www.mtc.umich.edu (May 12, 2014)
"There are hundreds of billions of dollars of economic activity that are enabled by the [connected] car, and it’s wide open."

"Every carmaker has invested copious amounts of money bringing electronics to their vehicles. It’s now less about the horsepower under the hood and more about the horsepower in the center stack of the dashboard."

Understanding the evolving industry ecosystem is important in order to appreciate how, where and why data about consumers flows or may flow among players. It is also important to identify entities that - if not custodians of data themselves - control the design of telematics technology or technological solutions. Such entities typically have choices as to whether and how to build privacy into the technology itself. Standards-setting bodies also play an important role in ensuring that new technologies and applications meet privacy standards and expectations.

---

1 Roger Lanctot, associate director at Massachusetts based consulting firm Strategy Analytics, quoted in Liza Barth, “How your car is tracking you”, Consumer Reports, July 22, 2014.

2 Mark Boyadjis, technology analyst for researcher HIS, quoted in Keith Naughton, “Cars are becoming increasingly important to the annual International Consumer Electronics Show”, <driving.ca>, Dec 29, 2014.

3 For example, the IEEE and Society of Automotive Engineers ("SAE").
carmaker is a wide and diverse array of vendors developing, manufacturing and marketing various devices, platforms and services that go into making Connected Cars work. As cars become fueled more by data than by gasoline, the central role of automakers is coming into question and a more collaborative industry environment based on data and intelligent machines is emerging.

According to one market report, “the global commercial telematics market was valued at USD 14.67 billion in 2013 and is estimated to grow at a CAGR of 18.0% during the forecast period from 2014 to 2020.”

There are hundreds of commercial entities playing, or vying for, a role in the marketplace for telematics-related goods and services. Automakers continue to take center stage, but behind - and beside - every
A lack of standards for much of the technology underlying Connected Cars (despite numerous industry efforts) has resulted in a highly fragmented market that is in constant flux. It has also created an opening for de facto standards-setters such as Google and Apple to lead the way in areas such as infotainment. Key players are those providing the operating systems, technology platforms and telecommunications networks on which telematics and infotainment services are delivered. Industry behemoths Google, Apple, Verizon and AT&T are becoming major actors in the Connected Car space, dramatically altering the industry ecosystem. Given their control over vast data warehouses and communications networks, these companies are wielding significant power in terms of the way in which Connected Car services are being offered now and will be offered in the future. Accordingly, automakers are treating these companies more as partners than as traditional suppliers. As the CEO of Verizon Communications Inc. is quoted as saying to the Intelligent Transport Systems World Congress in 2013: “The lines between communications, computing and content have come tumbling down. Now it’s time to shift into a higher gear.”

Categorizing players in the Connected Car industry by role is difficult because of the rapidly evolving marketplace and the fact that many players play multiple, often overlapping roles. Nevertheless, it is possible to identify broad categories of industry players.

THE PRODUCTION LAYER: AUTOMAKERS, THE AFTERMARKET AND INSURANCE PROVIDERS

Automakers

At the center of the industry are automakers who are increasingly incorporating telematics technology and infotainment services into their vehicles. Each OEM takes its own approach to the adoption of telematics and infotainment services. There are significant differences among brands and models, with high-end models typically on the cutting edge of new applications. General Motors (“GM”) was an early adopter of navigation systems with its “OnStar” service but other OEMs have quickly caught up and are challenging its traditional leadership in this area. Indeed, the rapid pace of development in the electronics and telecommunications industries compared with the long lifespan of vehicles (3-5 years to develop new vehicles, which then have a lifespan of 7-10 years) means that early adopters do not necessarily have the advantage in this industry. All major OEMs now have a Connected Car strategy that not only takes advantage of telematics but that involves offering models with some system for allowing drivers and passengers to continue to live their digital lives in the car. As industry analyst Thilo Koslowski notes:

“Automotive manufacturers and traditional suppliers that want to lead must extend product differentiation to create software-, service- and application-based value propositions in addition to mechanical engineering excellence. Technology leadership by automotive organizations is critical in creating the new era of smart mobility and the Internet of Cars, as part of the broader evolution of the Internet of Things (IoT).”

Telematics promises to lower OEM costs through, for example, the ability to update software remotely (and thus reduce recall and warranty costs) and the ability to engage in remote diagnostics (lower roadside assistance and repair costs). It also promises to generate new revenues for automakers and their dealers through the growing array of value-added telematics features that can be sold to customers. The revenue-generating potential of telematics does not end there: OEMs are being pressured to monetize customer data generated by their telematics systems, both through more effective internal analysis and use and by making it available to interested third parties such as advertisers, applications providers and data brokers. GM is on the cutting edge of this monetization with such services as its “AtYourService,” linking drivers with information and deals with merchants along their route. According to a January 2015 Detroit News report:

---

5 David Sedgwick, “Industry learns to share road with tech giants”, 15 September 2014, www.autonews.com
6 The following description of industry players and roles is based on research conducted in late 2014 and early 2015.
7 In Canada, automakers are represented by two industry associations: the Canadian Vehicle Manufacturers’ Association (representing the Canadian branches of Chrysler, Ford and GM) and Global Automakers of Canada (representing 14 other automakers who manufacture in Canada and/or import into Canada).
9 “BMW sounds alarm over tech companies seeking connected car data”, irishtimes.com, Jan.13, 2015.
“GM has said it sees many opportunities to boost revenue through connected vehicles by working with other companies in areas such as helping customers access fuel, parking, travel or hotel information. Some industry analysts see OnStar as a revenue boon for GM. In 2013, IHS Automotive estimated 4G LTE could add $400 million gross profit to GM by mid-decade.”

Automakers have a well-established supply network for components of their vehicles, and many of their traditional suppliers (e.g., Delphi, Harman) now provide telematics-related parts. But telematics has shaken the industry up in dramatic ways, such that OEMs are now partnering with entities such as Google, Apple, Verizon and AT&T – corporations with no significant history of involvement in the automobile industry, but with much more experience in managing customer data:

“Real-time dealer management, remote diagnostics, autonomous driving, cooperative routing and all the other connected-car services and solutions that are available today or will be tomorrow are all dependent on huge amounts of data, much of which will be personal.”

Not only is automobile hardware (e.g., dashboard, sensors) and software changing to accommodate telematics, but whole new types of inputs are now needed for cars to deliver telematics services to consumers. Data security and data analytics, rather than physical automobile design, are now considered

---

to be the biggest challenges facing OEMs. In this context, the need for automakers to address challenges such as “security, safety, regulation, lack of cross industry standards, widely varying industry dynamics and lifecycles, and limited initial addressable market sizes” is well recognized. Less appreciated is the need to make consumer privacy a design imperative, although some OEMs appear to be factoring it into their choice of technological solutions. (See “Industry Awareness of Privacy Concerns”, Chapter Five)

The goal of automakers is to sell cars and build brand loyalty with their customers. In today’s world, automakers are being pressured to deliver a product that not only meets consumer demand for safety, fuel efficiency and design, but that also allows drivers and passengers to stay connected with their digital lifestyles while in the vehicle. With the younger generation valuing internet access over car ownership, automakers are becoming increasingly service-centric, and looking to new revenue sources to fund the new digital services in which they are investing.

Carmakers have an advantage over other ecosystem players insofar as they can control access to vehicle data beyond the 213 OBD-II data points. While standardization of the OBD-II system went a long way toward leveling the playing field for pre-telematics vehicle diagnostics, OEMs now have the added advantage of being able to access this data remotely without the need to install a device in the vehicle. As one analyst noted:

“The era of the connected vehicle will help the automotive industry to redefine value propositions for its customers by going beyond realizing all profits at the point of sale when a customer purchases a vehicle. The ability to be connected and talk to a consumer while driving represents a unique and truly captive audience that other industries would love to have.”

But some new entrants to the industry such as Google, whose business model is based on data, could undermine that advantage if OEMs allow them access to vehicle data (see below, under Infotainment Platform Providers). While European and North American OEMs are treading cautiously in this area, China’s leading automaker, SAIC Motor Corporation, recently partnered with Chinese e-commerce giant Alibaba to deliver an “Internet Car” in two years. The Internet Car in development would use Alibaba’s Android-based operating system, navigation systems and cloud computing services. It is expected take advantage of Alibaba’s enormous and growing “cloud” of data on consumer online and offline activity to effectively integrate the internet with automobiles.

Gartner has predicted that by 2018, two automakers will have announced plans to become technology companies and expand their connected-vehicle value experiences to other industries and devices. By 2020, Gartner predicts that at least one auto company will derive 10% of its total revenues from connected mobility and service offerings.

Traditional OEMs, especially those that have chosen to offer their own embedded navigation and infotainment services and content (vs. those that have chosen simply to stream content via the owner’s smartphone), are not accustomed to their new role as custodians of sensitive personal data. On one hand, they see the potential for new revenue streams from this data and are under pressure to take advantage of the new data-rich environment they are enabling. On the other hand, they are aware of the challenges that data gathering and use poses from both privacy and security perspectives, and – in Europe and North America at least - are appropriately cautious about jumping into a wholly new industry in which they have no real experience. Now is the time to address the privacy challenge that the Connected Car presents by establishing clear and specific data protection standards for the automobile industry.

---

12 “Smart Car Innovation and Value Creation to Shift to the Boundaries between Automotive and other IoT Segments, According to ABI Research”, www.businesswire.com, June 18, 2014.
14 OEMs can also use intellectual property laws to try to prevent aftermarket players from accessing their proprietary systems: see “Ford Tries to Shut Down Independent Repair Tool with Copyright”, Jan.6, 2015, www.eff.com
Aftermarket

The automobile “aftermarket” industry comprises companies that manufacture, distribute and install automotive replacement parts, accessories, tools, and equipment independent of the OEMs. Aftermarket players include independent car dealers and repair shops, as well as companies that sell telematics products and services directly to consumers for installation in vehicles.

Independent Automobile Repair Shops

As OEMs build telematics functionality into their vehicles, the role of the independent garage could diminish. Of particular concern to the aftermarket sector is the use of telematics for remote diagnostics. With secure wireless communications systems, dealerships no longer need to physically plug a device into the vehicle’s OBD port in order to diagnose vehicle health (e.g., battery state, tire pressure, brake pad wear, engine health). Instead, they can obtain that information via the carmaker, monitor it remotely via their office computers and inform customers when their vehicles need attention. Without access to the same data other than via a special device that must be plugged into the OBD port, independent repair shops are at a significant disadvantage. This disadvantage compounds the disparity already existing as a result of the limited data available to the aftermarket via the OBD-II port.

The aftermarket sector is further concerned about OEMs using telematics to create a closed loop with their customers – for example, requiring that all repair or reconfiguration of telematics systems in the vehicle be done by the dealership, shutting independent repair shops out of that market opportunity. OEMs justify their closed proprietary systems on the grounds that secure vehicle communications are critical in order to ensure traffic safety: any compromise in that security could have fatal results. While no one disagrees that safety must take priority, there is concern that the need for secure communications could become a smokescreen for predatory commercial behavior at the expense of an important industry sector, not to mention consumer choice.

Aftermarket Telematics Service Providers

A number of non-OEM companies, from small start-ups such as Dash and Mojio to heavy-weights like AT&T and Verizon, are taking advantage of the existing market for telematics devices that can turn older model vehicles into Connected Cars. Mojio, a Vancouver-based company, offers a device that plugs into the car’s diagnostic port and pairs with smartphones to provide a variety of telematics-based services including vehicle diagnostics, real-time traffic reporting and directions, remote vehicle tracking and various other smartphone-based applications. Vinlii, Dash and Automatic are U.S. versions of the same plug-in device-based system with their own selection of applications that operate via the user’s smartphone. Dash, Vinlii and Mojio all operate open platforms for applications developers, hoping to attract new ideas for vehicle-based value-added services.

Verizon recently announced “Verizon Vehicle” in the U.S., a new telematics service that includes automatic incident alerts, emergency assistance, predictive diagnostics, maintenance alerts, roadside assistance, a mechanics hotline, parking tools and travel and repair savings. Like Verizon, many companies that supply to the aftermarket also supply to OEMs. Delphi, for example, sells “plug and play” telematics devices directly to consumers, while also supplying OEMs with infotainment and driver interface devices. Navigation device providers such as Garmin and TomTom sell aftermarket devices to consumers while at the same time supplying OEMs with built-in navigation systems. AT&T is partnering with numerous OEMs to provide connected car services while selling its own remote vehicle monitoring device, “Audiovox”, directly to consumers.

Insurance Companies

The growing use of telematics in automobile insurance is one of the strongest drivers for the commercial telematics market generally. Insurance companies seek to maximize profit by minimizing risk in the provision of their services. Generally speaking, they are interested in as much data as possible about applicants and claimants in order to assess risk and detect fraud. Usage-based insurance (“UBI”) is attractive to insurance companies for a number of reasons. In addition to more accurate risk assessment, the same telematics systems used for UBI can assist with fraud reduction, renewal retention, automated notice of loss (using data to detect signs of an accident in real time), improved accident investigations.

---

and liability determination based on recorded data such as speed and braking. Such benefits are for the most part not currently possible under current restrictions imposed by Canadian regulators, but may evolve over time.

Telematics also allows insurers to develop relationships with customers through the provision of value-added services such as the dashboard application that allow drivers to monitor their own behavior and improve their discounts. (Such aftermarket self-monitoring devices are widely available in the marketplace but many drivers may be unaware of this.) Other applications such as stolen vehicle tracking, vehicle monitoring and geo-fencing, emergency roadside assistance, fuel economy monitoring, and driver training programs are offered in other markets such as the UK and may be permitted in Canada in the future.

Automobile insurance is mandatory and highly regulated in Canada. It is provided by governments in three provinces (Manitoba, Saskatchewan and British Columbia).

Public insurers have different goals from those of private insurers: theirs is not to maximize profit, but rather to maximize the public good, which in the case of automobile insurance can be seen as improving traffic safety while ensuring equitable pricing and fair underwriting practices. So far, no public insurer has indicated a desire to offer UBI. However, two public regulators have permitted it. As of late 2014, six insurance companies offered telematics-based insurance products in the two provinces where it has been approved: The Cooperators, All State and the Canadian Automobile Association (“CAA”) in Ontario; Industrial Alliance in Quebec; and Desjardins and Intact in both provinces. Each of the six insurance companies uses a different telematics service provider, three of which - Baseline, iMetrik and Intelligent Mechatronic Systems (“IMS”) - are Canadian.

While insurers have so far operated separately from carmakers, relying on aftermarket devices to collect the data they need, OEMs are beginning to partner with insurance companies to offer this service directly. In early 2015, GM announced that it has partnered with Progressive Insurance in the U.S. to offer usage-based insurance to its OnStar customers.19

INTERMEDIARIES

Automobile Dealers

In between automakers and their customers are franchise car dealerships. Dealers are the customers’ point of contact when they purchase a new vehicle and, traditionally, the link between the automaker and the customer. Telematics has disrupted that link by allowing automakers direct access to vehicle data and customers remotely. Moreover, automakers contract directly with customers for Connected Car services, leaving dealers out of the loop. Even if OEMs do not let dealers in on the profits from connected services, aftermarket telematics products offer dealers tools to manage their inventory and opportunities to sell value-added services to customers.

Dealerships are separate legal entities from their associated carmakers. This is important as carmakers take no responsibility for the way in which their dealerships use customer data, including data which is shared by the carmaker with the dealer (e.g., for service or warranty purposes). In April 2014, a number of dealerships in the Vancouver area were found to have been scanning the drivers’ licences of people taking cars for test drives in order to build a database for marketing purposes, without telling customers, let alone giving them the option to refuse.20 A 2014 study of data brokers in the U.S. found that one of the many sources of data was automobile dealers.21

OEMs can share whatever data they wish with their dealers. If vehicle health data is shared, dealers could monitor their customers’ vehicles remotely and let them know when their tire pressure is low or their battery needs attention, for instance. Dealers can also use the vehicle data that the OEM shares with them to analyze their customers’ driving habits and customize their marketing. How much data OEMs share with their dealers and to what extent dealers take advantage of this data varies by automaker and has significant implications for customer privacy.

Automotive Financing Companies

Banks, OEM-affiliated financing companies and other entities that lease vehicles or loan money to car buyers

---

can use telematics devices to manage their assets or security. By attaching a telematics device to the OBD port, creditors can monitor the location of their vehicles, automatically inform customers of overdue payments and disable the ignition if payment is not made by a certain deadline, thereby significantly reducing delinquencies, improving on-time payments and repossessing vehicles with minimum effort.

**Insurance Brokers**

Insurance brokers act as intermediaries between consumers and insurance companies, helping their clients select appropriate insurance products based on their needs. Insurance brokers fear that proprietary telematics programs, frequently promoted as direct enrolment programs by insurers, will further exacerbate the trend of direct sales and bypass the broker entirely. They are also concerned that even if brokers are involved in the sales of such policies, they will not be able to access to customer data to the same extent as insurance companies.

Partially in response to this fear, the Insurance Brokers Association of Ontario (IBAO), through its subsidiary the Independent Broker Resources Inc. (IBRI) has announced plans to introduce broker-owned telematics products into the Canadian marketplace in the near future. IBRI has two proposed plans. The first, Ingenie, is a niche product for 16-24 year olds, offered in conjunction with a UK telematics broker. The second is a partnership with the UK-based technology vendor Quindell to create a general telematics offering that would give brokers access to client risk profiles in order to advise them on appropriate products and services. Both are yet to be approved. It remains to be seen what role, if any, insurance brokers will play in this industry ecosystem.

**Car Rental Agencies and Car Sharing Providers**

Both car rental agencies and car-sharing organizations use telematics to manage their fleets. Car rental agencies have been offering value-added navigation services to their customers for some time. In addition, they can use telematics in the same way that any fleet operator does – e.g., to track real-time vehicle location, obtain behavior-based alert information (speeding, acceleration and braking), vehicle usage behavior and vehicle diagnostic information. While telematics service providers advertise to rental car agencies, it is not known to what extent such agencies track customer use. As an indication, however, Hertz’s privacy policy states that it collects location data and “information regarding the vehicle or equipment rented and its operation during your rental” to, among other things, enforce our terms and conditions.” Hertz also lists as one of several sources of personal data “our in-vehicle or in-equipment technology or through other telematics devices”.

While currently a fringe service, car sharing is on the rise as younger generations appear to be less interested in car ownership than their forbears. For car-sharing, telematics is a key function that allows the service to operate efficiently (see “Car-sharing” in Chapter 3 - Applications).

**Comprehensive Telematics System Providers**

Several companies, including Ottawa-based QNX, US telecom giants Verizon and Sprint offer comprehensive integrated telematics and infotainment systems to automakers, drawing from the wide array of suppliers in areas in which they do not have expertise. Other companies provide similar systems integration services, effectively acting as general contractors for OEMs in the development, manufacturing and sale of connected cars. Wireless Car (owned by Volvo), UIEvolution (Toyota’s supplier), Airbiquity, and Tech Mahindra are examples of telematics platform providers that offer end-to-end services for OEMs to manufacture, market and service connected cars. Each system integrator has its own products, services or areas of expertise and draws on various technology partners for the remaining inputs.

For example, Airbiquity advertises its “Choreo” services as providing “connectivity, device integration, network access, and all the platform services you’ll need in an open, end-to-end connected car services solution...with global scalability, local adaptability, streamlined management and proven reliability...” The Choreo platform service includes (quoting from its website):

---

23 According to research recently conducted by Telefonica in Brazil, Germany, Spain, the UK and the US, 35% of consumers expect not to own their own car by 2034, and 53% of 18-34 year olds are interested now in participating in car sharing schemes: Telefonica, Connected Car Industry Report 2014, p.13.
• Subscriber Management (User and vehicle subscription management, billing payment);
• Content Delivery (Content acquisition, integration and dynamic updates);
• Application Management (Program and user application management by subscription level and user type);
• Speech Integration (System control via voice recognition and text-to-speech);
• Business Intelligence (Use, vehicle and platform data analysis and reporting);
• CRM (Business-to-consumer relationship marketing); and
• Private Cloud Model (Scalable multi-tenant cloud infrastructure).

THE SUPPLIER LAYER
At the base of the Connected Car industry are the many corporate entities that provide the necessary inputs for automobile telematics systems to operate. There are hundreds of suppliers of telematics-related products and services, from very small to very large in size, and from those that specialize in providing specific inputs to those that offer a range of products and services to the automotive sector. OEMs sometimes team up with competing suppliers for different kinds of services, keeping their options open while the industry sorts out which technology platform and connectivity approach will win out.

Critical hardware components including semiconductor chips, sensors and wireless modules are provided by numerous competing manufacturers including Qualcomm, Freescale, Intel and Bosch. The market for user interface devices is equally large, with numerous automotive suppliers such as Alpine Electronics, Harman and Pioneer competing. Niche software providers play an important role in the ecosystem, offering mobile software management (e.g., Red Bend), voice recognition (e.g., AT&T Watson), and Human Machine Interface (“HMI”) tools (e.g., Sencha Touch) among other services.

Short range mobile device connectivity for Connected Cars (e.g., Bluetooth, WiFi and Near Field Communications) is offered by numerous companies in addition to mobile network operators. Sierra Wireless and RACO Wireless, for example, offer solutions linking devices to enterprises via the “M2M cloud.”

Niche providers of particular telematics and infotainment services also form part of the industry ecosystem as direct or indirect suppliers to automakers, as well as suppliers to the aftermarket and to insurers. OEMs have a wide range of providers of telematics and infotainment services from which to choose. Advanced Driver Assistance Systems are offered by companies such as Continental and Nvidia. Navigation-related products and services are offered by numerous companies including Telenav, EnGIS, Inrix and Nokia HERE. Leading providers of audio services include Pandora, Spotify and Aupeo.

Telematics Operating System Providers
Connected Cars involve a myriad of devices, technologies, protocols, standards and user interfaces that pose an enormous challenge to automotive engineers. Embedded systems in particular require the integration of dozens of modules from multiple suppliers. The most ubiquitous operating system for Connected Cars is provided by QNX, an Ottawa-based software company owned by Blackberry. QNX works with dozens of technology partners to deliver software solutions for embedded automobile telematics, infotainment, hands-free systems, and advanced driver assistance among other things, running the gamut of Connected Car functionality. It offers either a complete software architecture or discrete modules, and provides services of some sort to virtually all OEMs (directly or via other telematics/infotainment system providers such as Delphi). In addition to offering its own complete infotainment platform, QNX provides the operating system for Apple CarPlay and is a partner in the MirrorLink consortium, both of which provide infotainment platforms for cars (see below).

In early 2015, Blackberry announced its new “IoT” Platform which, applied in the automotive sector, uses the QNX operating system and cloud services to deliver “a system for collecting and managing information between a vehicle and a customer’s back-end system. The platform provides a secure, hosted environment with the ability to collect data from vehicles, manage data flow intelligently, store data, and provide near real-time querying capabilities.”25

Until recently, Microsoft was a significant player in this part of the industry, powering the telematics and infotainment systems of Ford, Nissan, Fiat and KIA

with its Windows Embedded Automotive operating platform. While Microsoft has lost ground to QNX and infotainment giants Apple and Google, it continues to play a number of smaller roles. Many diagnostic tools are based on Windows PC technology, its search engine Bing is used by Wireless Car to deliver content to clients, and its Kinect video game technology is used by Toyota in automotive applications.

Linux unveiled its first open source “software stack” for the Connected Car in June 2014. “Automotive Grade Linux” is a collaborative project that, like other operating systems, allows automakers to create their own branded telematics and infotainment systems on a standard platform. Google’s autonomous cars operate on Linux systems, as do prototypes from GM and Volkswagen.

**Infotainment Platform Providers**

Several traditional OEM suppliers (as well as software architecture providers such as QNX) provide embedded automotive infotainment systems based on operating systems provided typically by QNX or Microsoft. These infotainment systems include features such as navigation, internet radio and video streaming, social media, networking and in-car WiFi, with voice recognition (hands-free operation) as a key component. However, most automakers including GM now appear to be deferring to Google and Apple’s market dominance in infotainment operating systems and are developing systems that accommodate both Android and Apple.

Apple’s release of its iOS-based “CarPlay” infotainment system in early 2014 caused major disruption to the Connected Car industry. Apple’s CarPlay offers hands-free and eyes-free operation of telephony, music and messaging via its Siri voice-recognition software, as well as satellite navigation via Satnav. Seeking to capitalize on the popularity of iOS products, numerous automakers quickly signed up with Apple to offer CarPlay in their vehicles.

At the same time, Google launched the “Open Automotive Alliance” initiative to develop standards for running Android phone-based infotainment in vehicles. Google’s foray into automobile infotainment systems has also attracted numerous automakers, many of whom are also working with Apple. Android Auto will offer the Google family of applications including Google Maps as well as other popular mobile services such as Spotify through in-dash display and controls. In addition, Google is expected to offer a growing array of vehicle-based applications that are being developed in response to its published application programming interfaces (APIs).

The move by tech giants Apple and Google into the automotive space is not surprising. Both companies have ambitions that go far beyond their origins in computers and internet search engines respectively, as well as their current dominance of the market for mobile device operating systems. Along with other connected devices, cars open up new potential revenue sources for both companies. While Apple may be focused on selling hardware and digital content, Google’s interest is likely in the new goldmine of consumer data that it can mine for targeted advertising purposes.

Although overshadowed by Apple and Google, there are three broad-based industry alliances developing open-source platforms for in-vehicle infotainment:

- **MirrorLink** is an initiative of the Car Connectivity Consortium (“CCC”) which was formed in 2011 to develop global non-proprietary standards for phone-centric car connectivity solutions. CCC has over 100 members covering over 80% of the world’s auto market and over 70% of the global smartphone market. MirrorLink allows drivers to control a nearby smartphone from the steering wheel or via dashboard buttons and screens.

- **Genivi** (“Geneva In-Vehicle Infotainment”) is a Linux-based system that counts GM, PSA/Peugeot-Citroen, Renault-Nissan, Hyundai and BMW among its members, as well as dozens of hardware, software and service suppliers. Genivi’s platform focuses on the core system requirements, leaving user interfaces to the domain of vendors who can distinguish their products as they wish.

- **A third initiative, Webinos, is a collaborative industry project with the goal of designing a secure application platform with web components based on open standards and open-source software that can be deployed in vehicles as well as mobile devices, PCs and TVs.**

Whether embedded in the vehicle or delivered via smartphones, infotainment services do not require access to vehicle diagnostics or operations: all that is needed in the vehicle is an interface that projects the phone-based interface on a screen built into the car dashboard. Infotainment systems are therefore typically separate from the vehicle’s telematics systems. Indeed, CarPlay, Android Auto, GenIVI and MirrorLink systems are all device-centric.
However, Google is apparently working with GM on an Android-based infotainment system that will be embedded into vehicles and thus more than simply a mirror for smartphone applications. The system would make online services available to drivers without having to plug in their phone or ensure that their phone batteries are charged. Not only would this be attractive to Android-using drivers, it could give Google access to detailed data about drivers and vehicles to feed into its data-hungry advertising business model. Google is also reported to be in discussions with car manufacturers on ways it can assist with telematics-related functions such as accident avoidance, emissions and efficiency of transport routes. As carmakers partner with Google to advertise online and improve sales, they are more likely to extend those partnerships in ways that benefit Google.

Some OEMs are publicly resisting Google’s move to gain access to vehicle and driver behaviour data. Responding to the leak about Android Auto systems being linked with vehicle systems, Audi Chief Executive Officer Rupert Stadler is quoted as saying: “The data that we collect is our data and not Google’s data. When it gets close to our operating system, it’s hands off.” Stadler echoes comments from the CEOs of Volkswagen and Daimler. German politicians also expressed concern about the country’s automobile industry becoming dependent on companies like Google.

Carmakers nevertheless remain in control of what services are offered via their vehicles. In particular, they can limit which apps are available via their infotainment systems, and can justify such limits on the grounds of safety. This legitimate concern about safety and driver distraction makes OEM infotainment services less vulnerable to disintermediation by Apple and Google than, for example, mobile carriers.

Mobile Telecommunications Network Operators

Telecommunications operators are major players in this industry as they control the networks over which much of the data flows. As a 2013 industry report noted, automobile telematics offers telecom operators “an opportunity to claim the only hours in the day still largely out of reach of broadband”. Moreover, it is predicted that annual mobile data usage generated by Connected Cars will grow by 188% over the next five years. It is recognized that the two industries, automotive and telecommunications, need to work closely together to surmount the problem of widely different product lifecycles and deliver seamless services to consumers.

But big telecom operators such as Verizon, AT&T and Sprint have quickly become more than mere pipeline providers. They now offer other back-end services such as content and application integration, subscription management and billing, network security and user authentication and customer support, as well as Connected Car services themselves (e.g., on-demand infotainment, navigation, remote diagnostics, safety and security). Indeed, all three telecom giants now offer comprehensive end-to-end telematics/infotainment solutions for OEMs. Verizon currently operates telematics services for Mercedes-Benz and Volkswagen while Sprint provides Connected Car services for Fiat Chrysler Automobiles (“FCA”), and Honda/Aeris. The Privacy Policies for each service apply equally to the OEM and Verizon or Sprint. As for AT&T, it is providing connectivity for several OEMs including OnStar and is seen as an industry leader with its “AT&T Drive Studio”, a 5,000 square foot research facility in Atlanta dedicated to Connected Car research and development.

In 2012, Verizon acquired Hughes Telematics Inc., a

---

27 “Germany’s top car companies don’t want Google in the driving seat”, www.bloomberg.com (Dec.22, 2014).
28 A number of OEMs have partnered with Google to drive online sales: www.thinkwithgoogle.com/industries/automotive.html, accessed Jan.19, 2015.
30 Ernst & Young, The quest for Telematics 4.0: Creating sustainable value propositions supporting car-web integration, 07 Jan 2013, Executive Summary, p.5.
31 Telefonica, Connected Car Industry Report 2014, p.26
33 Verizon Telematics was created after Verizon purchased Hughes Telematics in July 2012. AT&T promotes its “AT&T Drive” modular solution to carmakers, while Sprint offers a connected vehicle platform called “Sprint Velocity”.
major supplier of telematics and infotainment systems for vehicles. Verizon now plays multiple roles in the Connected Car ecosystem, including most recently the role of aftermarket telematics provider with its ground-breaking product, “Verizon Vehicle.” Targeting the over 200 million unconnected vehicles currently being driven in the U.S., Verizon’s device-based service will offer nation-wide roadside and live agent emergency assistance using GPS locating technology, automatic crash notification, remote diagnostics and mechanic hotline, maintenance alerts, and smartphone-based tools to help drivers find parked cars as well as keep track of how much time is left on the meter. AT&T also offers an aftermarket telematics product, Audiovox Car Connection, that allows users to track their vehicles, and get notices, safety alerts, diagnostic reports, trip summaries, and other driver feedback.

Canadian mobile network providers, in contrast, are just beginning to engage in the industry. Bell Canada and Rogers Communications were participating with other mobile operators and automakers in the GSMA’s “Connected Car Forum” as of May 2013. As of January 2014, Bell had made no announcements regarding Connected Car services but had opened a “M2M Management Centre” offering businesses “a comprehensive suite of tools to manage connected devices across their operation.” In September 2013, Rogers Communications announced a deal with Sprint under which automakers deploying Sprint Velocity in Canada will use Rogers’ wireless networks. Rogers also provides roaming services in Canada for AT&T’s LTE-enabled smartphone customers, but it is not clear whether this extends to OnStar or other AT&T-enabled Connected Car services. Nor is it clear which Canadian wireless provider is providing the infrastructure for Verizon’s connected car services in Canada. Of note is that Telus is partnering with Mojio to connect Canadian vehicles with the internet via the Mojio device (AT&T is providing Mojio’s connectivity in the US).

In any case, telecom operators are taking advantage of new business opportunities presented by the growth of Connected Cars, and are being encouraged by industry consultants to, among other things, “leverage data collection and mining capabilities to support carmakers.”

Data Analytics

Of particular relevance to this study are data mining and analytics services available to automakers and others. Telematics involves the generation and management of the huge amounts of data that automakers and others can leverage through predictive analytics. Data analytics services are becoming increasingly important elements of the Connected Car ecosystem as automakers and other players seek to maintain or improve profitability through insights gained from data generated by Connected Cars. The ability to gather, process and link data originating from various sources in order to generate useful insights is now recognized as a key skill that automakers of the future will require. Not surprisingly, OEMs are now hiring data analytics experts to help them “better anticipate consumers’ wants and needs” with a view to corporate profitability.

Data analytics services are offered by numerous companies including Agnik, Wipro, Cloudmade and Symphony Teleca, as well as well-established data management experts such as IBM and Cisco. Apple may be looking to offer more data analytics services to OEMs, having in 2013 acquired social media analytics provider “Topsy Labs”, which specializes in analyzing data from Twitter feeds and other sources to track consumer commentary and feedback for enterprises.

Google is of course a global leader in this field, but it remains to be seen how it will leverage its data analytics expertise in the Connected Car space. In contrast, Chinese e-commerce giant Alibaba has been clear about its intent to take full advantage of Big Data and computing capabilities in the automotive space. Reflecting its core business, Alibaba’s focus is not just on delivering customized in-car infotainment but extends much further to cloud computing and predictive data analysis. Having recently acquired China’s leading web-based mapping service AutoNavi,
music website xiami.com, launched virtual network operator Ali Telecom, and begun permitting online car purchases via its payment tool Alipay, Alibaba is positioning itself to become a major force in the Chinese automobile industry. It will do so using data generated not just by the Connected Car and its occupants but also by its enormous and growing e-commerce empire. Through its Online-to-Offline (“O2O”) data gathering and predictive analysis, Alibaba intends to provide detailed insight into the habits, preferences and likely interests of actual and potential OEM customers.  

As one commentator noted, with its retail/ecommerce base and data analytics capabilities, Alibaba “is definitely poised to make greater inroads into areas like customer behavior analysis, loyalty and CRM-focused applications. Alibaba, with clout and money, could buy several Connected Car players and create a truly connected platform with multiple apps, services. In doing so, it would, shift the focus from a niche Carplay-type offer to a much broader connected platform over the vehicle life cycle.” The same holds true for Google if automakers and regulators in North America and Europe allow it.

THIRD PARTY INTERESTS

Outside the telematics industry itself are a number of third parties with a strong interest in the data being generated, or capable of being generated, by telematics systems. These include local retailers and merchants, online advertising agencies, databrokers, application developers, private investigative bodies, and law enforcement agencies, among others. Any of these may partner with OEMs or aftermarket telematics service providers for the purpose of gathering data for their own use. Where corporate affiliations exist, data sharing is even more likely.

CONCLUSION

The Connected Car Ecosystem is in a state of constant flux as new technologies and applications are unveiled annually and non-traditional industry players such as Google and Apple enter the market. All of the corporate entities in this ecosystem are driven by the goal of profit-making. While some are content to deliver a specific type of product or service, others are looking for new revenue streams and see great potential in this respect from data generated by the various components of Connected Cars. Telematics is playing an increasingly important role in the automotive sector and is creating opportunities for these new players that could well turn the industry on its head as value propositions shift from the physical car to the data it produces. According to one industry commentator,

“The balance of power in the connected car space is shifting from B2C revenue-generating value proposition, including areas like software licensing, ads and services, to more long-term customer retention, focused on where the revenues and benefits will be generated at a B2B level within the OEMs.”

In other words, customer data is itself a commodity. Who owns the data produced by telematics is a key question, as automakers begin to see the potential new sources of revenue from the use of this data and the predictive insights it can generate to marketers, insurance companies and even governments. Which of the many companies involved in the operation of telematics and infotainment services will have access to data generated by the car, and under what circumstances will such data be made available to third parties?

The role of companies involved in the manufacture of Connected Cars and the components going into them is also important. To what extent can and will they design privacy into the vehicle software and services so as to limit data use and sharing from the outset?

CONNECTED CAR ECOSYSTEM

BIG DATA

Data Hosting and Analytics

External Data Sources

Third Party App Providers
Operating System Providers
Device Manufacturers

Aftermarket Telematics Service Provider

Call Centre

Automaker and/or Connected Car Service Provider

Insurer

Telecom Network Operators
Third Party App Providers

Mobile Device Operating System Providers

Lender
Dealer

CAR + owner / driver / passengers

Independent Repair Shops

Intelligent Transportation Systems
“Connectivity is gradually turning automobiles into highly efficient data harvesting devices.”

“...more than 480 terabytes of data will be collected from the OEM connected car landscape in 2013 through millions of small data transmissions sent through more than 26 million connected cars. 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 30 terabytes of data [will] be collected each day from the 152 million connected cars on the road in 2020, or about 350 megabytes per second, compared to about 15 megabytes per second in 2013.”

“Everyone is looking for another stream of revenue, and data is our next stream.”

---


3 Fred Cate, director of the Center for Applied Cybersecurity Research at Indiana University, quoted in Liza Barth, “How your car is tracking you”, Consumer Reports, July 22, 2014.
The Connected Car runs on data – data about vehicle operations, driver behaviour, vehicle location, and increasingly, data about drivers themselves: their identity, communications, contacts, schedules, destinations, content choices, service preferences, and even their personal health. It is entirely possible, as Ford’s Global VP of Marketing and Sales famously admitted in a panel discussion at the 2014 Las Vegas Consumer Electronics Show, for an automaker to monitor each of its customers’ driving habits and vehicle-related activities - to know “who breaks the law”, “when you’re doing it”, and “what you’re doing” with the vehicle.4 This was made disturbingly apparent some months earlier when the CEO of Tesla publicly rebutted an unfavourable review of the Tesla Model S car by a reporter who had taken it for a test drive by referring to detailed data that Tesla was able to access about the reporter’s location, energy usage, speed, temperature and other control settings.5

Mobile phone service provider Verizon trumpets the granularity of its data and its ability to detect where, when and for what purpose a customer is travelling, or in what context they are viewing certain content on their handset.6 Just as Verizon gathers and sells “anonymized” information about its customers’ “daily activity streams”, automakers and others gathering data from Connected Cars can engage in focused profiling of their customers – but with even more data coming from the vehicle. And even if they don’t themselves mine the data for insights useful to customer relationship management (“CRM”) and marketing, any such data collected and retained in the carmaker’s computer systems is vulnerable to unexpected uses by those to whom it has been entrusted as well as by third parties who gain access to it.

As mobile hotspots, connectivity and infotainment providers, cars are analogous to today’s smartphones and other mobile devices, raising the same concerns about data privacy. But as generators of data about vehicle operations and use, not to mention vehicle-based biometrics and health monitoring, automobiles offer a whole new universe of telematics data that can be fed into the analytics machine to produce insights into individual consumer behaviour, preferences, and vulnerabilities. This is part of what sets them apart from mobile devices and other data-generators in the Internet of Things, and justifies special focus on the Connected Car from a policy perspective.

While Ford later clarified that it does not in fact track individual customers in the way that its VP’s now famous comments suggested, the technology allows Ford and its partners to do just that. Even aftermarket providers and third party application providers are now technologically capable of gathering and making use of vast amounts of data via telematics devices and Connected Car services that can reveal intensely private details of a person’s life. Corporate ethics and industry codes of practice are helpful, but only our laws, ultimately, can protect us from privacy-invasive uses of technology that are seen as commercially advantageous.

**TELEMATICS VS. INFOTAINMENT DATA**

Telematics and Infotainment services generate different types of data: telematics systems produce data primarily about vehicle operations (e.g., fuel efficiency, engine failures, brake pad wear), driver behaviour (e.g., acceleration, speed, braking) and, with GPS units, vehicle location at any given time. They can also incorporate biometric sensors to identify or monitor individual drivers and adjust vehicle settings or operations accordingly. Telematics systems are also used to send automatic notifications to emergency call centres in the event of a vehicle crash and to facilitate voice communications with roadside assistance.

Infotainment systems, in contrast, generate data about the information and entertainment content choices of system users, their use of mobile applications and concierge services, their web browsing activity, social networking, voice, text, and email communications from the car. Infotainment systems can also gather and store data about the user’s contacts and personal calendar.

Increasingly, telematics and infotainment services are merging as new applications are developed to take advantage of vehicle data (e.g., location, speed) in the provision of information and communications services to drivers. Location data in particular is central to many new applications (e.g., automatic texting

---

5 http://www.teslamotors.com/blog/most-peculiar-test-drive. The New York Times rebuffed Tesla’s claims and defended its reporter’s story as “fair and accurate”.
of one’s estimated time of arrival). Sophisticated infotainment services can include automatic functions or adjustments based on certain vehicle operations (e.g., ignition, door unlocking, engine noise). It is up to each carmaker to decide whether, to what extent and how to integrate its infotainment system with its telematics system.

**DATA SENSITIVITY**

Although any piece of data associated with an individual could, depending on the context, be sensitive, in general, different types of data present different sets of privacy risks.

**Identification data** is data that exists in order to identify a particular individual (e.g., subscriber) or a device that can be linked to a particular individual. All cars have Vehicle Identification Numbers (“VINs”) that link to the registered owner of the vehicle, and all car dealers collect identifying information from their customers, and share it with the manufacturer. Connected Cars may use a number of additional identifiers: unique mobile device identifiers, SIM card numbers for voice and data connectivity, MAC addresses for Wi-Fi hotspots, and possibly RFID serial numbers for toll or other systems using that technology. Each of these identifiers links to the particular vehicle or to a particular individual for billing purposes. In addition, Connected Cars typically process telephone numbers, IP addresses and additional registration data for use by occupants of the public telephone network, internet and third party applications respectively. Some automakers are also developing biometric sensors that can identify individuals who enter the vehicle in order to personalize the driving experience.

These identifiers allow automakers and their systems providers to link data on vehicle health, driver behaviour, location and infotainment use with particular account-holders, putting them in a position to build detailed profiles on each vehicle and/or user.

**Customer Account Data** is information about customers kept on an internal customer account file by the dealer and manufacturer. Such data typically includes name, address, telephone number, date of purchase or lease, selling dealer, make and model of vehicle, VIN, license plate number, details of any trade-ins, details of service and repair at the dealership.

It may also include additional data provided by the customer through test drives, OEM websites, surveys, contests, or other promotions. It can further include “information which enables us to offer you products which better meet your needs including demographic such as age, education level, occupation, marital and family status, purchase preferences and interests.” It may also include financial and credit information shared by the OEM’s affiliated financing company. Because they are providing an ongoing service, Connected Car service providers also require subscriber billing information (e.g., credit card or bank account numbers). In addition, they typically require details about the mobile device(s) used to access the service such as cell phone number, device type and operating system. Customer account data includes identification data (above) and forms the basis of customer profiles that OEMs can use for secondary purposes such as marketing.

**Vehicle health data** is data generated by the vehicle’s internal system about the performance of all the various components of the vehicle: engine, transmission, brakes, climate control, safety restraints, tire pressure, etc. It is used for vehicle diagnostics and most telematics applications. While such data would seem to be non-personal data, it includes the VIN which is linked to the registered vehicle owner. Unless truncated, the VIN can thus be used to turn otherwise non-personal vehicle data into personal data (ie: vehicle data linked to an identifiable individual). The U.S. National Highway Transportation Safety Administration in its assessment of V2V communications technology has recognized that such data has privacy implications for individuals. If access rights are not strictly limited, for example, it could be used for state monitoring of compliance with emissions or safety regulations. The security of such data is also critical: the potential for physical damage as a result of malicious access to vehicle electronic systems is enormous (see below, under Security Risks).

**Driver behaviour data** is data about how and when the driver is operating the vehicle. This includes a subset of the data generated by the vehicle internal system: e.g., vehicle speed, acceleration, direction, braking, cornering, ignition, door locking. The disclosure of such data can have serious consequences for drivers and vehicle owners, such as in the context of accidents when facts regarding the vehicle’s speed, direction or acceleration can be critical. Computer-generated data
<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>Vehicle Health</th>
<th>Driver Behaviour</th>
<th>Location</th>
<th>Biometrics &amp; Health Data</th>
<th>Communications*</th>
<th>Info-tainment*</th>
<th>REVEALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Crash Notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Event details</td>
</tr>
<tr>
<td>Emergency Assistance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Event details</td>
</tr>
<tr>
<td>Roadside Assistance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Event details</td>
</tr>
<tr>
<td>Concierge Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal life; Interests</td>
</tr>
<tr>
<td>Remote Vehicle Diagnostics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Vehicle health</td>
</tr>
<tr>
<td>Fleet Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how driving</td>
</tr>
<tr>
<td>Usage-based insurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how driving</td>
</tr>
<tr>
<td>Auto Financing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where driving</td>
</tr>
<tr>
<td>Rental Cars</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where driving</td>
</tr>
<tr>
<td>Car Sharing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where driving</td>
</tr>
<tr>
<td>Electric Vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how driving</td>
</tr>
<tr>
<td>Remote Convenience Apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how using</td>
</tr>
<tr>
<td>Remote Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how driving</td>
</tr>
<tr>
<td>Navigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where driving; Personal Life</td>
</tr>
<tr>
<td>Traffic/Parking Apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When, where, how driving</td>
</tr>
<tr>
<td>Destination/local search</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal Life; Interests</td>
</tr>
<tr>
<td>Geo-fencing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Where, when driving</td>
</tr>
<tr>
<td>Location-Based Advertising</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Where, when driving</td>
</tr>
<tr>
<td>Stolen Vehicle Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hands-free voice &amp; data communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal Life, Interests, Social Circle, Contacts</td>
</tr>
<tr>
<td>Contacts, Calendar</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal Life; Contacts</td>
</tr>
<tr>
<td>Music, radio, books, podcasts, videos, internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal Preferences, Interests, Values,</td>
</tr>
<tr>
<td>Health monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal Health; Interests</td>
</tr>
<tr>
<td>ADAS - Biometrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Personal health; Driving habits</td>
</tr>
<tr>
<td>ADAS - Interior Cameras</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Occupants, activities in car</td>
</tr>
</tbody>
</table>

**TYPE OF DATA USED BY APPLICATION** This is a simplified portrayal of common data collection and use by application. Many applications combine functions and therefore use more data than shown. Applications may also be designed to use less data than shown. Telematics technology permits, and competition in the development of applications encourages, additional data uses.

* on-demand radio, music, video, other content, web browsing, internet-based applications
* voice, text and email communications, social networking, contacts and schedule
is likely to be treated as more reliable than witness testimony, and it will be difficult to challenge. Some drivers may prefer not to report minor accidents to their insurance company but rather pay any repair costs themselves – however telematics could deny them that option. Concern about such privacy risks is one reason for the decision by Canadian insurance regulators not to allow the use of telematics to deny coverage or charge higher premiums. Similar concerns have led to laws in the US restricting access to Event Data Recorder information (see next chapter for more specifics of these laws). Automakers themselves have recognized the highly sensitive nature of driver behaviour data.9

**Biometric and Health data** is information gathered by biometric or health monitoring devices in or linked to the vehicle. Such data can be used to identify individual drivers or vehicle occupants and/or to report on body signs such as heartbeat or head and eye movement. This information is clearly sensitive and has potential consequences for individuals who may have legitimate desires to remain anonymous in a given situation (such as a personal trip to the pharmacy or a political gathering), or to keep their personal health data out of the hands of others such as insurers.

**Location data** is data about the precise vehicle location at any given time. It is generated by GPS modules that typically form part of both the vehicle telematics and infotainment systems, and is used for numerous applications. It is often combined with vehicle data such as speed or direction (to provide navigation services) or with information requests (e.g. local point-of-interest searches). Location data is particularly sensitive because it can reveal intimate details of a person’s private life, such as the fact that she is playing hooky from work, interviewing for a job with a competitor, participating in a protest, or visiting a medical clinic. When tracked, location data paints a highly intimate picture of a person. Such data can be used to embarrass or blackmail a person, to stalk individuals, to steal identities, to facilitate robberies, or to create a profile that can then be used by commercial entities in unexpected ways, including to target advertising to that person.10 Automakers have also recognized the sensitive nature of location data.

**Personal Communications (voice, text, email, social networking)** data is generated by individuals in the vehicle and sent or received via the in-car infotainment system. Even systems that rely on the user’s smartphone for connectivity and intelligence receive and transmit data via the car’s human-machine interface (usually a screen in the dashboard), and are therefore capable of gathering and storing information about a person’s communications to and from the vehicle.

As a society, we treat unauthorized interception of communications as a criminal offence, reflecting the high value we place on the privacy of our personal communications. Yet Connected Car systems allow for the constant monitoring and gathering of our communications by automakers and their service providers under the guise of consent. For example, voice communications between car occupants and call centres or interactive voice recognition systems may be recorded, if only for purposes of “quality assurance.” But some Connected Car systems go further: one privacy policy states: “we and our Service Partners and the [OEM family of companies] may intercept any wire, wireless, oral or electronic communications made or transmitted through the Service, at any time and for any reason.”11

Communications are comprised of metadata (time, date, origin, destination, duration, network subscribed to, and other “envelope” information) as well as the voice, text, email or social networking message itself. Given how much it reveals about us, communications metadata is, like the communication itself, very sensitive and vulnerable to abuse if accessed by persons other than those for whom the communication was intended.12 Yet metadata of the various kinds of communications sent and received over Connected Car systems may be gathered, stored, and used by service providers for their own purposes, again, under the claim that the customer has given their consent.

---

12 For an analysis of the privacy interest in metadata, see Office of the Privacy Commissioner of Canada, Metadata and Privacy: A Technical and Legal Overview, October 2014.
It should also be noted that most services involve the use of cell phones or other remote devices, in which case the service provider typically collects information about the device, IP address, browser type, and internet service provider as well.

**Personal Contacts and Schedules** are capable of being stored by some infotainment systems, in order to offer customers greater convenience as they continue to live their digital lives in the car. Personal contacts are, like communications data, highly sensitive as they reveal the people with whom one associates and can lead to prejudicial assumptions about a person. A person’s daily schedule is also highly sensitive – imagine its value to a stalker! For those in the marketing business, contacts and schedules provide extremely useful information about their targets.

**Infotainment data** is generated by the infotainment system and includes users’ choice and use of music, radio, audiobooks, podcasts, backseat videos, internet sites and mobile applications accessed via the car. Connected Car systems gather information about the customer’s use of the vehicle’s features and systems, including functions used, search content, areas of the service visited and online activities over time. Such information can be highly revealing of an individual’s personal life, values, interests, and preferences, and is obviously sensitive given how it can be used to profile, target and discriminate among individuals in unacceptable ways.

**PRIVACY RISKS**

Connected Cars are a source of new and highly valuable data about individuals. The breadth and depth of information that can be culled from Connected Cars is significant and goes beyond the data already available to mobile device operating systems and mobile network providers. The value of this data to automakers and others is enormous, as senior executives from the Connected Car industry confirmed in a 2013 roundtable event, summarizing a key finding as:

“**Data as the key currency** — Dealers, insurance companies and retail stores would all be interested in utilizing data generated from telematics to redefine their own business propositions. The ecosystem needs to resolve issues of data portability and ownership (including privacy), as well as system investment, to create sustainable offerings.”

But the privacy risks entailed with collecting this kind of data and the surveillance that it enables – by corporations and governments - are well-documented. Connected Cars present unique privacy risks, not only because of the context in which data generated from the vehicle or its users is situated, but also because of the additional data that Connected Cars generate. As such, Connected Cars hold the potential for profiling, monitoring and making decisions about individuals based on data generated from various sources in the vehicle.

---

Cumulative data and the power of data analytics

While the collection and use of a given piece of personal data can have devastating consequences for the individual depending on context, the risks arising from cumulative or combined data about one’s vehicle use are much greater. As privacy scholar Daniel Solove has pointed out, the privacy risks arising from Connected Cars go beyond individual instances of use or abuse:

“In many instances, privacy is threatened not by singular egregious acts but by a slow series of relatively minor acts, which gradually begin to add up. In this way, privacy problems resemble certain environmental harms, which occur over time through a series of small acts by different actors.”

Separately, each piece of data about a person’s vehicle use, driving routes and destinations, or use of in-vehicle communications and infotainment services reveals something about that person. Combined or accumulated over time, such data – even if each piece seems innocuous in isolation - becomes highly revealing. It can divulge the identity of an otherwise unidentified person, as well as that person’s habits, routines and social circle. It can be used to ascertain the person’s religious and political associations. It can show when a person deviates from their normal routine, develops a health problem, or engages in activities that, if known, could harm their reputation.

As the US Court of Appeals stated in United States v. Maynard:

“It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person’s hitherto private routine....

“The sequence of a person’s movements can reveal still more; a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.”

Knowing when, where and how a person uses her vehicle is to know even more details of that person’s private life. In addition to the person’s location at any given time, it discloses the fact that they are in a particular vehicle. It further discloses highly specific data about how the vehicle is being driven – fast or slow, hard or gentle stops, hard or soft acceleration. If passengers log into the car’s hotspot, it can be determined who was with the driver at that time. With interior cameras and/or sound recording capabilities, information on occupants and activities in the car can also be recorded.

It is precisely this kind of information that feeds the business of data analytics and targeted marketing, and that, especially when aggregated with other data, offers the kinds of “actionable insights” that corporations thrive on. In the context of sales and marketing, data analytics is all about customizing the pitch to the individual, based on as much detail as possible about that person’s preferences. In the context of Connected Car service provision, it is increasingly about personalizing the experience so that the car recognizes the driver, adjusts settings accordingly, and can predict where the person is going and what they want to listen to in the vehicle.

Data analytics takes aggregate data about consumers and combines it in ways that reveal particular things about individuals (e.g., our habits, preferences, interests, social circles) that the individual might wish to keep private. On the basis of aggregate data, analytics can then make remarkably accurate predictions of individual behaviour, allowing corporations (or governments) to categorize individual consumers by behavioural profile and target them for marketing or other purposes. This is the Google model that has now become standard in the marketing industry. It is considered by industry to be a “legitimate business practice” that consumers understand and

---


accept, such that it requires no express informed
consent on the part of individuals and can be forced
on unwilling consumers even where not necessary for
the service in question. As Daniel Solove points out:

"People expect certain limits on what is known
about them and on what others will find out.
Aggregation upsets these expectations, because it
involves the combination of data in new,
potentially unanticipated ways to reveal facts
about a person that are not readily known. People
give out bits of information in different settings,
only revealing a small part of themselves in each
case. Indeed, people selectively spread around
small pieces of data throughout most of their
daily activities, and they have the expectation that
in each disclosure, they are revealing relatively
little about themselves. When these pieces are
consolidated together, however, the aggregator
acquires much greater knowledge about the
person’s life."17

Risks of Over-Collection

Personal data that is collected unnecessarily - and
worse, stored unnecessarily - creates a range of
privacy risks including vulnerability to security
breaches, to malicious access and use, to state
surveillance, and to other unexpected and undesired
uses by both the entity collecting and/or storing the
data as well as third parties who gain access to it. This
is why a fundamental principle of data protection law
is that the collection of personal information must be
limited to that necessary for the purpose for which it
was collected.18

Security Risks

The more data gathered and stored in databases,
cloud-based or otherwise, the greater the potential
damage from inevitable security breaches. According
to Symantec, there was a 62% increase in the number
of data breaches in 2013 compared with 2012, resulting
in the exposure of over 552 million identities, with	

"The size and scope of breaches is exploding, putting
the trust and reputation of businesses at risk, and
increasingly compromising consumers’ personal
information – from credit card numbers and medical

WHAT IS “PERSONAL DATA”?

“Personal data” in the context of privacy is data
about an identifiable individual. How difficult or
tenuous the association must be in order to take the
data out of the realm of “personal data” is debatable,
but it is widely accepted that data is “personal” even
if it doesn’t identify an individual per se, as long as
it can be associated with an individual without too
much difficulty.

The association need not be accurate for the
information to be “personal”. Associating data with
individuals has privacy consequences whether it is
accurate or not. Targeted marketing can be just
as unwelcome when based on inaccurate data
about a person. Decisions based on inaccurate data
associations can have reputational consequences.
And in cases where accuracy of identification is
important, making a link from the initially identified
individual (e.g., vehicle owner, registered user) to the
actual driver or user is usually not difficult to do.

It is commonly thought that vehicle health data is not
personal information – after all, it’s about the vehicle,
not an individual. But one of the 213 data points
universally available via the OBD-II port is the Vehicle
Identification Number (“VIN”), and a VIN can always
be associated with the registered vehicle owner. As
long as the vehicle owner is an individual, vehicle
information that includes the VIN is therefore almost
invariably “personal data”.

records to passwords and bank account details. Each
of the eight top data breaches in 2013 resulted in the
loss of tens of millions of data records. By comparison,
2012 only had a single data breach reach that
threshold.”19

A recent study of cybersecurity vulnerabilities in
Canada found serious deficiencies: 56% of 236 senior
IT and IT security professionals surveyed do not
think their organization is protected from advanced
cyber attacks and 59% doubt they can stop the
exfiltration of confidential information. Over one-third
of the companies represented in the research had
experienced one or more substantial cyber attacks in
the past year.20

---

17 See next chapter on data protection law.
8, 2014.
19 Ponemon Institute, Exposing the Cybersecurity Cracks: Canada; Part I: Deficient, Disconnected & in the Dark, June 2014;
“AGGREGATED”, “DE-IDENTIFIED” AND “ANONYMOUS” DATA

It is common for automakers and other service providers to treat “aggregated” data about consumers as non-personal information and therefore not subject to privacy laws or policies. Such data, from which personal identifiers have presumably been removed, is variously referred to in privacy policies as “aggregated”, “de-identified” and “anonymous” data, but without any definition of terms. All automakers, insurers, aftermarket providers and others whose privacy policies we examined in the course of researching this report reserve the right to aggregate their customer data and to do as they wish with the aggregated data on the grounds that it does not identify individuals. But none clearly state that the aggregation is done in such a way as to render re-identification statistically impossible.

Treating aggregated data as anonymous per se and therefore presenting no privacy risk is misleading. It ignores the fact that aggregated and de-identified data can often be associated or re-identified with individuals, sometimes with ease. Indeed, that is the very power of data analytics: the ability to cross-reference and correlate data so as to reach conclusions or make inferences that are not otherwise possible. Cross-referencing aggregated datasets with other available data can effectively re-identify individuals whose data was supposedly anonymized. Several studies have proven that supposedly anonymous data is actually not anonymous.

For example, in 2006, Netflix released 100 million supposedly anonymous movie ratings in a contest, inviting people to improve Netflix’s algorithm for predicting how a subscriber would rate other movies. Just 16 days later, two researchers announced that they had identified some of the “anonymous” subscribers by matching their movie reviews with data from other sites. The researchers were also able to reverse-engineer the Netflix data to find out a person’s viewing history.21

MIT researchers recently published the results of a study of 3 months worth of credit card “metadata” (i.e., large scale datasets of human behaviour, stripped of individual identifiers) for 1.1 million people. They found that four spatio-temporal points are enough to uniquely re-identify 90% of individuals. They further found that knowing the price of a transaction increases the risk of re-identification by 22%.22

As it turns out, human mobility traces are highly unique. University researchers have also shown that individuals in an “anonymized” mobile phone data set are re-identifiable using only four pieces of outside information – e.g., a tweet positioning the person at a certain place and time, or a publicly available movie review. The researchers concluded that even data sets with coarse information offer little anonymity.23

In February 2015, researchers in the U.S. and Israel showed that by simply reading aggregate power usage of a mobile phone over a period of a few minutes, an application can infer the user’s location.24 The researchers conclude that “providing applications with unrestricted access to sensors, can potentially result in a security breach and compromise sensitive information.”

It is possible to de-identify personal data in such a manner that it cannot be re-identified and is thus truly anonymous, but data that has been “aggregated” for commercial/marketing purposes is not necessarily (nor likely to have been) subjected to a rigorous and proven de-identification process. Characterizing merely aggregated data as “anonymous” and treating it as outside the bounds of privacy law is misleading and legally suspect, at best. Consumers have a privacy interest in their data even when it is stripped of identifiers and aggregated with other data, as long as it can be associated with them through increasingly sophisticated data analytics tools and techniques.

This disturbing state of affairs reflects a market failure with respect to data security incentives generally. As one expert recently stated:

“A fundamental failure to take responsibility for insecure systems and buggy code is at the heart of our cybersecurity woes. While data breaches do cause companies legal headaches, the massive verdicts that have prompted reforms of other defective products are absent in the case of computer intrusions. The companies that write bad code have effectively protected themselves through software license agreements, and many companies would still rather hope for the best than spend money to fix their systems.”

Although the risks of security failures for automakers would seem high given the potential for extremely damaging publicity, there are indications that security of vehicle systems is by no means assured through reliance on market forces alone.

In 2013, researchers demonstrated their ability to access a vehicle’s computer system and control ECU functions from a laptop so as to, for example, alter steering, apply brakes and accelerate the vehicle while it is in motion. While the researchers accessed the vehicle systems directly via the OBD port, they and others have pointed out that remote wireless access to vehicle ECUs is possible through various means including through Bluetooth connections, malware in a synced Android smartphone or a malicious file on a CD in the stereo. A computer expert participating in the Federal Trade Commission’s November 2013 workshop on the Internet of Things discussed his successful efforts to remotely access a car’s internal computer network, reporting that he was able to control the vehicle’s brakes and other critical functionality by hacking into the telematics unit. In the meantime, criminals are already finding ways to take advantage of insecure vehicle electronics: “keyless car thefts” have apparently become a serious problem in England, as criminals find ways to reprogram remote-entry keys. With the increasing use of smartphones for telematics applications, a further avenue of access and thus security vulnerability is created. As Kevin Curran, IEEE Senior Member and professor of Computing and Engineering at the University of Ulster, U.K., warned:

“As vehicles become more accepting of wireless communication, connected cars will become increasingly vulnerable to software hacks. Hackers could potentially have the ability to affect audio features, disable the vehicle’s ignition, override braking systems and infect the software with Trojans and viruses. In order to combat this, manufacturers need to begin setting firewalls in place to restrict access from integrated systems. There is a strong presence of interconnectivity between vehicle networks, so a breach in one network may cause havoc in another.”

Michal Braverman-Blumenstyk, general manager of cybersecurity at Azure, Microsoft’s cloud service, was quoted as saying:

“All too often, we hear about well-crafted cyber attacks that come from the outside, but the reality is that the most damaging attacks come from the inside. As we’ve seen time and again, the weakest link in our security is often our own employees.”

In a disturbing report issued in February 2015, entitled “Tracking & Hacking: Security & Privacy Gaps put American Drivers at Risk”, U.S. Senator Ed Markey revealed how sixteen major automakers responded to detailed questions he posed to them the previous year. According to the report, the responses from automakers “show a vehicle fleet that has fully adopted wireless technologies like Bluetooth and even wireless internet access, but has not addressed
the real possibilities of hacker infiltration into vehicle systems.”32

Specifically, the Senator’s survey of automakers found that nearly all vehicles on the road are vulnerable to hacking via at least one, and often many, wireless entry points (i.e., ways that vehicle electronics can be accessed remotely). Common wireless access points were found to include TPMS, Bluetooth, keyless entry, remote start, navigation, Wi-Fi, cellular communications, radio and anti-theft systems and features. The study further found that “security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers”, that “only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time”, and that when asked, most automakers did not describe effective means of protecting customer data held in the data centres of the OEM or its service provider. With respect to the storage of data, the report found:

“the security measures of these data collection systems vary widely by manufacturer, and in some cases there are none. In the case of on- board storage, no manufacturer described any security system to protect that data, and several of them noted that no security measure is needed since accessing data would require a hardwire connection.”33

The Senator’s survey focused on vehicle data, but as noted above, Connected Car systems also operate like mobile devices, collecting and storing vast troves of data about individual communications and use of features and applications. Connected Car systems that include storage of personal contacts, schedules and other sensitive data for use by particular individuals create additional security vulnerabilities by virtue of the service they provide. Unless they are carefully designed with privacy-friendly default settings such as automatic locking of the system when the driver leaves the car, deletion of recent destinations in the navigation system and prompts to turn off Bluetooth, infotainment systems present opportunities for stalkers and others to access the private information of car owners.34

Indeed, much of the information collected and used by the Connected Car is of great interest to identity thieves, voyeurs, stalkers and those seeking to blackmail or otherwise harm other people. In this respect, security requires not only strong physical/technical firewalls and appropriate default settings, but also internal organizational measures to prevent insider abuse or employee error. Such “human-induced” security breaches are not uncommon. Examples relevant to the automobile industry include the 1998 case of a police officer in Washington, D.C. looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners. In 2005, an Edmonton police officer was reprimanded for using the police electronic database in a failed effort to frame a local journalist who had been publicly critical of his force’s use of photo radar.35

Clearly, even the strongest security measures are not foolproof. The only sure form of data security is not to collect the data in the first place.36

Secondary Uses

As the quotes at the beginning of this chapter illustrate, industry players are looking to secondary uses of personal customer data as the very basis of the business case for developing more Connected Car services. This approach flies in the face of data protection laws and principles, and risks further undermining the increasingly fragile state of individual privacy in our increasingly digital society.

The collection and retention of personal data for secondary purposes not only exacerbates these security risks, but creates an architecture of surveillance into which the tentacles of the state can reach, with or without required authorization. Moreover, once collected, data becomes available for unexpected secondary uses by a range of other bodies including creditors, fraud investigators and opposing parties in disputes, incidents or investigations.

Secondary uses are particularly troublesome because they are mostly invisible: consumers, even if generally aware that their personal data is being gathered and used for marketing purposes, are unlikely to be aware of the extent of such data collection, retention, use and disclosure, if only because corporate privacy policies themselves are unclear. If they were aware, it is likely that many consumers would be uncomfortable allowing the secondary use and would opt out of it if they could.

33 Markey Report, p.11.
34 http://www.wsj.com/articles/SB10000872396390443995604578004723603576296
36 For more on this subject, see Bruce Scheier’s blog, www.schneier.com, and Schneier on Security, Wiley, 2008.
Such choice is particularly important given that secondary uses of personal data gathered for the purpose of operating Connected Car services could have significant consequences for individuals, even beyond security breaches. For example, customers could face discrimination in unexpected and possibly invisible ways such as charging higher insurance rates to those who drive and park in higher risk neighbourhoods. Or, customers may simply wish to maintain control of their data and not have it used for secondary purposes such as marketing. Using customer data to profile a customer for the purpose of future targeted marketing may to some not seem like a privacy invasion, but to many it is: fully 80% of respondents to a national survey of Canadians in 2014 expressed concern about marketing companies using their online data to analyse their likes and dislikes, with 41% saying they were “very concerned”.

Sharing customer data with affiliates and partners for marketing or other secondary purposes increases privacy risks further, increasing the likelihood that properly informed customers would choose not to let their data be so shared.

DATA FLOWS

Telematics and infotainment systems give different players access to different sets of data. In some cases, the access is direct; in others, it is indirect.

Automakers have direct access to customer account information, all vehicle health data, driver behaviour data, location data and any biometric or health data that their systems collect. In addition, OEMs can access infotainment and communications data travelling through the vehicle system, even if only to mirror what appears on the user’s smartphone screen. Communications metadata may be gathered directly or shared by the mobile network provider with the OEM, allowing the OEM to track when, from where and to where calls, texts or emails are made. In-vehicle conversations with the service provider may be recorded and used for service delivery, customer relationship or quality of service purposes. Vehicle systems that make a person’s contacts, schedule, past routes or destinations, favourites, settings or other personal information available to them through an on-board dashboard screen give the automaker access to that data as well.

OEMs typically use this data not only as technically needed to provide the service, but also:

- to customize the delivery of services to that individual customer;
- to market additional products and services to the customer;
- to prevent or detect fraud or misuse of the service;
- to evaluate and improve their services;
- to engage in other (unspecified) research; and
- for unspecified “internal business purposes”.

Automakers share this data with (or obtain it from) third party service providers, call centres and application providers. Account data is typically shared with affiliated dealers, to allow the dealer to manage the customer relationship and improve vehicle and repair services. Customer data may also (with customer consent) be shared with affiliated insurers and/or financing companies. Communications metadata and even content, as well as highly detailed information about use of the service may be gathered by the OEM’s telecommunications provider and shared with the OEM.

Dealers obtain some customer data from the customer directly. In addition, they have access to whatever vehicle or additional customer information the automaker gives them. Dealers may also use aftermarket telematics services to keep track of leased vehicles or to offer value-added services to customers, obtaining additional data about their customer through the telematics device. Dealers have a strong interest in leveraging whatever data they can gather about their customers.

Call center operations are typically outsourced by automakers and aftermarket service providers to third parties. Call centres receive and process voice calls in emergencies, for roadside assistance or for concierge services such as directions, local information, point-of-interest searches reservations and ticketing. Call centres may retain this data (voice recordings and/or notes about the call) and make it available to their corporate customers for purposes of quality control or, possibly, customer relationship management.

---

CONNECTED CAR DATA OUTFLOWS

**ENTITIES RECEIVING THE DATA**

- Intelligent Transportation Systems
- Third Party Service/Content Providers
- Aftermarket Telematics Service Provider
- Mobile Network Provider
- Mobile Device Provider
- Independent Repair Shop
- Rental Agency
- Insurer and / or Lender
- Call Centre
- Dealer
- Automaker and suppliers/service providers

**TYPES OF DATA**

- Vehicle Health
- Driver Behaviour
- Location
- Biometrics & Health Data
- Information†
- Communications‡

† on-demand radio, music, video, other content, web browsing, internet-based applications
‡ voice, text and email communications, social networking, contacts and schedule
Insurers use telematics devices (or possibly OEM systems) to access certain driver behaviour and vehicle location data for the purpose of assessing risk and adjusting insurance rates accordingly. Insurers have a strong interest in accessing additional data that could be relevant to their risk assessments and claims investigations. Insurers may also wish to expand their sources of revenue by using the data they gather to market value-added services to customers.

Lenders use telematics devices (or possibly OEM systems) to access certain driver behaviour (e.g., ignition) and location data in order to manage automobile leases and loans. Ignition data is used to trigger warnings that payments are due. Lenders also use telematics to disable and enable ignition for the purpose of loan management and vehicle repossession.

Rental Car Agencies and Car-Sharing Organizations use telematics devices to track the location of their vehicles. They can also track customer driving behaviour and vehicle health data. To the extent that they offer value-added navigation or infotainment services in their vehicles, such agencies have access to data about each customer’s use of the additional services.

Mobile Device System Providers such as Google (Android) and Apple (iOS) have access to all data running over their systems: depending on the system or service, this can include any of the categories of data set out above. It can include certain vehicle or driver behaviour data required for the purposes of specific mobile applications. It can also include location data via the car’s GPS module, even if the customer has turned off their mobile device’s GPS function. In the case of smartphone-based infotainment systems, the smartphone system provider has access to much of the data to begin with, and is simply sharing it with the automaker. However, vehicle-based applications that operate over the smartphone system provide the mobile device provider with additional data about the customer.

Mobile Network Operators have access to the communications metadata running over their networks – i.e., data about the time, origin and destination of a person’s voice, text and email communications as well as data about their downloading and content streaming activity from the vehicle. Mobile network operators can track use of their networks from vehicle WiFi hotspots as well as from voice and text communications systems based on Subscriber Identity Modules (SIM cards) embedded in the vehicle infotainment system. Through SIM cards, mobile network operators can also access the subscriber’s contacts and custom menus.

Aftermarket Telematics Service Providers have access to vehicle data and driver behaviour data via the OBD port, as well as location data either from their device-based GPS or radio-frequency locating system or from the customer’s mobile device. To the extent that they provide emergency, roadside assistance and concierge services, aftermarket providers can also accumulate data on customer use of these services. Similarly, aftermarket providers can track customer use of applications (their own or those of third parties) offered via the aftermarket device.

Third Party Application Providers have access to data about the use of their applications, whether offered via OEMs or aftermarket providers. Third party applications can gather personal data of all kinds, depending on the needs of the application and the data that is made available to them by the OEM and/or aftermarket provider. Importantly from a privacy perspective, third party applications commonly gather additional data directly from users, or from social networking sites to which they link, and combine it with telematics data in order to offer value-added services via their application or to distinguish themselves from other applications.

External sources of data

All of these entities have access to data from outside the Connected Car Ecosystem, either from their own separate dealings with the same customer (e.g., Insurers, Lenders, Mobile Device System Operators and Mobile Network Operators), or from affiliates, data brokers or other sources. Some Connected Car service providers note in their privacy policies that they collect (or may collect) data about the customer and his or her vehicle from third parties, including publicly and commercially available sources. By combining and correlating datasets from different sources, they can learn more about each user of their product or service.

---

38 E.g., Volkswagen/Verizon, op cit.; Kia UVO Privacy Policy effective Feb.1, 2013, s.1(d). OnStar’s Privacy Policy simply states that it may collect information about the customer from other sources.
DATA SHARING INSIDE AND OUTSIDE THE CONNECTED CAR ECOSYSTEM

Consumer data in the Connected Car ecosystem is shared among many players. The extent of such sharing varies by company and type of information, but automakers commonly share certain data with:

- comprehensive Connected Car service providers such as OnStar, Verizon and Sprint;
- specific service providers (e.g., call centres, roadside assistance providers, emergency service providers) to whom they have outsourced elements of their services;
- their affiliated dealers, financing companies and insurers;
- mobile network operators with whom they have partnered solely to offer human voice and data communications via in-car systems;
- smartphone operating system providers (in order to allow their services to operate via smartphones);
- third party application providers and advertisers; and
- other third parties with whom they contract for joint marketing offers.

Aftermarket telematics service providers commonly share with:

- Their corporate customers, who can be dealers, insurers, lenders, rental car agencies, and even automakers;
- Smartphone operating system providers in order to allow their services to operate via smartphones; and
- Third party application providers and advertisers.

A given entity may play more than one role. For example, a mobile network operator may provide the entire suite of Connected Car services to the OEM, and also sell an aftermarket telematics device to consumers (e.g., Verizon). Such multiple role-playing increases the likelihood of data sharing and secondary uses. Every additional entity that has custody of the data represents one more point of vulnerability to unauthorized or unwanted access and use.

Corporate affiliation is commonly used as a justification for sharing of data without explicit customer consent, and the automobile industry is no different from any other in that respect. But corporate affiliations are not always apparent to individuals, and even if they are, the fact of a corporate affiliation has no bearing per se on the privacy consequences of data sharing. Commercial exchanges of customer data, regardless of corporate affiliation, and regardless of the level of security applied to the data, have privacy implications for the individuals concerned.

The 2013 industry roundtable summary cited above also noted that selling driver data to third parties constitutes a key element of the industry’s business model - concluding, in part:

“Revenue model - A mixture of subscription, embedded, pay as you go (PAYG) and big data will need to be considered for successful mass market offerings. Product category based pricing makes most sense, with security features being embedded, infotainment being on a PAYG basis and data analytics being used to sell driver data to third parties.”

GM appears to be leading the way in Canada with its “AtYourService” offering, in which location information is shared with local advertisers to deliver up relevant ads in the vehicle as it approaches certain locations. While it is not clear what information, if any, is shared with the retailer, or whether the advertising company obtains any personal information in order to serve up relevant ads, it is clear that GM is using customer location data to generate new revenues through targeted advertising – a purpose unconnected to the purpose for which most customers purchase OnStar.

Indeed, personal data about vehicle purchasers is already being sold to third parties with no strings attached. A study of data brokers conducted by the US Federal Trade Commission in 2013-14 found that data brokers collect consumer data from numerous sources including “information from automobile dealers about sales and service, warranty, and aftermarket repairs.” The FTC concluded that data brokers collect, store and share billions of data elements covering nearly every US consumer, largely without consumers’ knowledge, and that this data is combined and analyzed to make inferences about individual consumers, “including potentially sensitive inferences.” Yet the sale of customer data to...

39 Ibid., p.5.
unregulated data brokers is apparently considered to be a legitimate business practice.

When a service provider’s business model is premised on data sharing, it is not surprising that slip-ups occur. In 2011, satellite navigation company TomTom was found to have sold driving data collected from its customers to the Dutch police for the purpose of setting speed traps. TomTom issued an apology, stating that the data had been anonymous but that it would change its licensing agreements to prevent such uses in the future.41 Like other aftermarket providers, a key element of TomTom’s business case is selling access to its traffic database to governments and corporations.

CONCLUSION

Connected Cars are set to become a major new source of data about individual drivers for use not only by automakers and their business partners, but also by third party insurers, lenders, content and service providers as well as by law enforcement agencies, debt collectors, fraud investigators, litigants and others with legal rights to access the data. Moreover, the private databases of vehicle and driver data created as a result of this new industry ecosystem, not to mention the transmission of vehicle data over cellular and short range wireless networks, presents a highly sensitive target for malicious hackers, stalkers and cyber-criminals.

---

This chapter sets out data protection law applicable to Connected Cars in Canada as a background to the privacy analysis of Connected Cars in Chapter Seven. In addition to general data protection legislation, we review the current state of regulation of usage-based insurance in Canada. Also provided for comparative purposes is a summary of U.S. law with respect to Event Data Recorders, key telematics-related legislation recently proposed in the U.S., and approaches to data protection in the context of public sector telematics initiatives in the E.U. and U.S.
THE RIGHT TO PRIVACY

In his landmark work, Privacy and Freedom, Alan Westin defined information privacy as “an individual’s right “to control, edit, manage, and delete information about them[elves] and decide when, how, and to what extent information is communicated to others.”1 In so doing, he took the established legal concept of privacy as “the right to be let alone”2 and recast it to make sense in an era of computers, credit cards and direct marketing. Westin’s concept of privacy has since formed the basis of data protection laws in Canada and throughout the western world, with the notable exception of the United States.

DATA PROTECTION LEGISLATION IN CONTEXT

North American automakers operate in a relatively integrated market. For this reason, great efforts have been made to harmonize the motor vehicle safety and emissions regulations demanded by the public and regulators. However to date, no effort has been made to establish harmonized data protection regulation, even as the car becomes a highly efficient data processing machine.

In the United States, there is a patchwork of data protection laws of limited scope that varies among states, leaving the industry largely unregulated other than with respect to specific issues such as Event Data Recorders. Although the Federal Trade Commission enforces the federal law requiring that companies comply with their stated privacy policies, there is no federal U.S. law setting out standards for such policies. In contrast, Canada (like Europe) has data protection legislation that is comprehensive with respect to both its content – a set of principles governing the collection, retention, use and disclosure of personal information – and its application - to all commercial activities, across sectors.

The purpose of this legislation, as set out in the federal Personal Information Protection and Electronic Documents Act (“PIPEDA”), S.C. 2000, c.5, section 3, is:

"... to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.” (emphasis added)

CANADA’S DATA PROTECTION LEGISLATION: AN OVERVIEW

Canada’s federal data protection statute, PIPEDA, applies to all organizations that collect, use or disclose personal information in the course of commercial activities either inter-provincially or in provinces and territories other than Quebec, Alberta and British Columbia (where substantially similar provincial legislation applies).3 All commercial stakeholders who collect, use or disclose “personal information” in the course of providing their services, whether to consumers directly or not, are therefore subject to PIPEDA or its provincial counterpart.

Together, the four laws create a nation-wide set of industry obligations based on what have become known internationally as Fair Information Principles. These principles were codified first by the OECD in its 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.4 In 1996, the Standards Council of Canada adopted a version of the same principles in a formal national standard developed by a multi-stakeholder committee of the Canadian Standards Association.5 PIPEDA incorporates the CSA Standard word for word, while the provincial statutes do so implicitly. The CSA Standard (now Schedule 1 to PIPEDA) establishes the following ten Principles of data protection:

1. Accountability: Organizations must designate an individual to be accountable for their compliance with the principles. They must also take responsibility for the compliance of third parties to whom they transfer data for processing.

2. Identifying Purposes: Organizations must identify the purposes for which they collect
personal information at or before the time of collection, and must specify those purposes to the individuals from whom the information is collected.

3. **Informed Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, other than as specifically permitted in statutory exceptions. Consent may be implied where it is reasonable to do so. Consent to secondary purposes (e.g., marketing and product improvement) may be obtained via negative option (also referred to as “opt-out”) as long as the sensitivity of the information and the reasonable expectations of the individual do not suggest otherwise. Organizations cannot, as a condition of the supply of a good or service, require an individual to consent to information collection, use or disclosure beyond that which is necessary to provide the product or service.

4. **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

Informed Consent is the cornerstone of this set of principles. However, an eleventh principle that operates regardless of consent was added to federal and provincial legislation:

**Purpose Limitation**: Organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (subs.5(3), PIPEDA).7

There are a number of exceptions to the requirement for informed consent including law enforcement, national security, emergencies, subpoenas, fraud investigation, statistical research and debt collection.6 No amount of technical security measures or privacy policy assurances can protect data from authorized access under one of these exceptions: if it is retained. Connected Car data is available to third parties for use in litigation (by subpoena) and to law enforcement or national security agencies in the context of their investigations (by court order or warrant).

---

6 PIPEDA s.7; Alta PIPA ss.14, 17, 20; BC PIPA ss.12, 15, 18.
7 See next page for footnote.
APPROPRIATE PURPOSES

What purposes “a reasonable person would consider appropriate in the circumstances” is often debatable. However, the Supreme Court of Canada has provided guidance on this question in the context of state surveillance. In that context, the court has ruled that if an individual has a “reasonable expectation of privacy” in any given data, the police must obtain a warrant before requesting such data from an intermediary such as an internet service provider. Applying this test to various fact scenarios before it, the court has clarified that the concept of “reasonable expectation of privacy” is normative, not simply descriptive of existing practices. In other words, it is akin to what “a reasonable person would consider appropriate in the circumstances.”

The Court has further found, in the state surveillance context, that individuals have a reasonable expectation of privacy in information that tends to reveal intimate details of their lifestyle and personal choices, including “information sought to support inferences in relation to other personal information.” This is a much narrower category of information than that protected by data protection statutes, which apply to all “personal information” regardless of how revealing of an individual the information is. Nevertheless, the Court’s findings with respect to when an individual has a reasonable expectation of privacy in their personal information is instructive.

In the 1992 case of R. v. Wise, the court found that ubiquitous monitoring by police of a vehicle’s whereabouts on public highways amounted to a violation of the suspect’s reasonable expectation of privacy, stating that:

“Personal privacy protects an individual’s ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual’s personal growth and the flourishing of an open and democratic society.”

In a more recent criminal law case, R. v. Spencer, the court referred to R. v. Wise, noting that “it could of course have been argued that the electronic device was simply a convenient way of keeping track of where the suspect was driving his car, something that he was doing in public for all to see. But the Court did not take that approach.” Noting further that “internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smartphones, or portable devices,” the court held that:

“The understanding of informational privacy as control ‘derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit’ (Dyment, at p. 429, quoting from Privacy and Computers, the Report of the Task Force established by the Department of Communications/Department of Justice (1972), at p. 13). Even though the information will be communicated and cannot be thought of as secret or confidential, ‘situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected’ (pp. 429-30).”

One of the arguments put forward by the state to defend police access to subscriber information without a warrant has been that the subscriber agreed to

---

7 In addition to limiting purposes using the same language as PIPEDA, the B.C. PIPA extends its reasonableness limitation to practices by way of section 4(a), which states: “In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.” Similarly, section 6 of the Alberta Act requires that organizations “develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act”. In addition, subsections 11(2), 16(2) and 19(2) of the Act state: “Where an organization [collects/ uses/discloses] personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is [collected/used/disclosed].” Section 2 of the Alberta Act establishes the standard for “reasonable” as “what a reasonable person would consider appropriate in the circumstances”. While the Quebec statute does not include a “reasonableness” standard per se, its express purpose is to establish rules “for the exercise of the rights conferred by articles 35 to 40 of the Civil Code...”. Article 37 of the Code mandates “serious and legitimate reason[s]” for the creation of a file on another person, and states that one must not, “when establishing or using the file, otherwise invade the privacy or damage the reputation of the person concerned”. Moreover, the Quebec Charter of Human Rights and Freedoms establishes privacy as a human right, stating that “Every person has a right to respect for his private life.” These provisions have been referenced in a number of cases involving alleged breaches of the Quebec private sector Act, as grounds for applying a reasonableness/proportionality test similar to that developed by the Supreme Court of Canada in R. v. Oakes.


terms of service that included a provision allowing the service provider to share subscriber data with law enforcement agencies. On that point, the Court stated:

“There is no doubt that the contractual and statutory framework may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy. So, for example in Gomboc, Deschamps J. writing for four members of the Court, found that the terms governing the relationship between the electricity provider and its customer were “highly significant” to Mr Gomboc’s reasonable expectation of privacy, but treated it as “one factor amongst many others which must be weighed in assessing the totality of the circumstances”: paras. 31-32. She also emphasized that when dealing with contracts of adhesion in the context of a consumer relationship, it was necessary to “proceed[d] with caution” when determining the impact that such provision would have on the reasonableness of an expectation of privacy: para. 33. The need for caution in this context was pointedly underlined in the dissenting reasons of the Chief Justice and Fish J. in that case: paras. 138-42 (emphasis added).”

These cases involve the particular privacy interests of citizens in respect of state surveillance, not corporate surveillance. There are obvious privacy risks entailed in state surveillance that do not arise with corporate surveillance (e.g., threats to personal liberty). Nevertheless, the court’s conceptualization of a citizen’s reasonable expectations of privacy in the context of state surveillance is instructive for the interpretation of informational privacy rights in the private sector, and in particular, for what “a reasonable person would consider appropriate in the circumstances” of Connected Cars and other aspects of today’s increasingly connected world.

Of particular note is the court’s characterization of “reasonable expectations” as normative not descriptive – i.e., just because the practice is widespread doesn’t mean that it is reasonably expected. Data protection legislation is explicit on this point: the ultimate test of business practices is not what a reasonable person would expect in the circumstances, but rather what a reasonable person would consider appropriate in the circumstances – a clearly normative test. In other words, what matters is what we as a society consider to be acceptable in terms of trade-offs between individual privacy and business interests. While our societal views of appropriateness may evolve over time, they are determined not by what technology permits, nor by the pervasiveness of the business practice, but rather by our values – those of a free and democratic society in which individual autonomy, dignity and privacy are key pillars.

Also of note is the Supreme Court’s warning that just because the terms of service imposed on a consumer in a contract of adhesion allow for certain uses or disclosures of the consumer’s data does not mean that those uses or disclosures meet the “reasonable expectation of privacy” test. Albeit in the context of state surveillance, the court is signaling that informed consent must be meaningful for it to be enforceable. The same reasoning applies a fortiori in the context of corporate surveillance, where individuals are expected to make informed purchasing decisions based on corporate privacy policies.

The Supreme Court of Canada has not yet addressed the issue of reasonable purposes in the context of corporate surveillance. However, it has confirmed that data protection legislation is “quasi-constitutional” in nature, noting in the private sector context that “the importance of the protection of privacy in a vibrant democracy cannot be overstated.” Meanwhile, the Ontario Court of Appeal has recognized a common law tort of “invasion upon seclusion”, finding that an employee’s intentional and unauthorized examination of the plaintiff’s private bank records amounted to an unlawful invasion of the plaintiff’s private affairs. In creating this new cause of action, the court referred to the Supreme Court of Canada’s criminal law jurisprudence and reasoned that:

“For over 100 years, technological change has motivated the legal protection of the individual’s right to privacy. In modern times, the pace of technological change has accelerated exponentially...The Internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information....

It is within the capacity of the common law to evolve to respond to the problem posed by the
routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order.\textsuperscript{16}

It is in this context that courts will interpret Canada’s data protection legislation, and in particular, whether certain purposes specified by organizations in their privacy policies meet the “appropriate purposes” test.

REFUSAL TO DEAL

In addition to the rule against inappropriate purposes, Canada’s data protection laws prohibit corporations from refusing services to consumers who do not consent to unnecessary collection, use or disclosure of their personal data. The relevant provision of PIPEDA is as follows:

“An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes. (PIPEDA, Sch.1, 4.3.3)”

The three provincial provisions impose similar limits but do not require an assessment of purposes; rather, the test they establish is whether the required collection, use or disclosure is necessary for the provision of the good or service in question.\textsuperscript{17} Read in the context of PIPEDA as a whole, it is clear however that the federal “legitimate purposes” test is no different from the provincial tests. Subsection 5(3) limits “legitimate purposes” to those “that a reasonable person would consider are appropriate in the circumstances.”

Needless to say, “the circumstances” in such cases include refusal to deal. Reasonable people would probably consider it inappropriate to require a buyer to agree to an unnecessary purpose in order to obtain the service. Appropriateness, and thus legitimacy, of a given purpose therefore depends critically on whether or not the purpose is necessary for the organization to provide the requested service.

Where there are different uses of a given piece of personal information, some necessary and some not, organizations must separate out necessary and unnecessary uses, and offer consumers the ability to opt-out of unnecessary ones. Just because the information is necessary for one use does not give the organization the right to force consumers to agree to other, unnecessary uses.

The combined effect of PIPEDA’s Principle 4.3.3 and subsection 5(3) of PIPEDA is effectively the same as the “refusal to deal” tests set out in provincial legislation: organizations must not require individuals to agree to collection, use or disclosure of their personal data in order to obtain a product or service for which such collection, use or disclosure is not necessary.

As stated by former B.C. Information and Privacy Commissioner David Loukidelis in a 2009 decision under the B.C. legislation:

“…personal information must certainly be more than simply convenient to have or of some possible future use. For personal information to be “necessary” for the purposes of s. 7(2) of PIPA, the purposes for the collection, use or disclosure must be integral to the provision of the product or service. In addition, the personal information in question must fulfill a significant role in enabling the organization to achieve that purpose. It is also important for the organization's purposes to be stated as precisely as possible, avoiding overly generalized objectives. In addition, it is necessary to consider whether the scope of the collection is appropriately tailored to the purposes for which it is collected. In assessing these questions, the sensitivity of the information may play some role in determining the level of scrutiny to be applied.”\textsuperscript{18}

MEANINGFUL NOTICE AND CHOICE

The requirement for “informed consent” with respect to secondary uses was clarified by then-Privacy Commissioner of Canada George Radwanski in a 2002 finding involving wireless carrier Bell Mobility. The Commissioner determined that Bell Mobility had failed to obtain informed consent of its customers to its policy of sharing customer data with other Bell Canada affiliates for secondary marketing purposes.

\textsuperscript{16} Jones v. Tsige, 2012 ONCA 32 (CanLII), paras.67-68.
\textsuperscript{17} B.C. PIPA subs.7(2); Alta PIPA subs.7(2); Quebec Act, s.9.
\textsuperscript{18} Cruz Ventures Ltd. (Wild Coyote Club) (Re), 2009 CanLII 38705 (BC IPC), para.40.
The Commissioner explained his findings as follows in his letter to the Complainant:

“I note that Principles 4.2.3 and 4.3.1 clearly support your expectation that an organization should not merely make policy documents generally available, but should actually bring to the attention of the individual at the time of collection its purposes for collecting, using, and disclosing personal information. When an organization collects personal information during an application, subscription, or purchasing process, it should take reasonable steps during the same process to specify to the individual, and seek the individual’s express consent for, any intended secondary uses or disclosures. It follows that the organization should be prepared to provide the individual, on the spot, with whatever information he or she may require to make a knowledgeable consent decision. In such situations, I consider it entirely reasonable, as you have suggested, for an individual to expect not to have to seek out or otherwise rely upon information that is not immediately at hand.

I also consider it only reasonable for the individual to expect to be informed, likewise during the same process, of the opportunity and a convenient method for withdrawing consent.

Finally, where an organization intends to disclose personal information that the individual is likely to consider sensitive, such as credit records and complaint records, I consider it reasonable for the individual to expect to be consulted directly and positively in the matter of consent. In such a situation, the organization should use positive or “opt-in” consent rather than the negative option.”

“PERSONAL INFORMATION”

PIPEDA and its provincial counterparts protect “personal information”, which is statutorily defined as “information about an identifiable individual.” As discussed in Chapter Five, this definition extends beyond information that itself identifies an individual, to information that can be linked – if, for example, combined with other information - to an identified individual. As the Privacy Commissioner of Canada stated in his 2001-2002 Annual Report to Parliament:

“the definition is deliberately broad...It does not matter who generated the information, or how, or who technically “owns” it...information [is] personal even if there is the smallest potential for it to be about an identifiable individual.”

More recently, the OPCC stated in a finding under PIPEDA that:

“In general, “personal information” means information about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.”

According to the British Columbia Information and Privacy Commissioner (“BCIPC”),

“in order to be personal information, the information must be reasonably capable of identifying a particular individual either alone or when combined with information from other available sources. The information need not identify the individual to everyone who receives it; it is sufficient in a case such as this if the information reasonably permits identification of the individual to those seeking to collect, use or disclose it.”

Courts, for the most part, have adopted similar tests in determining whether data that does not itself identify the particular individual in question can still be considered to be “personal information” under PIPEDA. The Federal Court of Canada, for example, has ruled that:

“information recorded in any form is information “about” a particular individual if it “permits” or “leads” to the possible identification of the

---

19 See http://www.piac.ca/our-specialities/commissioners-findings-bell-mobility.
20 P.56.
21 OPCC PIPEDA Finding No.2013-017: Apple use of unique device ID for ad targeting.
22 BCIPC Order No.P12-01, 2012 BCIPC No.25 (CanLII).
23 The Ontario Court of Appeal has affirmed a lower court finding that the test is whether “there is a reasonable expectation that, when the information in it is combined with information from other sources otherwise available, the individual can be identified...”: Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner), 2001 CanLII 32755 (ON SCDC), (aff’d Ontario (Attorney General) v. Pascoe, 2002 CanLII 30891 (ON CA), (2002). The majority decision of the Alberta Court of Appeal in Leon’s Furniture Limited v. Alberta (Information and Privacy Commissioner), 2011 ABCA 94 (CanLII), leave to appeal dismissed 2011 CanLII 75277 (SCC) stands in contrast to the weight of jurisprudence on this issue. In that case, two of the three judges reasoned that licence plates were not “personal information” because they were about vehicles, not individuals.
individual, whether alone or when combined with information from sources “otherwise available” including sources publicly available (underlining in original).”

Moreover, the initially identified individual need not be the same individual to whom the information relates. As long as the individual in question (e.g., driver; internet user) can be traced (e.g., via the vehicle owner), the information is considered to be “personal information” relating to that person.

Thus, for example, the following data has been found to constitute “personal information” under PIPEDA or its provincial counterparts:

- An IP address, as long as the entity holding the IP address can associate it with an identifiable individual, even if that individual is not the particular internet user in question;25
- Data collected by employers via GPS devices in their vehicles, as long as it can be linked to specific employees, even if the data does not identify the specific employees at all times to all users of the system; 26
- Information stored by temporary as well as permanent “cookies”; 27
- A mobile device unique ID which on its own does not identify the user, but which can be associated with the account details for the user; 28
- Telematics-based location, engine status and driver behaviour data from employer fleet vehicles;29 and
- License plate information, because it can be linked to individuals via the motor vehicle registration database.30

There can be little doubt, therefore, that VINs constitute “personal information” under Canadian data protection laws. To the extent that vehicle health data can be linked with the VIN, it therefore constitutes “personal information.” One possible way of removing the link between VINs and identifiable individuals is to automatically delete the last several digits of the VIN as it is being collected.

Whether or not “aggregated” data constitutes “personal information” under Canadian law will depend on the ease with which it can be re-associated with identifiable individuals using data analytics technology. Given the power of such technology to parse and correlate vast amounts of data from multiple different sources in order to generate linkages and insights, much aggregated data likely falls within the definition of “personal information” despite claims to the contrary. Indeed, as explained in Chapter Five, researchers are proving that data that was thought to have been effectively anonymized was, in fact, easily re-identifiable. If an organization wishes to treat aggregated customer data as non-personal information, the organization should state clearly in its privacy policy that the aggregation process is done in such a way as to render the risk of re-identification statistically impossible (or specify the statistical risk).

REGULATION OF TELECOMMUNICATIONS IN CANADA

In Canada, telecommunications is federally regulated by the Canadian Radio-Television and Telecommunications Commission (“CRTC”). Since enactment of PIPEDA, privacy-related complaints involving telecommunications service providers have, for the most part, been directed to and handled by the Office of the Privacy Commissioner of Canada under that legislation. However, the CRTC has continued to administer rules regulating unsolicited calling and, most recently, is considering an application filed by the Public Interest Advocacy Centre (“PIAC”) and the Consumers’ Association of Canada (“CAC”) challenging Bell Canada’s collection, use and disclosure of customer information gathered from its wireless customers for marketing purposes as contrary to Canadian telecommunications policy.31

One of the objectives of Canadian telecommunications policy, set out in s.7 of the Telecommunications Act, is “the protection of the privacy of persons.” PIAC/CAC argue in their application that Bell’s “Relevant Ads” program violates Canadians’ reasonable

---

24 Gordon v. Canada (Minister of Health), [2008] FC 258 at para.33
25 OPCC PIPEDA Finding No. 2009-010: Bell use of Deep Packet Inspection, para.47
28 OPCC PIPEDA Finding No.2013-017: Apple use of unique device ID for ad targeting.
29 BCIPC, Order P12-01 re: Schindler Elevator Corporation, 2012 BCIPAC No.25 (CANLII).
30 OIPC, Privacy Investigation: The Toronto Police Service's use of Mobile Licence Plate Technology to find Stolen Vehicles (April 29, 2003); and British Columbia Information and Privacy Commissioner (“BCIPC”), Investigation Report F12-04 - Use of Automated Licence Plate Recognition Technology by the Victoria Police Department (Re), 2012 BCIPC 23 (CanLII).
expectation of privacy and is therefore contrary to the Telecommunications Act. They also argue that Bell’s secondary marketing program violates both the Commission’s rules for Internet Traffic Management Practices, and the CRTC’s Confidential Customer Information rules, among other things. The Commission has asked Bell numerous questions about its practices in two rounds of interrogatories so far, with submissions still being made as of February 2015. It thus remains to be seen how the CRTC will decide on PIAC/CAC’s application, and how its decision will affect determinations under PIPEDA on similar matters.

REGULATION OF USAGE-BASED INSURANCE IN CANADA

Automobile insurance is regulated at the provincial/territorial level in Canada; insurers are therefore subject to provincial data protection laws where they exist (Alberta, British Columbia and Quebec) and to PIPEDA elsewhere in Canada. Nevertheless, at least one provincial insurance regulator has seen fit to develop and apply regulations limiting the personal information that insurers are permitted to collect via UBI, and others are expected to follow suit.

UBI programs are now operating in Ontario and Quebec, and are expected to be approved in Alberta later this year. The only detailed guidelines for UBI implementation publicly issued by a provincial regulator as of February 2015 are those published by the Financial Services Commission of Ontario (“FSCO”). The FSCO Filing Guidelines constitute, to a large degree, UBI-specific implementation of data protection obligations set out in PIPEDA. The Guidelines state:

“A key component of a UBIP [UBI Pricing] program is the collection and processing of this personal telematics information for the purposes of auto insurance rating. While FSCO does not oversee personal privacy legislation, it is important to FSCO that UBIP programs respect the privacy of consumers and comply with all applicable legislation.”

Telematics data collected about a driver is specifically classified in the FSCO Guidelines as “personal information.” In this respect, the guidelines state:

“UBIP technologies are capable of collecting detailed telematics information about where, how and when vehicles are driven. Although telematics devices do not currently have the capability to identify who is driving a vehicle at any particular time, in many circumstances (for example where a vehicle has only one listed driver), the data collected by the device may reasonably be assumed to be about that individual, with the result that the data is personal information as defined in PIPEDA.

Where a vehicle has a number of listed drivers (for example in a family), information is collected on all of those individuals, and can affect the rating for a policy insuring all of those individuals, even if the specific driver at any given time cannot be identified. FSCO therefore takes the position that telematics data should be treated as personal information even if it is not about the driving behaviour of any one identifiable individual, and should be handled accordingly.”

Conditions for approval of UBI in Ontario include:

• “UBIP programs must be voluntary and enrollment must include the express, informed consent of the policyholder to the collection, use and disclosure of personal information by the insurer or third party provider.”
• “Prior to enrollment, insurers need to inform consumers what personal information is being collected, who may use or have access to the information, how the information is being used, under what circumstances the information will or could be disclosed to other parties, and what their rights are with respect to the information.”
• “Consumers should also be made aware of, and given the opportunity to give or withhold consent to, any relevant changes to what or how personal information is collected, used or disclosed.”
• “Any personal information collected through a UBIP program, or its accompanying devices or software, should not be disclosed to any other party unless expressly consented to by the person or as required by law.”
• “Drivers should be able to enroll in a UBIP program without being required to share their personal information for non-UBI purposes (e.g., marketing, offering of additional services such as vehicle location services or assistance in emergency situations). Therefore, insurers should not require consumers to consent to the collection, use or disclosure of information beyond that required by a UBIP program as a condition of participation. Consumers should be given the

---

33 Bulletin NO. A-05/13, Section 1.
opportunity to actively opt-in, rather than opt-out, to the collection, use or disclosure of personal information for non-UBIP purposes.”

- Insurers must take reasonable steps to ensure that the data collected by UBI telematics is accurate, secure, and stored/retained/deleted appropriately.
- Insurers must provide adequate customer service mechanisms to allow policyholders to discuss or dispute the accuracy and use of their data.
- UBI customers must have meaningful access to their personal information, including the ability to transfer their personal UBI data to another insurer.
- Insurers should consider privacy-by-design principles when developing a UBI program.

The requirement for informed consent of consumers to UBI is enforced through FSCO review of all customer-facing documents including marketing material, agent sales scripts and terms of service. While the FSCO has no authority over third party device and data service providers, the guidelines make insurers explicitly responsible for ensuring the compliance of third party partners:

“Insurers remain accountable for the collection, use or disclosure of personal information associated with a UBIP program. Insurers are also required to ensure that any third party providers who collect, use or disclose personal UBIP information provide a level of protection comparable to that expected of the insurer. Insurers must be certain of the type of information being collected by the third party provider, that it is free of manipulation, and that the provider is collecting, using and disclosing the information only as consented to by the consumer.”34

Third party use of consumer data collected as a condition of their participation in a UBI program is currently not permitted without express consent. While only those extended uses of data that are specifically insurance-related would technically fall within its purview, the FSCO has the authority to investigate in order to ensure compliance with policy terms and conditions (e.g., to ensure that customer data is being used or disclosed to third parties only in ways consented to by the customer).

Importantly, the FSCO has approved UBI only for the purposes of offering discounts to customers, stating:

“At this point in time, UBIP programs, including program-provided devices and applications, should collect and use UBIP data solely for discount-setting purposes, and not to decline, cancel or refuse to renew risks or to confirm rating criteria currently used (e.g., where vehicle is principally garaged, distance driven, pleasure/commute/business use). Additionally, it would be inappropriate for insurers to use UBIP data for claims-related purposes at this time.”

These limits could change if data accumulated during the first 24 months of UBI operation supports the actuarial efficacy of telematics ratings criteria. In this respect, it is worth noting that telematics is being used by insurers in other countries to adjust rates upwards as well as downwards, to monitor accidents, to contribute to claims adjustment, and to deny coverage.35

In Quebec, the provincial government takes care of personal injury automobile insurance via the Société de l'assurance automobile (“SAAQ”), while property damage insurance coverage is left to the private sector. Currently, only the private sector offers UBI in Quebec. Two of the three programs available in Quebec also operate in Ontario and therefore adhere to the FSCO guidelines.36 The provincial brokers’ organization is calling on the provincial regulator to issue guidelines for insurance telematics. Its chairman, Jean Bilodeau stated in a press release: “The AMF has yet to issue guidelines on telematics-based devices. These guidelines should be issued as a matter of urgency and should apply to all insurers.”37

The SAAQ recently announced its intention to begin offering a UBI program in 2016. Although the program will initially be voluntary, the Quebec Minister of Transportation has stated that he might in future

---

34 Bulletin NO. A-05/13 section 12, Roles and Responsibilities: Insurers and Third Party Providers.
36 The third, Mobiliz, is a specialized program designed for young drivers.
consider requiring telematics devices for drivers previously convicted of dangerous driving: “À partir de là, suite à une accusation, à une sentence, il pourrait y avoir ce type de technologie. Moi, je ne ferme pas la porte.”

Alberta is the next Canadian province where UBI programs are expected to be introduced. The Alberta Superintendent of Insurance has indicated that guidelines will be made public in spring 2015, with an anticipated implementation date of June 2015. Key issues for the Alberta regulator in considering the introduction of UBI have been informed consent and privacy. The Automobile Insurance Rate Board of Alberta, in its 2013 annual report, specifically noted that “the issue of informed consent by Alberta consumers must be satisfactorily addressed prior to the introduction of any programs.” Indeed, the offices of the Superintendent of Insurance and the Information and Privacy Commissioner of Alberta have been working closely together to prepare appropriate guidelines, policies and procedures prior to implementing UBI in Alberta.

In sum, automobile insurance in Canada is subject to general data protection laws. Nevertheless, provincial insurance regulators are seeing fit to establish UBI-specific data protection regulations, thus ensuring that UBI complies with data protection laws and providing more guidance to insurers as how general data protection obligations apply in the UBI context.

DATA PROTECTION REGULATION IN THE UNITED STATES

As noted above, the United States lacks cross-sectoral data protection legislation such as PIPEDA. Privacy law in the U.S. is best characterized as a patchwork of sector-specific and issue-specific laws at both federal and state levels, leaving significant geographic and subject-matter gaps. One issue that has prompted recent legislative action in the U.S. is privacy of driver data in Event Data Recorders. Other privacy issues related to telematics that have resulted in legislation in the U.S. include the use of telematics for insurance and in the context of rental cars.

Regulation of Event Data Recorders

As noted in Chapter Five, telematics technology allows automakers to collect data on accidents. Indeed, many OEM Connected Car privacy policies expressly identify information about collisions, including direction of impact and airbag deployment, as one type of data that is collected automatically from the vehicle.

Interestingly, such data is already the subject of strict regulation in the context of Event Data Recorders (“EDRs”). EDRs collect crash-related data from the vehicle including direction of impact, airbag deployment, vehicle speed, engine throttle, brake activation, crash forces, and seat belt use in the seconds before and during a crash. They are triggered by deployment of airbags or other safety restraint systems. The data collected is stored in the device and cannot be accessed other than directly by someone with physical access to the vehicle. EDRs have been installed in vehicles for many years and are now in widespread use by many, if not most, automakers.

Paralleling the expansion in use of EDRs have been growing privacy concerns on the part of the American public. The U.S. National Highway Transportation Safety Administration (“NHTSA”) set standards for EDRs in 2006 but did not make them mandatory. In late 2012, the NHTSA proposed requiring EDRs for all new vehicles sold in the U.S. after September 1, 2014. In response to its proposal, the agency received numerous submissions, some expressing serious concerns about “the substantial privacy risks posed by the agency’s proposal”. As the new rules had not been released by mid-February 2015, the NHTSA has obviously deferred their implementation.

In the meantime, in response to significant privacy concerns about EDRs, fifteen U.S. states have so far adopted laws that restrict access to EDR data. The state laws require that manufacturers of automobiles equipped with EDRs disclose in the owner’s manual the fact of the EDR along with the type of data that is recorded, stored or transmitted on the EDR. All state laws treat EDR data as owned by the owner of the vehicle.

---

40 49 C.F.R. Part 563.
motor vehicle and prohibit third party access to EDRs without the express consent of the vehicle owner or operator. Exceptions include release pursuant to a valid court order or search warrant, for research purposes or for diagnostic purposes such as servicing or repairing the vehicle. In addition, some states prohibit insurance companies from requiring access to EDR data, or from penalizing a customer because they refuse to grant access to EDR data. Oregon and North Dakota statutes prohibit insurers from requiring customers to consent to allowing the insurer to access EDR data as a condition of obtaining insurance.

Washington State is an example of a jurisdiction that provides a notably robust degree of privacy protection: its statute would seem to cover telematics devices that record data (other than onboard diagnostic systems whose exclusive function is to capture fault codes for diagnostic purposes) as well as EDRs, and it covers all means of access not only to recorded information but also to information in transmission. Moreover, under the Washington statute, any person who accesses EDR data without the consent of the vehicle owner and who does not otherwise have authority under certain narrow exceptions, is guilty of a misdemeanor.

Federal legislators in the U.S. have not overlooked the issue. U.S. Senate Bill S.1925 (introduced January 14, 2014), entitled the Driver Privacy Act, would treat EDR data as belonging to the vehicle owner. It would prohibit others from accessing it without the consent of the vehicle owner except in connection with an “event” (as defined in the EDR regulations) and either pursuant to a court order, for emergency medical reasons, or for certain enumerated kinds of investigation or traffic safety research purposes, provided in both cases that neither personally identifiable information nor VIN is disclosed.

California laws

The state of California has enacted legislation to protect the privacy of its citizens in respect of certain aspects of automobile telematics. For example, s.637.7 of the California Penal Code prohibits the use of electronic tracking devices to determine the location or movement of a vehicle without the consent of the registered owner, lessor or lessee of the vehicle. California has also prohibited vehicle rental companies from using, accessing, or obtaining information relating to a renter’s use of a rental vehicle obtained using onboard electronic surveillance technology, except in limited circumstances. Rental companies must obtain the renter’s consent before using or disclosing information about the renter’s use of the vehicle. As well, California requires transportation agencies that use electronic toll collection systems to have a privacy policy that addresses collection and use of personal information, which policy must be posted on the agency’s website.

Proposed U.S. Legislation

Federal: Location Privacy Protection Act of 2014; Bill S.2171

This Bill was introduced by Senator Al Franken in March 2014, with hearings conducted by the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law in June 2014. The Bill would amend the federal criminal code to prohibit private individuals or tother non-government entities from knowingly collecting or disclosing to another person or non-government entity geolocation information from an electronic communications device without the consent of the individual using the device. Exceptions are provided for the provision of fire, medical, public safety, or other emergency services, and for collection or disclosure pursuant to a court order or a request by a law enforcement agency.

“Geolocation information” is defined as specified information that is not the contents of a communication, is generated by or derived from the operation or use of such a device, is sufficient to identify the street and city or town in which the device is located, and does not include the Internet protocol address or the home, business, or billing address of the individual. “Consent” is defined as affirmative express consent after receiving clear, prominent, and accurate notice that (1) informs the individual that his or her geolocation information will be collected, (2) identifies the categories of covered entities to which the information may be disclosed, and (3) provides the individual easy access to the collecting agency’s geolocation information website.

---

43 E.g., Virginia Code § 38.2-2213.1; 23; Arkansas Code § 23-112-107
44 Oregon Rev. Stat. § 105.935
45 Washington Rev. Code § 46.35
46 Washington Rev. Code § 46.35.030
47 California Civil Code, s.1936.
48 California Streets and Highways Code, s.31490.
Among other things, the Bill requires that an entity collecting geolocation information in an imperceptible manner, in addition to obtaining consent, provide clear, prominent, and accurate notice to the individual, not earlier than 24 hours nor later than 7 days after the initial collection, that geolocation information is being collected. It further requires that entities collecting the geolocation information of more than 1,000 electronic communications devices in a year maintain a publicly accessible Internet website that includes (1) the nature of the information collected; (2) the purposes for which the covered entity collects, uses, and discloses the information; (3) the specific covered entities to which the collecting entity discloses geolocation information; and (4) how an individual may electronically revoke consent for the collection and disclosure of such information.

California: Consumer Car Information and Choice Act, SB 994

This Bill was introduced by Senator Bill Monning in February 2014, but died without being passed. It would have extended the existing EDR-related privacy protections to all personal data collected by means of vehicle telematics. In particular, it would have required that automakers disclose to consumers what personal information they record, generate, store or collect, and provide a system for registered owners to access the information collected about them.

The Bill would also have required that automakers allow vehicle owners to opt out of vehicle-based recording, generating, storing or collection of such information other than that needed for repair or maintenance of the vehicle or for motor vehicle safety. Automakers would have been prohibited from denying any service or benefit to vehicle owners who opt out, unless the service or benefit is technically dependent on the vehicle information that is not longer recorded, generated, stored or collected due to the opt out.

The Bill would have further prohibited automakers from conditioning the sale or lease of a vehicle on the customer’s consent to allow the automaker to disclose vehicle information to persons other than the vehicle owner. It would have also prohibited the collection of vehicle information without the owner’s consent, except by court order, by a repair shop, by the automaker, or by a device for vehicle safety or traffic management purposes.

Rhode Island: Consumer Car Information and Choice Act, Senate Bill No. 2945

A similar Bill to California SB 994 was introduced in Rhode Island in May 2014. That Bill was referred to the Senate Judiciary but hearings have yet to be held.

PUBLIC SECTOR CONNECTED CAR INITIATIVES

Policy-makers and legislators are also addressing privacy concerns with respect to the adoption of telematics systems for public sector purposes such as eCall in Europe, V2V systems in the U.S., and distance taxation in Oregon.

Europe: eCall Data Protection Regulations

In mandating that all passenger vehicles be equipped with automatic emergency calling capability in the event of an accident, the European Commission did not overlook privacy issues. As explained in a Q&A provided in response to citizens concerned about the privacy implications of the new eCall system, the European Commission notes the following data protection measures:

- Any processing of personal data through the eCall in-vehicle system shall comply with the personal data protection rules provided for in Directives 95/46/EC and 2002/58/EC;
- Manufacturers shall ensure that the eCall in-vehicle system is not traceable and is not subject to any tracking before the eCall is triggered;
- In the internal memory of the eCall in-vehicle system, retention of previous locations of the vehicle is permitted, but that data must be continuously removed to ensure that only data strictly necessary to specify the current location and the direction of travel are retained. This data must not be available outside the in-vehicle system to any entities before the eCall is triggered;
- Privacy enhancing technologies shall be embedded in the in-vehicle eCall system in order to provide eCall users with the appropriate level of privacy protection, as well as the necessary safeguards to prevent surveillance and misuse;
- The minimum set of data sent by the eCall in-vehicle system shall include only the minimum as referred to in the standard EN 15722:2011 “Intelligent transport systems - eSafety - eCall minimum set of data (MSD);”
- The personal data included in the eCall in-vehicle
system shall not be retained longer than necessary for their transmission to the appropriate PSAP. Data submitted shall only be used for the purpose for which they were submitted. They shall be deleted as soon as they are no longer necessary for the purpose for which they were collected.49

United States: Adoption of Vehicle-to-Vehicle (“V2V”) Communications Technology

As noted Chapter One, the U.S. National Highway Transportation Safety Administration (“NHTSA”) is currently consulting the public on a proposal to require V2V communications devices in new light vehicles for safety purposes. The NHTSA’s research suggests that by warning drivers of impending crashes, V2V systems could help drivers avoid hundreds of thousands of crashes and hundreds of consequent deaths. In developing its proposal, the NHTSA addressed privacy concerns head-on, stating in its News Release that:

“V2V technology does not involve collecting or exchanging personal information or tracking drivers or their vehicles. The information sent between vehicles does not identify those vehicles, but merely contains basic safety data. In fact, the system as contemplated contains several layers of security and privacy protection to ensure that vehicles can rely on messages sent from other vehicles.”50

Nevertheless, in its August 2014 research report “Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application”, that was issued together with the “Advance Notice of Proposed Rule-Making”, the NHTSA devotes a chapter to “Privacy Considerations”, in which it provides the results of its interim privacy risk assessment of the initial proposed V2V system. Significantly, that assessment concludes that further privacy research is needed, with input from external security and privacy experts, in order to properly assess the privacy risks inherent in the V2V system that is ultimately adopted. In particular, the NHTSA plans to conduct further specific privacy risk assessments with respect to location tracking, identification capabilities, and privacy controls, as well as a comprehensive privacy risk analysis of all aspects of the V2V system.

While it remains to be seen how individual privacy is affected by future V2V and other ITS systems, it appears that government agencies are at least paying attention to the issue and designing the system with protection of individual privacy in mind.

CONCLUSION

Data Protection law in Canada establishes a number of obligations on organizations that wish to collect, use or disclose personal data of individual consumers. It requires that commercial organizations refrain from collecting, using or disclosing personal information without the informed consent of the individual, except in certain specified situations. It also limits the right of organizations to force consumers to agree to unnecessary collection, use or disclosure of their data in order to obtain the product or service. Moreover, it applies an outright prohibition on the collection, use or disclosure of personal data for purposes that a reasonable person would consider inappropriate in the circumstances. These limits have been applied and clarified over the last several years in various cases by courts and Privacy Commissioners, offering guidance to the automobile industry and its partners in how to ensure compliance with Canadian privacy laws as they develop and offer Connected Car services.

Also relevant to this analysis are specific regulations applied to usage-based insurance by Canadian regulators, to publicly mandated telematics in the European Union, and to similar data collection and use in the context of Event Data Recorders in the United States. Further, legislative initiatives and proposals affecting telematics in the United States and elsewhere are notable insofar as they reflect public concern and indicate a direction in which regulation of telematics is heading in that jurisdiction.

50 Notice and NHTSA report outline promise of cutting-edge technology, NHTSA 34-14, August 18, 2014.
Having explained in Chapter Six the substance of data protection law in Canada, this chapter applies the law to Connected Cars. It sets out key provisions of data protection legislation in Canada and explains how they apply in the commercial Connected Car context. Each legislative requirement is then applied, first to Usage-Based Insurance (“UBI”) as it is currently offered in Canada, then to the Automakers’ Privacy Pledge of November 2014 (“OEM Pledge”), and finally to some examples of Connected Car terms or privacy policies that were publicly accessible online.

1 This analysis does not cover public sector initiatives, such as Intelligent Transportation Systems, which are subject to different legislation governing the public sector.

2 Commitment of the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. to the Consumer Privacy Protection Principles for Vehicle Technologies and Services, November 12, 2014 (“OEM Pledge”).
Documents relied upon for UBI policies include:

- Allstate “Your Privacy Matters”, dated 2014 and accessed February 13, 2015;3
- CAA Insurance UBI Terms and Conditions, dated January 2014, accessed February 13, 2015; 4
- Cooperators Enroute Program Terms and Conditions, accessed February 13, 2015;5
- Dejardins Ajusto Program Terms and Conditions, accessed February 13, 2015;6 and
- Intact myDriving Discounts Terms and Conditions, accessed February 13, 2015.7

Supplementing our analysis of the OEM Pledge, we provide examples from various current OEM Connected Car privacy policies based on documents that were publicly available online in January/February 2015. Wherever possible, we reference policies applicable in Canada. In most cases, however, the only privacy policies applicable to Connected Car services that we could find apply in the U.S. We use these examples for illustrative purposes, looking at the North American market as an integrated whole. Specific documents that we relied upon for examples of current OEM policies include:

- FCA/Sprint Uconnect Privacy Policy effective July 1, 2014 (“Uconnect Policy”); 8
- NissanConnect Apps Services Terms and Conditions, effective July 9, 2013 (“NissanConnect Policy”); 12
- Nissan general privacy policy effective March 20, 2014 (“Nissan Policy”); 13
- OnStar User Terms and Privacy Statement, effective June 1, 2014 (“OnStar Policy”); 14
- OnStar RemoteLink Privacy Statement, last updated January 1, 2014;
- Toyota Canada Privacy Policy posted July 1, 2014 (“Toyota Policy”); 15
- Toyota USA Safety Connect Terms and Conditions effective October 20, 2010 (“Toyota Safety Connect T&C”); 16 and
- Volkswagen/Verizon Car-Net Privacy Policy, effective June 2013 (“VW Car-Net Policy”); 17

We also visited three dealerships (GM, Ford and Chrysler/FCA) in Whitehorse, Yukon on February 5, 2015 and asked them about their privacy policies and any other privacy policies relating to the vehicles they sell.

Legislative references are to PIPEDA, Schedule 1 unless otherwise specified.

APPLICATION OF DATA PROTECTION LAWS

As noted in the previous chapter, automakers, insurers and all other entities collecting, storing, using or disclosing personal data in the course of commercial activities are subject to PIPEDA or its provincial counterpart statutes.

Insurers offering UBI in Canada are also subject to provincial industry regulation. As of February 2015, the only UBI programs operating in Canada were in Ontario and Quebec. See Chapter 6 for a summary of the Ontario guidelines. In brief, the Financial Services Commission of Ontario (“FSCO”) requires that insurers comply with PIPEDA, while imposing additional duties on insurers for openness and transparency regarding specifics of their UBI programs. Furthermore, it places limits on UBI programs consistent with PIPEDA. Terms

---

5 https://enroute.cooperators.ca/
7 http://www.intact.ca/my-driving-discount-terms-and-conditions (Ontario and Quebec versions are accessed by toggling the province setting on the site)
8 http://www.driveuconnect.com/privacy/index.html
9 http://www.ford.ca/help/privacy/
10 https://support.ford.com/tools/account/sync-terms
11 http://www.honda.ca/privacy
15 http://www.toyota.ca/toyota/en/privacy/toyota
of service for UBI programs are typically more detailed than the insurer’s general privacy policy.\(^{18}\)

1. SCOPE OF PROTECTED INFORMATION

**WHAT THE LAW REQUIRES:**
Canadian data protection law protects “personal information”, which is defined as “information about an identifiable individual”.\(^{19}\)

See chapter 6 for a discussion of what this means.

Usage-Based Insurance

All UBI insurers in Canada define “personal information” as the customer’s name, address, and Vehicle Identification Number (“VIN”) in addition to the driving data collected by the telematics device. Telematics data collected about a driver is treated as “personal information” even though a given driver may not be the insured. This is consistent with Canadian data protection law.

Only Desjardins’ Ajusto terms of service address the use of “anonymized” customer data. They specify that once its third party data services provider, iMetrik, sends the Collected Data to the insurer for the purposes of assessing rate discounts, it will “anonymize and later aggregate Collected Data for the purpose of providing third parties with general information that cannot be linked to a specific vehicle (for example, aggregated traffic volumes).” The nature of the anonymization process is not explained, leaving consumers unaware of the degree to which their identities are protected by iMetrik’s de-identification process. Other insurance telematics service providers likely also use or share “anonymized” customer data for unstated purposes; many advertise the size of their databases of detailed driving data to insurers. For example, Octo, the service provider for Intact insurance, claims to have 121 billion data points collected from drivers worldwide to “deliver insight to our partners.”\(^{20}\)

**Most UBI providers do not disclose to consumers their use of anonymized customer data, and none specify the ways in which data is anonymized or the risk of re-identification.**

The Automakers’ Pledge

The OEM Pledge defines “Covered Information” as:

1. “Identifiable Information that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with Vehicle Technologies and Services; or
2. Personal Subscription Information provided by individuals subscribing or registering for Vehicle Technologies and Services.”

“Identifiable Information” is defined as “Information that is linked or reasonably linkable to i) the vehicle from which the information was retrieved, ii) the Owner of that vehicle, or iii) the Registered User using Vehicle Technologies and Services associated with the vehicle from which the information was retrieved.”

“Vehicle Technologies and Services” is defined as “Technologies and services provided by, made available through, or offered on behalf of Participating Members that involve the collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle.”

The OEM Pledge definition of “personal information” is consistent with Canadian data protection law. However, it expressly excludes aggregated or de-identified data, stating as follows:

“If Participating Members collect Covered Information and then alter or combine the information so that the information can no longer reasonably be linked to the vehicle from which the information was retrieved, the Owner of that vehicle, or any other individual, the information is no longer Covered Information. If Participating Members attempt to link the information to specific, identified individuals or vehicles or share the information without prohibiting the recipients from attempting such linking, the information becomes Covered Information.”

\(^{18}\) All of the documents reviewed in this chapter relating to UBI are from Ontario programs or programs offered in both Ontario and Quebec; the Mobiliz program, the single UBI program offered only in Quebec, does not supply a public version of their terms of service on their website.

\(^{19}\) PIPEDA s.2; AltaPIPA s.3; BCPIPA s.3; Quebec Act, s.2.

This exclusion is consistent with the OEM definition of “Identifiable Information” as information that is “reasonably linkable to” an individual. It is also consistent with the legislation as it acknowledges that re-linking data to an identifiable individual brings the data back into the category of “Covered Information.”

However, the OEMs’ implicit acknowledgement that some aggregated or de-identified data is in fact linkable back to the individual suggests that the OEMs’ concept of “reasonably linkable” excludes much data that is in fact susceptible to re-linking. As noted in the previous chapter, with the right datasets and computer technology, supposedly anonymous data can now be linked back to individuals without great effort. At the same time, de-identification technologies exist and are being further developed to address the range of needs with respect to different kinds of data with different risk profiles.21 In an era of Big Data and powerful analytics, it is incumbent on corporations and governments that want to take advantage of “aggregate”, “de-identified” or “anonymous” data to commit to a threshold of re-identification risk that is clearer than the term “not reasonably linkable.” In this context, “not reasonably linkable” needs to be more clearly defined, with reference for example to the specific level of risk of re-identification.

The OEM Pledge defines “Identifiable Information” consistently with Canadian data protection law but fails to establish a clear threshold for determining when data is “not reasonably linkable” to an individual.

OEM Policies22

OEMs typically treat “aggregate”, “de-identified” or “anonymous” data about customers as outside the scope of their data protection obligations, but policies differ in terms of their definition of this excluded data. Definitions, where they are provided, include:

- Information “that no longer reasonably identifies you or your vehicle”;23
- “Non-personally identifiable information”;24
- “Information that does not identify you specifically”;25 and
- “Information that cannot be used to directly identify you or your vehicle.”26

No OEM policy that we reviewed provided further details as to the basis on which it determines that the information is no longer linkable to an individual. OEMs typically allow themselves to use such information for any purpose or share it with any party.

OEMs typically treat aggregated customer information that does not itself identify individuals as available for any use or disclosure, without specifying the risk of re-identification.

2. OPENNESS AND ACCOUNTABILITY

GENERAL

WHAT THE LAW REQUIRES:

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. (4.8)

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization’s policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable. (4.8.1)

The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;
(b) the means of gaining access to personal information held by the organization;
(c) a description of the type of personal information

22 The “policies” we refer to in this analysis are those applying to OEM Connected Car services. OEMs typically have general privacy policies that may or may not apply to the Connected Car service. For example, GM’s general privacy policy does not apply to OnStar. However, Ford Canada’s privacy policy does include sections on Vehicle Data Recorders, 911 Assist, SYNC, Location and GPS, and Ford Works. FCA Canada’s website privacy policy refers readers to Chrysler Canada Inc.’s “complete Privacy Statement”, which is a brochure largely repeating PIPEDA requirements and providing no detail as to the collection, use or disclosure of personal data for the purposes of providing Uconnect services.
23 OnStar Policy
24 FordSYNC Policy
25 Toyota Privacy Policy
26 Uconnect Policy
held by the organization, including a general account of its use;
(d) a copy of any brochures or other information that explain the organization’s policies, standards, or codes; and
(e) what personal information is made available to related organizations (e.g., subsidiaries). (4.8.2)

What this means:

This requirement is meant to ensure transparency of commercial data processing activities, not just to customers but to the public generally. Such transparency is essential for a data protection regime that is based on the theory of consumer choice. If consumers are to be able to base their purchasing decisions on companies’ privacy practices, they need to be able to access, understand and compare the companies’ privacy policies without having to first subscribe to the service and without unreasonable effort. At a minimum:

- An up-to-date and complete version of the policy should be easily and publicly accessible online;
- The policy should be sufficiently detailed and clear that an ordinary person can understand what data may be collected, how it will be used, for how long it will be retained, to whom it may be disclosed and for what purposes, and what limits will be placed on those to whom it is disclosed; and
- The policy should provide contact information for an individual responsible for the organization’s compliance with the policy.

Usage-Based Insurance Policies

All of the Canadian insurers currently offering UBI programs provide terms of service documents and/or privacy policies for their clients describing the way the customer’s personal information is collected, the nature of the information collected, and the ways it will be used. These documents are for the most part written clearly, although with varying language levels and levels of detail. In general, an average consumer would be capable of reading and understanding their provisions. CAA is a stand-out in this category, with nicely detailed, clearly laid out, and well-written terms of service.

Contact information for a privacy officer, ombudsman, or, in the case of Desjardins, Customer Relationship Services, are publicly accessible in connection with online privacy policies or terms of service documents, although only the office, rather than the relevant individuals, are named in online materials.

Canadian UBI Program providers are providing relevant policy documents publicly, allowing consumers to see and compare the degree of privacy protection each company provides.

The Automakers’ Pledge

The OEM Pledge contains nothing with respect to openness to consumers generally. The “transparency” that it commits to is limited to owners and registered users of vehicles equipped with Connected Car services. Nor does the Pledge commit to providing contact information for the person accountable for compliance with the OEM’s privacy policy, even to owners and registered users.

The OEM Pledge fails to commit to openness and transparency as required by Canadian data protection law.

OEM Policies

OEM privacy policies applicable to Canadian customers of OEM Connected Car services are not always accessible online. The only Canadian policies applicable to Connected Car services that we were able to find were those of OnStar (whose policy refers to AT&T as the wireless service provider although AT&T is not licensed to provide service in Canada) and NissanConnect. We could find no relevant privacy policy for HondaLink nor for Hyundai BlueLink. We were able only to find policies applicable in U.S. for FordSYNC, KIA UVO, FCA Uconnect, Toyota Safety Connect and Volkswagen Car-Net, although the full privacy policies of Ford SYNC and Toyota Safety Connect could be accessed online only by registered users.

Some policies are incomplete and/or so vague or open-ended that it is impossible for readers to know what limits, if any, apply to data collected or uses and disclosures thereof. FCA US’s Uconnect Privacy Policy is relatively short and remarkably open-ended, with no limits on the personal information that may be collected nor any limits on the purposes for which it may be used by Sprint or FCA US. Moreover, the Uconnect policy lacks any notice about the customer’s right to access their personal data held by Sprint or FCA US.

Most OEM Connected Car Privacy Policies applicable to Canadian consumers are not publicly
available and therefore cannot be reviewed without purchasing the vehicle or service.

Some OEM Policies are so incomplete, vague or open-ended in certain respects that they are unhelpful other than serving as a warning that the OEM does not respect consumer privacy.

3. ACCOUNTABILITY WITH RESPECT TO THIRD PARTY PROCESSORS

WHAT THE LAW REQUIRES:
An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. (4.1.3)

What this means:

Automakers, insurers and others who provide Connected Car services to consumers typically rely upon third party service providers to provide all or part of the service. These third party service providers have no relationship with the consumer; instead, they contract with the automaker, insurer or other retail provider to conduct the necessary data gathering, storage, analysis and disclosure to enable the service to function. Because the consumer has no control over the company’s use of third parties, the company remains accountable under its privacy policy for all data processing that it outsources to third parties.

The term “processing” is not defined in PIPEDA. This leaves some uncertainty as to whether, for example, transfers to dealers for use in servicing vehicles, or to third party service providers for the purpose of providing the service, constitutes “processing.” We submit that it does, on the grounds that (a) the dealer and third party service provider are acting for or in partnership with the OEM, and (b) the consumer has no choice with respect to the disclosure.

Usage-Based Insurance Policies

In general, Canadian insurers hold their data-handling partners to the same standards of data protection as themselves. For example, Allstate’s terms state that “Modus Solutions LLC manages customer driving data on behalf of Allstate, and are bound to the same standards of Canadian privacy law and Allstate data and personal information security.”

Canadian UBI programs acknowledge their responsibility for the data handling practices of their third party service providers in relation to personal information.

The Automakers’ Pledge

In keeping with this principle, the Pledge commits to taking reasonable steps to ensure that Third-party Service Providers adhere to the Principles in providing Connected Car services. Third-party Service Providers are defined as “Companies unaffiliated with Participating Members that receive Covered Information when conducting business on behalf of a Participating Member.” It is unclear why affiliated companies are not covered by this commitment if they are providing services to the OEM.

Moreover, the Pledge expressly excludes independent dealerships, despite the fact that dealerships conduct sales on behalf of OEMs and despite the fact that consumers have no choice but to purchase through a dealer. In other words, OEMs take no responsibility for the data handling practices of their affiliated dealerships (other than the few that they own).

In their Pledge, OEMs fail to take responsibility for the use and disclosure of personal data they share with their affiliated dealers, contrary to Canadian data protection law.

OEM Policies

With the exception of Nissan, no OEM policy that we reviewed indicates that the OEM places any requirements on its dealers to protect customer data. Indeed, some policies expressly deny responsibility for their dealers’ handling of customer data, advising the customer to contact the dealer to find out about its data protection practices.

Some policies state that the OEM or joint provider of the service (e.g., mobile network operator) may share customer data with third party service providers, but provide no undertaking to use contractual or other means to ensure a comparable level of protection of

27 http://www.allstate.ca/webpages/auto-insurance/drivewise-overview.aspx
28 E.g., Ford Policy.
the data by such parties. KIA UVO’s policy states that “third party analytics service providers may set and access their own Tracking Technologies on your Device and they may otherwise collect or have access to information about you...We are not responsible for those third party technologies or activities arising out of them.”

OnStar states that it requires its third party service providers to apply similar security safeguards to the data it shares with them, but expressly denies responsibility for customer data handled by its wireless voice, wireless data and satellite radio service providers such as AT&T. It refers customers to the AT&T Privacy Statement. FordSYNC’s limited Privacy Notice states that its service providers are required to keep certain customer data confidential and are not permitted to use it for any other purpose than providing the service for Ford. Yet the data covered by this statement is limited – it doesn’t, for example, include all customer account data, vehicle health data or driver behaviour data.

Personal data is sometimes shared with these third party service providers for unnecessary purposes such as marketing or research and development, yet the OEM still does not take responsibility for the third party’s use or disclosure of the data.

OEMs share customer data with dealers but do not require that their dealers provide comparable data protection.

OEMs share customer data with wireless and other service providers in the course of providing Connected Car services, but do not always require that such third parties provide comparable data protection.

Some OEMs deny responsibility for privacy breaches by third parties to whom they have entrusted customer data.

4. INDIVIDUAL ACCESS TO HIS OR HER OWN DATA

WHAT THE LAW REQUIRES:
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. (4.9)

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual. (4.9.3)

What this means:
A critical component of data privacy is the ability of data subjects to be able to find out what information is held about them by corporations and to whom it has been disclosed, as well as to have inaccurate data corrected. This right is important not only to help ensure that decisions are made on the basis of accurate data about individuals, but also to help prevent the Kafkaesque scenario of individuals being refused services or subjected to discrimination based on information about them that they have no knowledge of nor ability to challenge.

Usage-Based Insurance Policies

In their general privacy policies, insurers typically offer customers the opportunity to review the personal data on file. Information regarding the right to dispute and request corrections to personal information is not specified in the UBI terms of service documents reviewed, but is present in the applicable company privacy policies. While it would be more convenient for consumers to have this information consolidated, particularly since in most cases the specific terms of service are deemed to have precedence over the general privacy policy, the information is accessible. Some insurers indicate that there may be a “reasonable fee” for reproducing or transmitting information in the case of a customer request for access.

In addition, as a value-added feature, UBI customers are typically provided with the ability to view their data as it is collected via the telematics device on a secure personal web portal (“personal dashboard”) at any time. The specific information made available for monitoring by customers includes the driving metrics

29 Uconnect Policy (FCA US and Sprint), VW Car-Net Policy (VW Group of America and Verizon), KIA UVO Policy.
used to assess driving behavior for the purposes of insurance discounts. Additional data or services such as “personal alerts” may be offered to customers (and not disclosed to insurers) via the third party service provider for the purpose of assisting drivers in improving their driving behaviour.

In addition to standard individual access rights, UBI providers typically allow customers to monitor their personal driving data collected via the telematics device.

The Automakers’ Pledge

The Pledge commits to offering customers “reasonable means to review and correct Personal Subscription Information” (contact and account information that individuals provide during the subscription or registration process). Beyond that, OEMs commit only to “exploring additional means of providing Owners and Registered Users with reasonable access to Covered Information...” This undertaking is not sufficient to comply with Canadian law.

The OEM Pledge does not meet legal standards in Canada for individual access to personal data.

OEM Current Policies

OEMs typically offer to provide customers with access to certain account information but not to records about one’s use of the Connected Car services. In some policies (including OnStar’s policy applicable to Canadian customers), only California residents are provided with the option of obtaining a list of their data shared with third parties for marketing purposes, along with the names of those third parties during the previous calendar year.30

OEMs typically do not permit customers to find out what information about them has been shared with third parties for purposes other than service provision, nor do they offer to provide customers (other than California residents) with the names of third parties to whom customer data has been disclosed for purposes other than service provision.

5. ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. (4.6)

Not all services require accurate information about the subscriber. However, to the extent that a Connected Car service can result in decisions that prejudice an individual (e.g., denial of insurance or higher interest rates), accuracy of the information on which such decisions are made is important. Accuracy of data used for internal company purposes or for marketing purposes is less important from a privacy perspective.

Usage-Based Insurance Policies

Data accuracy is essential to UBI, as rates are affected by the driving data. Not surprisingly, regulators require proof that reasonable processes and policies are in place to ensure the accuracy of data on which rates are determined. Insurers must also have processes in place to respond to consumer inquiries or complaints about the accuracy of the data that is used to assess discount eligibility.

UBI providers are subject to regulation requiring accuracy of the data on which they make insurance decisions about individual customers.

The Automakers’ Pledge

Participating OEMs commit to “implementing reasonable measures to maintain the accuracy of Covered Information.”

OEM Policies

OEMs typically commit to taking various measures to keep customer account information (e.g., contact information, vehicle ownership information) up-to-date, including by purchasing change of address data from licensed third parties.

OEMs have committed to taking reasonable steps to ensure accuracy of customer data.

30 in accordance with California law.
6. SECURITY

WHAT THE LAW REQUIRES:
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. (4.7)

What this means:
This provision requires that OEMs, and all of their service providers who deal with personal customer information in any way, apply security measures sufficient to protect that information from unauthorized access, whether by outsiders such as computer hackers, identity thieves or stalkers, or by insiders who have no need to see the data.

As discussed in the previous chapter, there are many different kinds of threats to personal data and many different entry points for attackers especially in wireless systems. Automakers and others who gather, store or transmit personal data must have strong firewalls and other physical IT security systems in place to protect data both in transmission and storage either on board the vehicle or in external computer systems. They must also have internal business systems that effectively address the risks of misuse of personal data by employees and third party service providers. Systems must be able to detect and respond in a timely and effective way to intrusions.

Note: Limiting access to personal data to those with a need to know is a fundamental principle of data security as well as privacy. However, it should not be used as a reason to deny car owners and their preferred service technicians access to vehicle data. Strong security can be achieved while allowing car owners the right to have their vehicles repaired by their technicians of choice.

Usage-Based Insurance
If they address security at all, the privacy policies and terms of service of insurers offering UBI make general statements, such as that provided in Allstate's privacy policy: “We take all reasonable steps to develop and maintain security measures to protect against loss, theft, unauthorized access, use, alteration, destruction or disclosure of your personal information contained in electronic and/or paper record files.” This provision applies to all personal information collected by all types of policies and is not specific to the highly detailed personal driving information collected and wirelessly transmitted to third party data service providers in the UBI program. Some insurers specifically address internal data access, specifying that personal information is accessible only by authorized personnel. Security in data transmission via wireless services is seldom dealt with directly in terms of service; only one insurer specifically mentions the encryption of data transmitted wirelessly.

Canadian insurers offer general assurances of data security in the provision of UBI.

The Automakers’ Pledge
Participating OEMs “commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.” “Standard industry practices” are considered to be “reasonable measures,” and it is noted that such practices will evolve over time in response to evolving threats and identified vulnerabilities.

The OEM Pledge offers general assurances of data security in the provision of Connected Car services.

OEM Policies
Most OEMs make similar broad statements and qualified promises about how they protect customer data against unauthorized access, use or disclosure. The Uconnect policy states that: “Sprint uses a variety of procedural, physical, and technological safeguards in our efforts to protect your information…” Ford’s general policy provides more detail, stating for instance that customer personal data is encrypted with SSL when sent to the Ford website and that personal customer data is “only accessible by appropriate personnel who have a business need for this information.”

Many policies note that the cellular network is not fully secure and state that they cannot guarantee security of customer data in transit. Some policies attempt to limit the liability of OEMs and their Connected Car service provider partners for security breaches. NissanConnect’s Terms and Conditions (s.3.6) state: “You agree that we will not be liable for any damages for any loss of privacy occurring in communication over [third party] networks.” Uconnect’s policy states: “Neither Sprint nor FCA US can guarantee that your information will never be disclosed in a manner inconsistent with this Policy (for example, as the result of illegal acts by third parties).” KIA UVO’s states: “...you provide us with your information at your own risk.” Both FordSYNC and NissanConnect policies
require customers to agree that they will not hold the companies liable for any loss of privacy occurring in communications over wireless networks.

Actual security practices of OEMs in the U.S. in 2014 were reviewed and assessed by the staff of Senator Edward J. Markey in a report entitled “Tracking & Hacking: Security & Privacy Gaps put American Drivers at Risk” (“Markey Report”). The report found that almost all cars now being sold include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions. It found that many OEMs are not keeping track of hacking incidents and that security measures to prevent remote access to vehicle electronics are inconsistent and in many cases ineffective. Finally, the report concluded that many OEMs do not appear to have systems in place to detect and respond effectively to security intrusions.

Some policies state that individual customers are entirely responsible for keeping their account information (e.g., password and/or PIN) confidential and for any unauthorized use of the services when appropriate authentication has been provided. In addition, Ford’s general policy advises SYNC customers to “erase all stored information” if they no longer plan to use the system, noting that the customer’s cell phone book, call history, past text messages, log of the last ten minutes of system activity and other information “will remain in the vehicle unless you delete them.” The policy specifies that while such data is “generally accessible only in the vehicle when the cellular phone or media player is connected”, other parties may seek to access it. While it is reasonable to make customers responsible for security measures entirely under their control, the service provider, when collecting and storing such sensitive data, must design the system so as to minimize the chance of unauthorized access. Such a design may include, for instance, automatic log-off or system shutdown and locking when the car is parked and doors opened, and automatic deletion of call history upon parking and exiting the vehicle, with options for allowing limited storage in the vehicle (which should come with warnings about security risks). We did not review or assess these practices.

**OEMs do not protect customer data according to a consistent set of industry standards, and there are serious questions about the adequacy of security measures currently applied by OEMs.**

**Some OEMs expressly deny responsibility for security breaches by third parties to whom they have entrusted customer data.**

Some OEMs make customers responsible for any unauthorized access to or use of the services when appropriate user authorization has been provided, without explaining how the service has been designed to minimize the risk of such unauthorized access or use.

### 7. PURPOSE SPECIFICATION AND NOTICE

**WHAT THE LAW REQUIRES:**

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. (4.2)

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. (4.2.3)

Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. (4.3.2)

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. (4.2.4)

What this means:

This principle is really two-in-one: first, it requires that the data collector identify internally, before collecting personal data, the reason for such collection. This forces the company to think about whether it really needs that particular data, and if it does, to specify the purposes for which it needs the data. Internal specification of purposes is an important element of fair information practices for that reason.

Second, the company must advise individual customers of the specific purposes for which it wishes to collect their data. This second part of the principle is known in the U.S. as “Notice.” Notice is critical to consent-based regimes for obvious reasons: individuals cannot consent to collection, use or disclosure that they don’t know about. Effective notice requires both:

---

• Bringing data collection to the attention of the customer; and
• Clearly explaining it so that the customer can understand exactly what data is being collected, how it will or may be used by the company, to whom it may be disclosed and what limitations will apply to the third party’s use of the data.32

“Function creep” is prohibited – new purposes require new customer consents.

Usage-Based Insurance

The reviewed insurers’ terms of service and other public-facing information on company websites are reasonably clear, and include detailed explanations of information collected via the telematics device, and how it will be used to affect insurance premiums. The terms also specify what the data will not be used for. In Ontario, for example, because telematics data is not used for claims or underwriting purposes, it may not be used to increase premiums, cancel policies, deny policy renewal, or to process or deny claims. This is stated in the policy terms. In Quebec, terms vary slightly due to regulatory differences between provinces. Policies still note that telematics data will not be used to cancel policies or refuse renewal, but neither Intact’s my Driving Discount policy nor Desjardins’ Ajusto policy refutes using telematics data when processing claims. Ajusto’s terms includes the statement that the data will not result in premium surcharges on renewal.

All reviewed terms include promises that personally identifiable information will not be used for purposes other than those to which drivers expressly consent. Insurers in Ontario also commit to making changes to the terms and conditions only on renewal of the policy; however, this is a requirement of the Insurance Act. In Quebec, advance notice is required but terms may change mid-term. Although the terms and conditions discussed in this chapter were explicitly reviewed in relation to compliance with data protection legislation, it is not possible to discuss the program differences across provinces without acknowledging the varying legal requirements for insurers that affect the way they design their programs and communicate with customers, particularly in this category of purpose specification and use.

The Automakers’ Pledge

The first principle of the Automaker’s Pledge is “Transparency”: participating OEMs commit to providing vehicle owners and registered service users with “ready access to clear, meaningful notices about the Participating Member’s collection, use and sharing of Covered Information. In addition to being clear and meaningful, notices about the collection of geolocation data, biometrics or driver behaviour data (all defined) must be “prominent.”

Members commit to “providing notices in a manner that enables owners and registered users to make informed decisions” and list the topics their notices must address:

• Types of information that will be collected;
• Purposes for which the information is collected;
• Types of entities with which the information may be shared;
• Deletion or de-identification of information;
• Choices Owners and Registered Users may have regarding information;
• Whether and how Owners and Registered Users may access their information; and
• Where Owners and Registered Users may direct questions about the collection, use, and sharing of their data.

With respect to how notices are to be communicated to customers, the Pledge notes that “there is no one-size-fits-all approach,” and commits only to posting notices on publicly available websites. Participating Members commit to “taking reasonable steps to provide Owners and Registered Users with ready access to clear, meaningful notices prior to initial collections of Covered Information.”

The Pledge commits signatories to taking “reasonable steps to alert” customers prior to changing their data practices in ways that have a material impact on the customer. It also commits signatories to obtaining Affirmative Consent (defined as “a clear action performed in response to a clear, meaningful and prominent notice...”) for new practices that involve using customer data in a materially different manner than claimed when it was collected.

Canadian insurers offering UBI programs include detailed information regarding the specific types of personal information collected and the potential uses of that data.

32 See Chapter Six, under “Meaningful Notice and Choice”.

The OEM Pledge commits to providing clear, meaningful notice in accordance with Canadian data protection law, but does not commit to bringing such notice to the attention of customers.
OEM Practices

While we did not research how OEMs bring their privacy policies to the attention of customers during the purchase/registration process, it is likely that customers of Connected Car services are required to agree, at the time that they register for the service, to a detailed set of terms and conditions that refers to a privacy policy. Given that registration may be done in the vehicle, over the phone or via the internet, customers are unlikely to be provided with a copy and may simply be referred to a website where the policy is posted. Interestingly, none of the three dealerships we visited could refer us to the OEM’s privacy policy. As noted, we were unable to find any privacy policy specific to the Connected Car service for some OEMs who sell Connected Car services,33 and for most, we could only find policies applicable to U.S. customers.

With the exception of OnStar, which commits to bringing any material changes to its Privacy Statement to the attention of customers (e.g., by email or postal mail), OEMs whose policies we reviewed allow themselves to change their privacy policies without any notice to customers (other than posting on the website).

Purposes specified by OEMs include such broad items as: “perform market research”, “improve our service”, “research”, “prevent fraud”, “internal business purposes”, and “as otherwise set forth in this Privacy Policy or our Master Terms of Service or any applicable Additional Terms.” Senator Markey’s study of U.S. OEMs found that even when asked about their practices, OEM responses were so vague and ill-defined that they leave consumers “with little knowledge about how the companies actually use their data.” Needless to say, such vague descriptions of purposes and uses meet neither the OEM Pledge nor the requirements of Canadian data protection law.

Some OEMs leave their purposes open-ended, effectively giving themselves the right to use personal customer data for any purpose. For example, FordSYNC’s policy states that: “Ford may use the vehicle information it collects, as well as information regarding individual access to Vehicle Health Reports at www.syncmyride.com for any purpose.” Worse, Uconnect’s policy states that: “Sprint and FAC US use Collected Data for a variety of purposes including but not limited to….This list is not meant to be exhaustive.” It goes on to allow the same unlimited uses by third parties to whom either Sprint or FCA US disclose the data. “Collected Data” includes, among other things, any “information about the way you use the U connect Services that helps FCA US and Sprint improve, customize or communicate about services which are offered to you.” Toyota Safety Connect’s T&Cs lists a number of uses, also ending with: “This list is not meant to be exhaustive.” Volkswagen/Verizon CarNet’s policy states: “[We] and our Service Partners and the Volkswagen Companies may intercept any wire, wireless, oral or electronic communications made or transmitted through the Service, at any time and for any reason.”34 Such open-ended purposes violate legislative requirements for purpose specification and do not meet the OEMs’ own Pledge.

OEMs typically leave it up to customers to inform themselves of applicable privacy policies and of any changes to the policies.

Some OEMs do not limit the purposes for which they collect, use and disclose customer data, allowing themselves to collect and use an unspecified amount of personal data for an unlimited range of purposes.

8. PURPOSE LIMITATION

WHAT THE LAW REQUIRES:
An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. (subsection 5(3))

What this means:
The purposes for which personal data can be collected and used are not unlimited. Regardless of consent, only those purposes “that a reasonable person would consider are appropriate in the circumstances” are permitted. See discussion in Chapter Six for detailed discussion of what this limitation means.

Usage-Based Insurance

The terms of service reviewed for Canadian insurers consistently indicate that personal information will only be used to provide insurance services, including any applicable UBI program discount. Each insurer

33 E.g., HondaLink, Hyundai BlueLink.
also specifies that personal information will not be shared with third parties for purposes unrelated to the provision of insurance services without express, opt-in consent.

This contrasts with general insurance privacy policies that may permit broader uses of customer data. For example, Allstate’s general privacy policy indicates that the company may share personal information with “selected companies which provide insurance-related and other products and services” as permitted by law in order for those companies to provide Allstate customers with information about additional products and services.

*Personal data collected for UBI purposes is not used or disclosed for any other purposes without express consent.*

**The Automakers’ Pledge**

Pledge signatories commit to limiting their purposes to “legitimate business purposes”, an undefined and ambiguous concept that effectively leaves it up to OEMs to decide what they can include as purposes for data collection. On one hand, “legitimate business purposes” could be equated with “purposes that a reasonable person would consider are appropriate in the circumstances.” On the other hand, “legitimate” could simply mean “lawful” or “conforming to accepted business standards”, neither of which is necessarily “appropriate in the circumstances.” Without a definition that meets or exceeds legal standards, the term “legitimate business practices” is too vague to be compliant with Canadian data protection law.

Participating Members also commit to “making reasonable and responsible use” of customer data, noting that “reasonable and responsible practices may vary over time as business practices and consumer expectations evolve.” This statement is circular, suggesting that it is appropriate to allow evolving business practices to determine what business practices are “reasonable and responsible” at any given time. It puts businesses, not society, in the position of deciding what limits should apply. The Supreme Court of Canada has firmly rejected such a notion, finding that the concept of “reasonable expectation of privacy” (on which Charter rights are based) is normative, not simply descriptive of what is happening in the marketplace. It does not simply describe what a person might expect given technological capability and actual business practices, but rather what a person should be entitled to expect given societal values of the day.

What purposes “a reasonable person would consider appropriate in the circumstances” may well evolve over time. Such evolution should be driven not by technology and business practices, but rather by what we as a society value and wish to protect. Taking into account the circumstances of Connected Cars – i.e., cars as essential modes of transportation for most Canadians; cars as private places; cars coming with wireless connectivity regardless of what the consumer wants; and cars gathering a range of highly sensitive data about individuals that is vulnerable to hacking - it is likely that reasonable Canadians would question the appropriateness of OEMs and their partners collecting, retaining, using and disclosing sensitive customer data for purposes other than the provision of the requested services.

Yet, the OEM Pledge includes in its list of “reasonable and responsible” ways in which they may use or share any of the customer data they collect a number of purposes that go well beyond providing the services requested, including, among other things:

- To conduct research or analysis for vehicles (use or sharing);
- To improve products and services and develop new offerings (use or sharing); and
- To engage in marketing of products and services to customers (use only).

Given the privacy risks to personal data collected by OEMs in the context of Connected Cars, treating any unnecessary, secondary uses as non-optional purposes is likely to be considered inappropriate by most Canadians.

*The OEM Pledge treats marketing, product development and improvement and internal R&D as non-optional purposes for which personal data may be used (and in the case of product development, improvement and R&D, disclosed).*

**OEM Policies**

As noted above, some OEMs do not limit their purposes for collection and use of certain personal data. For example, FordSYNC states that it may use

---

25 Other questionable purposes include “to prevent fraud”; and “to protect the ...property or rights of...Participating Members, or others”. Such purposes could be used to justify inappropriate surveillance of customers.
“Vehicle Health Reports” (including customer cell phone numbers) “for any purpose”, and Uconnect expressly does not limit the purposes for which Sprint, FCA US or any of their third party service providers may use any of the personal data they collect (moreover, their collection of data is not limited beyond broad categories).

All OEM policies that we examined include research, product improvement and/or marketing as additional non-optional purposes for collecting customer data in order to provide Connected Car services. While the extent to which OEMs share sensitive customer data with third parties for marketing purposes varies, all OEMs we surveyed reserve the right to use personal data of customers for the purposes of their own target marketing (i.e., profiling customers and customizing marketing to their particular profiles) as well as that of their business partner in the case of joint policies (e.g., Sprint/FCA; Verizon/VW).

Use of personal data for product R&D and marketing is not necessary for provision of Connected Car services. Many customers may be surprised to learn that their personal data is used for these purposes. Indeed, many customers may not want their personal information – especially their sensitive personal information – used for marketing or R&D, if only to limit the risk of unauthorized access to or use of their data. At a minimum, customers should be given a choice in the matter. In circumstances where customers are given no choice but to allow their often sensitive personal data to be collected and used for unnecessary secondary purposes such as marketing (whether by the OEM or third parties), reasonable people are likely to consider such purposes to be inappropriate.

Some OEMs do not limit the purposes for which they collect, use and disclose personal customer data.

OEMs treat marketing and product R&D as appropriate purposes for non-optional collection of sensitive customer data.

Some OEMs also reserve the right to share sensitive customer data with unnamed third parties for marketing purposes, without offering any opt-out by customers.

9. LIMITS ON COLLECTION

WHAT THE LAW REQUIRES:
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. (4.4)

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. (4.4.1)

What this means:

Automakers and others must not collect more personal data than needed for the (appropriate) purposes that they have identified and communicated to customers and to which customers have consented.

Usage-Based Insurance

The types of information that are collected by telematics devices for use in UBI are typically listed in detail in policy terms and conditions and may include any of the following:

- Vehicle location (GPS)
- Odometer reading
- Average speed
- Average acceleration
- Distance travelled
- Elapsed time of travel
- Road type
- Ignition on/off events
- Accelerometer data (acceleration, deceleration, cornering)
- Connection and disconnection status of the device
- Start and end date and time of travel
- VIN
- Mileage

According to the program terms and conditions, this data is used solely for the purpose of administering the insurance policy and providing agreed-upon insurance services, including determining if the consumer is eligible for premium discounts based on their driving behaviour. For example, the CAA terms

36 Some OEMs (e.g., FordSYNC, OnStar) limit the kinds of data that they will share with third parties for marketing purposes, while others (e.g., Uconnect) do not.
of service specify that the data is used “to build up a profile on how, where and when your vehicle is driven and to determine if you are eligible for the additional discounts.” Descriptions of data uses and the limits to such uses are provided in promotional materials for the programs as well as in formal terms of service documents, providing an additional level of accessible consumer information. Any use of personal information not expressly necessary for the provision of insurance services requires opt-in consent from consumers.

UBI programs limit the collection of personal information to that necessary for insurance purposes.

The Automakers’ Pledge

Participating Members commit to collecting customer data only as necessary for “legitimate business purposes.” Those purposes include a non-exhaustive list of numerous secondary purposes going beyond provision of the requested services.

A broad commitment to collect only that data necessary for a lengthy and non-exhaustive set of “legitimate business purposes” that includes unnecessary secondary purposes fails to ensure that personal data is not collected unnecessarily. Purposes such as “providing customers with information about goods and services that may be of interest to them” can be used to justify the collection of vast amounts of personal data in order to build profiles on each customer for the purpose of tailoring advertising pitches to each individual. This purpose has nothing to do with most Connected Car services. By lumping secondary purposes such as marketing together with the primary purpose of delivering the service in question, and by leaving the list of purposes open to expansion “as business practices evolve”, OEMs can justify the collection of far more data than they need to provide Connected Car services. On this basis alone, the OEM Pledge fails to comply with this fundamental principle of data protection and key provision of PIPEDA.

Moreover, many of the purposes identified in the OEM Pledge can be accomplished using non-personal data. It is unclear, for example, why personal customer data is needed “to conduct research or analysis for vehicles”, “to improve products and services”, or to “develop new offerings.” OEMs appear to make no effort to minimize their use of personal data in order to accomplish purposes that can be achieved with the use of non-personal data.

The OEM Pledge does not limit collection of personal data to that necessary for the purpose of the Connected Car services being provided.

OEM Policies

As described in Chapter Five, Connected Cars are now collecting vast amounts of information about customers, much of it highly sensitive. Each OEM policy lists or refers to different categories of personal data that it collects, and explains how it uses and shares the data. Some policies distinguish among different categories of data when listing uses and disclosures, but others do not. In any case, it is impossible to determine from the policies how much personal data is being collected on an ongoing basis, for which of the many identified purposes each type of data is actually necessary, and what limits, if any, are applied to the collection of any given type of data. Thus, data needed for one purpose (e.g: account data needed for the purpose of service provision) can be used for another specified purpose (e.g., marketing) even if it is not needed for that second purpose.

As with the OEM Pledge, OEM policies themselves are woefully deficient in terms of limiting collection of personal data to that necessary for provision of the service in question and any appropriate related purposes.

OEMs justify the collection of vast amounts of personal data about customers by improperly including marketing and other secondary uses in their non-optional purposes of collection.

OEMs collect so much personal data for so many purposes that it is impossible to determine the extent to which they are collecting more personal data than necessary for each purpose other than via an audit.

OEMs collect and use personal data for purposes that could be accomplished with anonymous data.

10. LIMITS ON RETENTION

WHAT THE LAW REQUIRES:

Personal information shall be retained only as long as necessary for the fulfilment of those purposes. (4.4)
What this means:

OEMs must consider the purposes for which they collected the data, then:

a) determine whether personal data needs to be retained at all in order to fulfill the (appropriate) purposes that they have specified and communicated to the customer; and
b) establish retention schedules for the personal data that they determine is necessary, for each type of use and disclosure.

Usage-Based Insurance

There is little information provided about data storage or retention periods in UBI terms of service. Allstate is typical of those that mention retention in that it does not specify a retention period, stating only that: “Files are destroyed when there is no longer any possibility of them being used or when required to do so by law.” Additionally, third party data retention policies are not addressed in the information publicly available for review. Only the CAA terms of service address what happens to consumer data when a customer withdraws from the UBI program: “CAA will continue to use the Data collected from the Device for analytics and rate filing purposes with the Financial Services Commission of Ontario.” An option to opt-out of this use in writing is provided.

Keeping personal data until there is no possibility of it being used does not meet the legal standard in Canada for data retention. More insurers should provide information regarding what will happen to customer data upon termination of the policy, and any ongoing use of personal data after the customer relationship has ended should require express, opt-in consent.

The Automakers’ Pledge

Participating Members commit to retaining customer data “no longer than they determine necessary for legitimate business purposes.” (emphasis added)

As already noted, “legitimate business purposes” is far too broad and vague a notion to satisfy the first principle of limiting purposes to those that a reasonable person would consider appropriate in the circumstances. The OEM Pledge fails the test of acceptable data retention policies on this basis alone. In addition, the Pledge sets out an entirely subjective test: OEMs permit themselves to determine what retention period is appropriate for any particular type of data or purpose. But the legal test for retention is objective, not subjective.

The OEM Pledge fails to limit the retention of personal data as required under Canadian data protection law.

OEM Policies

OEMs retain different kinds of customer data for different purposes in different places. They often entrust data retention to third parties. Yet, their privacy policies are not specific and make no distinctions among different kinds of data, different purposes and different contexts. Instead, they simply attempt to reassure customers that their personal data will be retained no longer than the OEM deems appropriate.

Actual OEM practices with respect to data retention require an audit to assess properly. However, it is worth noting that Senator Markey’s survey of U.S. OEMs found that there was a wide range of practices with ultimately no limit on retention other than the OEM’s own interpretation of “legitimate business purposes.”

OEMs retain customer data for secondary purposes such as marketing, and do so for as long as they decide is appropriate, without reference to any objective industry standards.

11. LIMITS ON USE AND DISCLOSURE

WHAT THE LAW REQUIRES:
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. (4.5)

What this means:

OEMs must either:

a) ensure that personal customer data is neither used nor disclosed for any purpose other than

37 Markey Report, p.11.
the (appropriate) purposes that were properly communicated to customers at or before collection of the data, or those purposes that customers would reasonably expect (e.g., use of contact information to send billing notices); or b) obtain consent from the individual customer for the new use or disclosure.38

Usage-Based Insurance

The terms of service reviewed for this report consistently specify that personal information is shared only with third party service providers and only for the purposes of administering a UBI policy. Consent for this information sharing is required in order to enroll in the UBI program, but the terms of service limit the third party service provider’s use of the insured’s personal data to providing insurance-related and UBI program-related services specified in the policy. Terms of service similarly indicate that consent will be expressly sought for other uses of personal information beyond those necessary to provide insurance services.39 All insurer’s terms of service specify that data may be shared with third parties where required by law.

Canadian insurers limit uses and disclosures of personal information to the purposes for which it was collected.

The Automakers’ Pledge

Participating Members commit to “using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.” The OEM Pledge states that whether a given use or disclosure is “consistent with context” depends on a number of factors, including whether the customer was notified of it, gave permission for it, can reasonably be expected to have agreed to it, and “how the use or sharing will likely impact them.” In particular, all uses and sharing that are set out in “clear, meaningful notices” are considered to be “consistent with the context of collection.”

The Pledge requires customer consent in only two circumstances:

1. Use of Geolocation, Biometrics and Driver Behaviour data “as a basis for marketing”; and
2. Sharing such data with unaffiliated third parties for their own purposes.

While the Pledge appears to be consistent with the principle of limiting use and disclosure, it is deficient in a number of respects:

1. The purposes for which customer data is used or disclosed may not meet the requirement of “appropriateness”;
2. Despite “clear, meaningful notice”, customers may not be aware of the uses and disclosures. The Pledge considers it sufficient for OEMs simply to post their privacy policies online, thus shifting the burden to customers to go online, find the Privacy Policy, and inform themselves as to the proposed uses and disclosures;
3. Other than in a narrow set of circumstances, the Pledge does not require that OEMs obtain customer consent for new uses and disclosures, either via opt-in or opt-out mechanisms; and
4. The Pledge appears to allow OEMs to use or disclose sensitive customer data in ways that may not be specified in the notice or that the customer has expressly not permitted, if the OEM determines that the impact on the customer is negligible.

The OEM Pledge allows OEMs to use and disclose personal data of customers for unnecessary purposes without informed consent of customers.

OEM Policies

As already noted, some OEMs do not limit their uses of the vast amounts of personal customer data that they collect in the course of providing Connected Car services. Specified uses are often worded in such broad and vague terms as to be of little help to customers wishing to understand how their personal data may be used.

With some limited exceptions (e.g., using location data for marketing purposes), customer consent to listed uses is not sought and customers are given no option to refuse to allow their personal data to be used for such unnecessary, secondary purposes as marketing or product improvement.

With respect to sharing customer data with third parties, OEM policies are somewhat more restrictive but still fail to meet Canadian legal requirements insofar as:

---

38 unless the use or disclosure is required by law.
39 Third party service providers are however allowed to use aggregate non-personal data for purposes outside the scope of the policy terms without consent.
a) Marketing or any other secondary purpose for which the OEM shares personal customer data is not a purpose that “a reasonable person would consider appropriate in the circumstances” where no opt-out is offered; and

b) Consent to the sharing has not been expressly provided and cannot reasonably be implied.

OnStar, for example, states that it may share “Account Information” (which includes communications metadata and “information about how you use your vehicle’s features and systems”) and “Vehicle-Related Information” (which includes VIN, refueling data, ignition status and collision information among other things), but not “Driving Information” (which includes GPS speed and location data), for marketing purposes with GM, GM dealers, wireless telecommunications providers and other third parties with whom OnStar contracts. FordSyNC puts more limits on what third parties can do with personal data that Ford discloses to them, stating that it will not share location data, call recordings or call details pertaining to customer use of the SYNC service with independent third parties for their independent use unless required by law, in exigent circumstances, or to protect Ford’s property or legal rights. Ford’s general privacy policy states the same restriction differently: Ford will not share personal data provided by the customer to Ford with any third parties for their own independent marketing purposes or uses without the customer’s consent. Uconnect’s policy states that Sprint and FCA US may share Collected Data with each other as well as with any third parties who facilitate or provide some aspect of the Uconnect services, for any use whatsoever (the list is explicitly non-exhaustive).

In all cases, as with internal marketing and R&D, customer consent is not sought for most sharing of the customer’s data - regardless of how sensitive the data - and customers are given no option to refuse sharing with third parties, even for such unnecessary secondary purposes as marketing or product improvement.

OEMs use customer data for a wide range of sometimes vaguely worded purposes including marketing, R&D and other secondary uses, without clear customer consent. The OEM Pledge would require consent for the use of certain sensitive data for marketing purposes.

OEMs share customer data with third parties for a wide range of sometimes vaguely worded purposes including marketing, without clear customer consent. The OEM Pledge would require consent for sharing with unaffiliated third parties.

12. INFORMED CONSENT (CHOICE)

WHAT THE LAW REQUIRES:
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. (4.3)
The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. (4.3.4) In obtaining consent, the reasonable expectations of the individual are also relevant. (4.3.5)

What it means:
Informed consent is required for all collection, use and disclosure of personal information. There are three ways in which consent can be obtained:

1. Implied consent – where the individual provides his or her data directly to the OEM and where the use or disclosure in question is so obvious that it need not be set out in a notice.
2. Opt-out consent – where consent can reasonably be assumed based on notice of the proposed collection, use or disclosure and an opportunity to opt-out (or refuse the service) that is not exercised.
3. Express consent – where the customer, having been informed of the proposed collection, use or disclosure, provides affirmative consent without which the collection, use or disclosure will not proceed.

Usage-Based Insurance

UBI programs in Canada are currently voluntary. All of the Canadian insurers offering UBI programs must acquire express signed consent from insured persons to all proposed collection, use and disclosure of personal information at the point of program enrolment.

Consumers may withdraw their permission for the use of their personal information at any point, but this withdrawal will result in their removal from the UBI discount program, although not in the complete cancellation of their policy if it is midway through their term.
Data collection functions of the telematics device are under consumer control insofar as individuals can simply remove the device from their vehicle. But such functions must be active in order for insured persons to remain enrolled in a UBI program and policy discounts will be forfeited if the device is removed for a period of time exceeding limits specified by each insurer.

**Insurers obtain express, informed consent of customers to all collection, use and disclosure of customer data for UBI programs.**

### a) IMPLIED CONSENT

An individual is deemed to consent to the collection, use or disclosure of personal information by an organization for a purpose if

a) at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person, and

b) the individual voluntarily provides the personal information to the organization for that purpose. (BCPIPA, s.8(1))

**What it means**

The customer’s knowledge and consent to some collection, uses and disclosures of their data are obvious and can reasonably be implied even without express notice – for example, collection of account data directly from the customer and use of such data to bill for service. In the context of Connected Cars, most data collection, uses and disclosures are not obvious to the customer and need to be explained in order to ensure that the customer is informed. There are few instances of properly “implied consent” in the Connected Car context.

### b) OPT-OUT VS. EXPRESS CONSENT

An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. (4.3.6)

An organization may collect, use or disclose personal information about an individual for specified purposes if

a) the organization provides the individual with a notice, in a form the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual’s personal information for those purposes,

b) the organization gives the individual a reasonable opportunity to decline within a reasonable time to have his or her personal information collected, used or disclosed for those purposes,

c) the individual does not decline, within the time allowed under paragraph (b), the proposed collection, use or disclosure, and

d) the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances. (BCPIPA s.8(3))

**What this means:**

This provision acknowledges that there are different ways of obtaining consent (opt-in vs. opt-out) and directs OEMs to take into account the sensitivity of the customer information as well as the reasonable expectations of the individual when deciding whether it can fairly rely upon opt-out consent.\(^{40}\)

If the information is likely to be considered sensitive, the default must be not to collect, use or disclose the data, and consent must be obtained expressly, through an “opt in” process. While any data can be sensitive depending on the context, it is generally the case that driver behaviour data, biometric or health data, location data, communications and infotainment use data is sensitive. In terms of general categories of data, only vehicle health data would not be considered

---

\(^{40}\) PIPEDA Sch.1 4.3.4 - 4.3.7; Alta PIPA, subs.8(3); BCPIPA subs.8(3).
sensitive per se. Unless the context clearly renders generally sensitive data into non-sensitive data, companies are required to use opt-in forms of consent; they cannot assume that customers have consented based on notice alone or even notice with an opt-out. De-identifying customer data to the extent that re-identification requires a level of effort that third parties are unlikely to engage in may constitute a context that reduces the sensitivity of personal data to make opt-out consent acceptable.

The reasonable expectations of the customer are also relevant. In order to be allowed to assume the customer’s consent to a particular collection, use or disclosure of their data, the OEM must be able to show that the customer would reasonably have expected that collection, use or disclosure based on the context or the notice provided. If the notice is not properly brought to the attention of the customer, or if it is so vaguely or broadly worded as not to clearly encompass the particular use or disclosure, OEMs cannot rely on the notice to assume informed consent on the part of the customer.

The Automakers’ Pledge

The Pledge commits Participating Members to obtaining express (“Affirmative”) consent for only two particular practices:

1. Use of personal Geolocation, Biometrics or Driver Behaviour data for marketing; and
2. Sharing of Geolocation, Biometrics or Driver Behaviour data with unaffiliated third parties for their own purposes, including marketing.

Consent is assumed for all other collection, use and disclosure, and, contrary to Canadian data protection law, there is no commitment to offering mechanisms by which customers can opt-out of non-essential collection, use or disclosure of their data.

The OEM Pledge fails to require customer consent for even non-essential collection, use and disclosure of customer data, contrary to Canadian data protection laws.

OEM Policies

Policies often leave open the possibility of additional uses or disclosures with the consent of the customer.

Examples include:

- Ford’s policy of not sharing personal customer data with third parties for their own independent marketing purposes or use, without additional customer consent, and;
- OnStar’s policy of obtaining the customer’s “prior additional consent” before using location data for marketing purposes, and before sharing a customer’s “Driving information” (GPS location, speed, safety belt usage and other information about how the vehicle is used) with unaffiliated third parties.

Otherwise, none of the policies we reviewed rely upon affirmative consent for the collection, use or disclosure of any customer information for any listed purpose. Instead, consent is simply assumed for virtually all collection, use and disclosure set out in the policy, regardless of the sensitivity of the data.

Opting-out of certain data collection, use or disclosure is very limited if offered at all. Typically, the only opt-out is for receipt of marketing communications: customers can ask not to receive promotional messages from the OEM or its partners, but they cannot stop the OEM from using their personal data (e.g., from profiling them) for marketing purposes. NissanConnect is an exception: its policy states: “You may at any time withdraw your consent for the future use of data for promotional purposes.”

The OEM Pledge not to use location data, biometrics or driver behaviour data for marketing purposes without the express consent of customers is a major step forward. However, it ignores the communications and infotainment data that OEMs can now gather and combine with vehicle data via Connected Cars. This gap needs to be addressed, not just by automakers but also by mobile network operators and mobile device operating system providers who are involved in the data gathering and who engage in the same practices. The OEM Pledge also ignores vehicle health data, which could be used in combination with infotainment data for marketing purposes against the customer’s desires.

The OEM Pledge not to share location data, biometrics and driver behaviour data with unaffiliated third parties for their own purposes without the customer’s express consent is another important step forward.

---

41 See Chapter Five for a more extensive discussion of data sensitivity.
42 OnStar’s policy suggests that customers may have other choices they can exercise with respect to the collection, use or sharing of their personal data and states “To learn about the choices available to your, please contact us at privacymanager@onstar.com.”
However, it also leaves open the possibility of an OEM sharing vehicle health data and/or customer communications and infotainment use data with third parties for their own use, without the customer’s express customer consent.

**OEMs assume consent by customers to the collection, use and disclosure of vast amounts of often sensitive personal data, for a wide range of purposes many of which are not essential to provision of the services in question.**

*With limited exceptions, OEMs do not allow customers to opt-out of listed uses or disclosures of their personal data even where such uses or disclosures are not essential to provision of the service.*

**OEM policies do not provide sufficient detail for customers to understand the uses to which their personal data may be put.**

### 13. REFUSAL TO DEAL

**WHAT THE LAW REQUIRES:**

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. (4.3.3)

An organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service. (BCPIPA, s.7(2))

**What this means:**

This provision prohibits companies from requiring customers to consent to unnecessary data collection, use or disclosure. Secondary uses of personal data collected in order to provide Connected Car services (e.g., marketing and product improvement) must not be forced on customers through terms of service. Instead, consent must be obtained, either through an opt-in process or, if the data is not sensitive and the privacy risks are low, through an opt-out process. Otherwise, only non-personal data can be used for secondary purposes. Policies that do not offer customers the ability to opt-out of all collection, use or disclosure of their personal data that is not necessary for the service in question violate the refusal to deal rule.43

### Usage-Based Insurance

No Canadian insurers require consent to non-essential collection, use or disclosure of personal customer data in order for consumers to sign up for UBI. In Ontario, secondary uses are expressly disallowed without clear, opt-in consent on the part of the customer. In Quebec, despite lack of similar regulation, the terms of service reviewed clearly specify that consumers are consenting to the use of their data by the insurer or third party service providers only for the purposes of administering their policy.

**No provider of UBI in Canada requires that customers consent to any non-essential collection, use or disclosure of their data in order to sign up for the UBI program.**

### The Automakers’ Pledge

The OEM Pledge allows OEMs to refuse to provide Connected Car services to customers who do not consent to having their personal data collected, used or disclosed for marketing or other unnecessary purposes that the OEM may insist upon, except with respect to:

1. the use of location data, biometrics or driver behaviour data as a basis for marketing; and
2. the sharing of location data, biometrics or driver behaviour data with unaffiliated third parties for their own purposes.

For these two categories of secondary use and disclosure, express opt-in consent of the customer is required. However, consent is simply assumed for all other collection, use and disclosure of customer data and the Pledge offers consumers no choice with respect to other non-essential collection, use or sharing of their personal data.

Moreover, there is no attempt by OEMs otherwise to separate essential from non-essential uses, or to categorize data according to its sensitivity and treat it accordingly.

**The OEM Pledge violates the “refusal to deal” rule in Canadian data protection law except with**

---

43 See Chapter Six for more discussion of the “Refusal to Deal” rule.
respect to the use of certain kinds of customer data for marketing purposes and the sharing of such data with unaffiliated third parties for their own purposes.

OEM Policies

While most policies we reviewed allowed customers to opt out of receiving marketing communications, few allowed customers to opt out of having their data collected, used and/or disclosed for marketing purposes in the first place, and none allowed customers to opt out of other unnecessary uses of their personal data such as R&D or product improvement. FCA US customers must cancel the service entirely if they don’t agree to any of the unnecessary uses and disclosures set out in the policy or if they don’t want to give a blank cheque to FCA US and Sprint with respect to their data. OnStar’s policy states that: “some collection and sharing practices are tied to the Services we offer. To stop the collection or sharing of some information, you may have to decline those Services or be willing to accept limited functionality.” After listing a number of purposes for collection of location and other information, FordSyNC’s Privacy Notice states: “If you don’t consent or wish to disclose this information, do not activate or use SYNC Services.”

Senator Markey’s survey of U.S. OEMs also found that “Customers often cannot opt out without disabling valuable features such as navigation.”

OEMs often require that customers agree to unnecessary collection, use or disclosure of their personal data in order to register for Connected Car services.

CONCLUSION

Usage-based insurance programs in Canada are currently compliant for the most part with data protection law, reflecting the ability of sectoral regulators to require that any insurer offering UBI meet specific requirements with respect to consumer privacy and choice.

In contrast, in their actual and proposed provision of Connected Car services, automakers are non-compliant with Canadian data protection law in various respects. Indeed, our review of publicly available terms and policies suggests widespread disrespect for the privacy of customers by companies offering Connected Car services. The privacy pledge issued by a large group of major automakers in November 2014 is promising but falls far short of Canadian legal standards. In particular, it does not meet Canadian legal standards with respect to openness, accountability, individual access, consent, or limiting collection, retention, use and disclosure of personal data. Nor, in our view, does it meet the requirement for purposes to be limited to those that a reasonable person would consider appropriate in the circumstances.

A non-comprehensive review of current Connected Car privacy policies and terms of service confirms deficiencies apparent from the OEM Pledge, and more. Particular concerns include:

- Failure to make privacy policies publicly available for consumers to consider when shopping for Connected Cars;
- Treating website posting of policies and policy changes as effective notice to customers;
- Treating aggregate customer data as non-personal data without specifying the level of risk of re-identification;
- Failure to take responsibility for personal data shared with dealers and service providers;
- Failure to offer customers access to more than basic account data or to a list of companies with whom their personal data has been shared for marketing purposes;
- No clear limits on collection or retention of personal data;
- Lack of customer choice with respect to non-essential collection of personal data;
- Lack of choice with respect to non-essential uses of personal data;
- Lack of choice with respect to non-essential sharing of personal data with affiliates, dealers and service providers; and
- Refusing to provide services to customers who do not agree to allow their personal data to be collected, used or disclosed for non-essential purposes.

In the case of both UBI and Connected Car services, insurers and automakers alike typically treat “aggregated” data as free of restriction but fail to provide more than unspecific assurances that such data cannot reasonably be re-linked to individuals. In an environment of increasingly powerful data analytics, such assurances are less and less credible. This issue needs to be addressed, along with other deficiencies in OEM provision of Connected Car services.
CONCLUSIONS AND RECOMMENDATIONS

“...if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated.”

Cars are private places in which Canadians spend a great deal of time and conduct a great deal of personal business. Where people go, how they drive, and what they do in their vehicles are private matters that, especially when tracked and combined, can reveal intimate details of a person’s life. According to the Supreme Court of Canada, it is exactly this kind of data in which, Canadians have a reasonable expectation of privacy.

Until recently, cars functioned simply as a mode of private transportation, albeit one on which Canadians are highly dependent. With wireless connectivity and telematics, however, cars are now much more than modes of transportation – in addition to serving as mobile communications portals and Wi-Fi hotspots, they are quickly becoming vast data harvesting devices. As a key component of the expanding Internet of Things, Connected Cars are now feeding the Big Data machine and in particular, the increasingly personalized and targeted commercial marketing industry. The same technologies that create this data also create new security risks. Besides exposing vehicle operations to malicious hacking through new wireless entry points, they are creating huge new databases of personal data that is vulnerable not only to unauthorized access but also to unexpected use by governments, law enforcement agencies, insurers and others seeking to identify, monitor or take action against individual drivers or car owners.

In part, the Connected Car functions as another mobile device, raising the same unresolved privacy issues as mobile devices and the applications running on them. However, Connected Cars are much more than mobile communications devices: they generate a whole new universe of data about the vehicle being driven and how it is being driven – data that is valuable to insurers, litigants, governments and law enforcement agencies as well as commercial entities seeking to develop new revenue sources. Moreover, they provide a context in which to place the data generated by onboard communications that significantly enriches the data generated. Knowing that a person is in a particular location is one thing; knowing that they are in their car in that location is another. It is therefore not surprising that the data analytics and marketing industries are at automakers’ steps, clamouring for access to this new treasure-trove of consumer data.

The Connected Car offers undeniable benefits to car owners and drivers. However, it is not just about connecting drivers to services. It is also about automakers being able to monitor their vehicles and connect directly with their customers. Less obviously to consumers, it is about various service providers connecting with the data generated by Connected Car services to leverage their competitive intelligence about what happens in the car. Automakers are not the only commercial entities availing themselves of this new source of revenue; their partners and service providers are also doing so. Indeed, the Connected Car “data rush” has already started, with telecommunications and telematics service providers leading the way, and Google hot on their heels with its evolving infotainment operating system for cars.

In the frenzy to take advantage of this new technology and keep up with the competition, automakers and their corporate partners appear to have ignored Canadian data protection laws. Our review of Connected Car terms of service and privacy policies (those we could find) indicates that automakers are failing to meet their legal obligations under almost every principle of data protection law. The Consumer Privacy Protection Principles adopted by several major automakers and released in November 2014 are promising, but fail to meet the standards of Canadian data protection law in numerous respects including openness, accountability, individual access, notice, consent, and limiting collection, retention, use and disclosure to that necessary for purposes that reasonable Canadians would consider appropriate in the circumstances.

A certain amount of data collection, retention, use and disclosure is necessary for Connected Car services to work, and it is fair to require customers to agree to some data gathering in order to use the service. However, Connected Car service providers, with the exception of insurers, are currently requiring customers to agree to various unnecessary uses and disclosures of their personal data as a condition of subscribing to the service. Purposes include marketing and product development, as well as “research”, “safety”, “prevention of fraud” and “business purposes”. The OEM Pledge does not alter this except with respect to location data, biometrics and driver behaviour data, for which affirmative consent is required for use “as a basis for marketing” and for sharing with unaffiliated third parties for their own purposes. That leaves customer account data, vehicle data, communications and infotainment data free for OEMs to collect, use and disclose for whatever purposes they specify as a condition of providing the service.

This is a blatant violation of data protection law in Canada. Use of any personal data for secondary purposes such as marketing is unnecessary and
therefore, at a minimum, requires clear, informed customer consent – not “consent” assumed by virtue of use, nor “consent” buried in a long and detailed set of terms that no one is expected to read and that may be changed at any time without notice. Use of sensitive data such as communications, contacts or infotainment use for unnecessary purposes requires more care in the form of affirmative consent. Yet OEMs are neither obtaining nor promising to obtain express consent for anything other than the particular categories of data, uses and disclosures identified above. This “all or nothing” approach to the collection, retention, use and disclosure of different types of data for multiple purposes, some of which are not necessary for provision of the service, does not comply with Canadian data protection law. By failing to distinguish between essential and non-essential purposes, and then failing to obtain informed consent from customers to collection, use or disclosure of their personal data for non-essential purposes, Connected Car service providers are violating a fundamental principle of data protection law. As well, by failing to identify the personal data needed for each separate purpose or to limit their collection and retention of personal data to what is actually needed for each purpose (using data silos as appropriate), OEMs and their service providers are further offside Canadian data protection laws.

It is evident that automakers, like many other service providers in the digital economy, are categorizing secondary uses of information as “legitimate business purposes” that do not require consent. But in the context of cars (i.e., essential modes of transportation for most Canadians; private places; increasingly telematics-equipped by default) and in the context of Connected Cars, which gather a range of sensitive personal data that is vulnerable to unexpected uses and misuses, it is likely that reasonable Canadians would consider the non-optional collection, use or disclosure of their personal data for purposes other than those necessary to provide the requested services as inappropriate. Thus, what might in other contexts be “legitimate business purposes” (e.g., marketing) are not legitimate purposes under PIPEDA. This is a major deficiency in the OEM Pledge and, in our view, a serious violation of data protection law.

On the other hand, by focusing on context rather than forms of consent, the OEM Pledge implicitly acknowledges that models of data protection based on meaningful consumer choice are unworkable in this industry. There are too many players in the Connected Car ecosystem. Many of these players have their own terms of service and privacy policies that consumers are expected to read, understand and agree to (or else seek an alternative with a more acceptable policy). Meaningful consent in this context is virtually impossible. Even if OEMs competed on privacy and provided more privacy options in their terms of service, average consumers simply do not have the time, never mind the expertise, to review and take into account so many different terms of service and privacy policies.

And the reality is that OEMs do not compete on privacy. The focus of automobile marketing is on excitement and functionality, not data protection. In any case, privacy is just one of many factors in a consumer’s purchasing decision. Moreover, the complexity of telematics data gathering and management makes it difficult, if not impossible, for consumers to make informed decisions based on OEM privacy statements. Furthermore, as the OEM pledge suggests, there is convergence in the industry with respect to data collection, use and disclosure; if all of the OEMs adhere to the same policy of requiring consumers to consent to secondary uses of personal data for purposes such as research or marketing in order to receive Connected Car services, there is no real choice for consumers at all.

Rather than relying on the fiction of choice and consent, what is needed in this industry are clear, specific and relevant limits on collection, retention, use and disclosure of personal customer data. We need industry-specific data protection regulations for the Connected Car industry.

“It’s just really important that we have boundaries and guidelines to operate. Our homes, the cars, everything is going to be on the Internet. Everything’s going to be connected. And so what are the guidelines? What do we want?” Then Ford CEO Alan Mullaly, speaking to reporters at the 2014 Detroit auto show.2

We have seen fit to place strict limits on Event Data Recorders; why not apply the same limits on wireless disclosure of the same data? We have seen fit to impose strict limits on the use of telematics for insurance purposes in some jurisdictions; why not for every jurisdiction, and for all other purposes that raise similar privacy concerns? Public sector Intelligent Transportation Systems such as V2V are being
designed with privacy as a foundational principle; why not ensure that privacy is designed into private sector Connected Car systems as well?

Concerns about motor vehicle safety have led to the development of extensive safety standards that are enforced through regulations under the Motor Vehicle Safety Act. The vulnerability of vehicle telematics data to hacking raises a new kind of safety concern - one that has yet to be addressed through industry regulation. As the Markey Report and ongoing testing demonstrates, Connected Cars are vulnerable to malicious hijacking of vehicle operations, as well as to theft and misuse of personal data. Motor vehicle safety standards and regulations need to be updated and expanded to cover this new, serious threat to North American drivers.

The most effective way to protect data is to **not to collect or retain it in the first place**. This should be the starting point for data protection standards in the automobile industry: hard limits on purposes for which personal data may be collected and the collection of data, by type of data and approved purpose. There are serious risks to individual privacy through over-collection and over-retention of data in the context of Connected Cars. There are no longer any significant technological limits on data collection and storage, and entities with vested interests in monetizing data cannot be expected to forego opportunities to do so. Instead, we must use law and policy to establish and enforce appropriate limits on the collection, retention, use and disclosure of personal data in the Connected Car context. Such limits will then guide “Privacy by Design” approaches to the development of Connected Car systems, establishing standards by which aftermarket telematics services can be judged.

In the not too distant future, all cars will be connected one way or another. Consumers will have no choice in that respect. Without strict, legally enforceable standards that do not rely on fictional consent, that go well beyond the standards committed to by OEMs in their Privacy Pledge, and that meet the requirements of data protection law, individual privacy - and likely the reputation of automakers - will suffer irreversible damage. Now is the time for industry stakeholders, regulatory bodies, government agencies, consumer advocates and experts in the field to come together and develop appropriate data protection standards for the North American automobile industry.

Now is also the time for insurance regulators to develop data protection standards for usage-based automobile insurance, together with insurers, brokers, privacy commissioners and consumer organizations. Usage-based insurance is one choice among many automobile insurance products at the moment, but if it grows in popularity, driven by discount-based promotions in the initial years of offering, premiums based on individual driver behaviour could become the industry standard. Even if the programs remain voluntary, there is a risk that insurers may at some point choose to penalize drivers who do not ‘voluntarily’ choose to participate, and drivers could one day be faced with the difficult choice between obtaining affordable insurance and surrendering their right to privacy. Such a result needs to be avoided.

Right now, as we have detailed in this report, the majority of UBI programs are in Ontario and subject to strong regulation. As a result, we have assessed UBI compliance with data protection legislation positively. But there is no guarantee that other provinces will enact similar regulations. Indeed, in Quebec no such regulation is in place although plans are being developed to expand the use of telematics-based insurance in that province. Furthermore, there is no guarantee that even the Ontario regulations won’t change over time as UBI becomes more established in the marketplace. In the absence of strong guidelines, UBI poses the same risks of data over-collection, unexpected uses, and unpredictable consequences for consumers that we currently see in the broader Connected Car ecosystem. Rather than waiting for insurers to push the limits of privacy and dealing with applications by insurers to offer UBI products on a one-off basis, jurisdiction by jurisdiction, provincial and territorial insurance regulators and privacy commissioners should work together with the industry to develop national standards that meet the need for consumer choice as well as data protection.

**RECOMMENDATIONS**

**Recommendation #1: Establish data protection regulations for the Connected Car industry.**

The legal obligations set out in **PIPEDA** and related data protection legislation are purposefully broad, designed as they are to apply across sectors. It is up to each industry sector to apply the law in its own context - to develop industry-specific standards, guidelines and policies that translate general data protection standards into specific standards applicable to that industry sector. Until recently, the automobile industry was not a big player in the market for personal data. That has changed dramatically with telematics: automakers and their various service
providers are now central players in the data market. They need industry standards, not just to guide themselves in meeting legal requirements but also to ensure a level playing field for the industry.

Once such standards are developed and implemented by OEMs and their service providers, market forces should be sufficient to ensure compliance by aftermarket providers.

Data protection regulations for the automobile industry could be enacted under the regulation-making powers of PIPEDA and related provincial legislation. Security-related regulations could also be enacted under the federal Motor Vehicle Safety Act, alongside the existing Canada Motor Vehicle Safety Standards.

The process for developing data protection standards should involve all stakeholders, including Privacy Commissioners and interested consumer organizations. It could be led by Industry Canada, given that department’s expertise in digital policy and past experience and success in working with multi-stakeholder groups to develop privacy and security-related standards and guidelines for industry. It could also be led by Transport Canada, with its knowledge of the automobile industry and experience developing motor vehicle safety standards, but digital policy expertise would also be needed. A joint initiative of both departments would make sense.

The time is ripe for such an initiative; if left too long, business practices and expectations will become entrenched and it will be difficult and costly for industry players to change their approaches. The industry needs guidance now.

Specific Data Protection Standards for the Connected Car Industry

Our analysis of the OEM Pledge and publicly available Connected Car policies identified numerous deficiencies with respect to Canadian data protection legislation. The following are some recommendations for compliance:

- All OEMs should take responsibility for their dealerships’ handling of customer data and should require their dealerships to adopt and adhere to the OEM’s privacy policy.
- OEMs should take responsibility for the handling of customer data by all of the service providers they use in the provision of Connected Car services, and should require that all such service providers protect customer data to a degree comparable to that provided by the OEM.
- OEMs should establish systems that permit customers to find out what information about them is being collected via Connected Car services and to whom it has been provided for purposes other than provision of the services in question.
- OEMs should ensure that their Connected Car services are designed with default privacy-friendly settings.
- Where OEMs are relying on customer consent, notice of the practice in question must be brought to the attention of the customer, as well as clearly worded and comprehensively explained so that the customer can understand exactly what they are agreeing to. Affirmative consent is always preferable to opt-out consent. Personal data of customers should not be collected without the customer’s awareness except as demonstrably needed to provide the service, or as expressly consented to by the individual.
- Consent should not be assumed merely by virtue of use of the service other than for obvious purposes that a reasonable person would understand and agree to.
- Consent to use or disclosure of one’s personal data for secondary purposes such as marketing, product improvement or research and development should never be assumed. It should always be explicit and affirmative.
- Connected Car services should not be denied to customers who refuse to agree to let their personal data be collected, used or disclosed for unnecessary purposes.
- All OEMs should establish and adhere to retention schedules for personal customer data.
- Before treating “aggregate” customer data as outside the scope of protected information, organizations should assess the risk of re-identification using scientifically accepted methods. Only where the level of risk of re-identification is statistically insignificant should such data be treated as non-personal data.

A number of the problems identified in our analysis of Connected Car services are not unique to the automobile industry. Just because they are endemic in
other sectors does not mean the problems should not be addressed. Indeed, the fact that a given practice is widespread may be reason to make addressing it on a broader scale a priority.

**Recommendation #2: Develop national data protection standards for usage-based insurance.**

UBI is regulated at the provincial level, and is only just beginning to be offered in Canada. Rather than having each provincial and territorial regulator develop its own set of standards for UBI, a working group should be established with industry stakeholders including the Insurance Bureau of Canada, the Insurance Brokers Association of Canada, insurance companies, provincial associations, provincial regulators, and the federal and provincial privacy commissioners to develop national standards for use by each provincial/territorial regulator. A standards-based approach would allow provincial regulators to customize their approaches to UBI based on provincial needs and priorities. It would also lower the cost of compliance for private insurers operating in more than one jurisdiction. Finally, and importantly, it would provide Canadian consumers with a consistent, and persistent, level of protection across the country.

Specific Data Protection Standards for Usage-Based Insurance should recognize that any telematics data that can be linked to an individual, whether the driver or not, constitutes “personal information” under data protection law, and should require that:

- Current terms of service and privacy policies are made publicly accessible via insurers’ websites.
- Insurers are responsible for ensuring that all aspects of a UBI program meet the requirements of relevant privacy legislation, and are accountable for compliance with such legislation.
- Insurers are accountable for all personal information collected for the purposes of administering their UBI programs. This includes responsibility for ensuring their third party service providers comparable levels of protection for customer data.
- The specific types of data collected by insurers or their third party service providers through the telematics devices are clearly detailed in the policy terms of service.
- The policy sets out data retention policies, including what happens to the personal data of customers when they withdraw from the UBI program.
- All possible use(s) of the collected data are clearly indicated in terms of service. In particular, consumers need to know if their information will be used for underwriting, for claims investigation, or to cancel or refuse policy renewal, as such uses could have significant consequences for individuals.
- Secondary uses of personal data – i.e. beyond that necessary for administration of the UBI program – are assessed for appropriateness before being approved by the regulator.
- Express, opt-in consent is obtained from consumers to all permitted collection, use or disclosure of their personal data for secondary purposes;
- Personal information is transmitted, stored, and deleted in accordance with appropriate security standards.
- Insurers retain personal information no longer than necessary for the purpose of providing the service.
- UBI programs are voluntary and require express, informed consent on the part of the insured person to the collection, use and disclosure of personal information by the insurer and third party partners.
- Insurers provide policy-holders with access to their collected information, and also provide mechanisms to resolve complaints or disputes, particularly in relation to the accuracy of data that affects policy rates.
- Before treating “aggregate” customer data as outside the scope of protected information, organizations assess the risk of re-identification using scientifically accepted methods. Only where the level of risk of re-identification is statistically insignificant should such data be treated as non-personal data.
- Consumers are informed when insurers or their third party partners intend to anonymize and aggregate data, and of the actual or potential uses for that aggregate data.

**Recommendation #3: Involve privacy experts in the design stage of Intelligent Transportation Systems, including Connected Vehicle research projects.**

This study did not focus on public sector “Connected Vehicle” or V2V initiatives, but there is clearly a need for privacy to be designed into these initiatives. While there appears to be widespread acknowledgement of the need to ensure data privacy in the design of such systems, it is not clear to what extent privacy experts are involved in current research and design initiatives. Academic research projects on ITS should involve privacy/legal experts as well as engineers. Stakeholder
groups developing standards for ITS should likewise include people with expertise in data protection.

Recommendation #4: Adopt Privacy by Design Principles and Related Tools.

It will take time to develop data protection standards for the Connected Car industry and to incorporate them into industry regulations. In the meantime, automakers and other industry players should adopt “Privacy by Design” principles and tools such as Privacy Impact Assessments to bring themselves into compliance with Canadian data protection law and to prepare themselves for industry-specific regulation. According to privacy expert Ann Cavoukian:

“[Privacy by Design] prescribes that privacy be built directly into the design and operation, not only of technology, but also how a system is operationalized (e.g., work processes, management structures, physical spaces and networked infrastructure)”

Achieving privacy compliance involves implementing a combination of measures across multiple layers of the organization and organizational boundaries to include sub-contractors, service providers and business partners. It also requires strong leadership, a sustained commitment to improving business practices and the will to innovate. Systems can be improved upon by thinking about the privacy ramifications early on.4

It has been said that:

“No single designer can achieve privacy within an organization, and no single organization can achieve privacy within an industry. Concurrent with traditional, internal considerations such as the Privacy Impact Assessment, privacy/security Gap Analysis, and the Threat Risk Assessment, each of which is becoming common practice within numerous industries, privacy must be considered in a holistic, ecosystem-wide manner if it is to be both effective and lasting.”

The following recommendations begin with a list of specific actions that individual organizations should take internally, followed by collaborative actions to develop tools that could be used by all parties to the benefit of the industry and consumers.6

Recommendation #4A – Establish a Privacy Management Program

The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia have worked together to develop a document on what it means to be an accountable organization. It is intended for organizations subject to Canada’s private-sector privacy legislation and outlines what regulators expect to see in a privacy management program.

The document, entitled “Getting Accountability Right With A Privacy Management Program”,7 outlines the best approaches for developing a sound privacy management program for organizations of all sizes, in order to meet obligations under applicable privacy legislation. The document outlines “building blocks” or baseline fundamentals for every organization. It also discusses how to maintain and improve a privacy management program on an on-going basis.

Part A – Building Blocks

Buy-in from the top: Senior management support for privacy compliance is key to a successful business decision-making process. Senior management should endorse the Privacy by Design principles as the doctrine to be applied throughout the organization end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure.

Create a Privacy Officer position: The role should exist and be integrated with decision-making processes. The role and responsibilities for monitoring compliance should be clearly identified and communicated throughout the organization. The Privacy Officer

---

6 The recommendations in this section are not meant to be exhaustive or limit the responsibility of organizations to respond to regulatory requirements. They are meant to highlight key considerations in the protection of personal information in connected cars.
should be responsible for the development and implementation of program controls and their ongoing assessment and revision.

**Create a Privacy Office:** An advisory group should be defined and resourced appropriately to monitor compliance and foster a culture of privacy within the organization. The Privacy Office ensures privacy protection is built into every major function involving the use of personal information.

**Reporting:** Reporting mechanisms need to be established, and they need to be reflected in the organization’s program controls.

**Personal Information Inventory:** The organization must be able to identify the personal information in its custody or control; its authority for the collection, use and disclosure of the personal information, and the sensitivity of the personal information.

**Policies:** Organizations must develop and implement internal policies that address specific privacy obligations under the law and incorporate privacy compliance requirements in other policies as appropriate. Policies should also reference industry standards as the basis for security controls and control objectives, such as ISO 17799:2005, ISO/IEC 27001:2013, ISO/IEC 27002:2013, CAN-CSA Q850-97. These policies need to be available to employees, who must periodically sign off on them.

**Program controls:** Additional program controls help ensure that what is mandated in the governance structure is implemented in the organization. These measures include risk assessment tools like Privacy Impact Assessments (PIA), Threat Risk Assessments (TRAs), Vulnerability Assessments (VA), staff training and education, breach and incident management protocols, Service Provider management and external communication.

**Part B – Ongoing Assessment and Revision**

- Develop an oversight and review plan: The Privacy Officer should develop an oversight and review plan on an annual basis that sets out how s/he will monitor and assess the effectiveness of the organization’s program controls.

The Privacy Officer should also:

- Update personal information inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Modify training and education
- Adapt breach and incident response protocols
- Fine-tune service provider management
- Improve external communication

**Recommendation #4B – Identify and Avoid Unintended Uses**

When designing a technical system, the potential for unintended uses of personal information should form part of a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA). This is fundamental to minimizing the privacy impact of Connected Cars where the potential for re-identifying individuals using data that has been de-identified, aggregated, anonymized is very high.

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy should still remain intact. Privacy should therefore be the default setting. One of the ways this can be achieved is by ensuring cars are delivered to customers with potentially privacy-invasive features (e.g., geolocation information accessible by applications) turned off.

Precise location information should not normally be generated as a standard feature of the service, but only “on demand” where it is needed to provide a certain service that requires knowledge of the location of the user’s device.8

Of all the information generated on the Connected Car, personal information deserves special attention for protection and prevention of unintended uses. This includes location information, identification information, account identifiers and biometric/health data that is strongly associated with individuals.

The context of a situation where personal information is present plays an important role in the amount of information that should be shared. The context also determines the sensitivity of the information. A critical

---

step in the design of information systems involving personal information is to identify what kind(s) of data is needed to meet a defined objective and apply controls over the data depending on the potential privacy harms.

For example, there are different information requirements in each of the following scenarios:

- Buyer buys a new car;
- Car owner drives to work / goes shopping;
- Car owner takes along a passenger;
- Car owner loans the car to a temporary driver;
- Driver takes the vehicle in for servicing;
- Driver rents a vehicle;
- Car owner sells the vehicle;
- Driver wants to turn off any and all tracking / monitoring;
- Car owner licenses the vehicle to a driver for business purposes;
- Car is in an accident.

For each scenario, different entities should have access to personal information, or not, as the case may be.

**Recommendation #4C - Be Open and Transparent**

All parties that collect, use and disclose personal information should use a broad range of methods to provide customers with information about the data they collect and transmit to other parties and how it will be used. The methods should include more than simply publishing policies on the company’s website. Front-line staff need to be educated and trained to respond to questions from customers about privacy practices. All staff should know how to contact the privacy office for guidance on their privacy responsibilities and to forward customer’s questions.

Automakers must refrain from using invisible or covert tracking / monitoring devices. At a minimum, drivers must be notified in an intelligible way that tracking / monitoring is about to start. The vehicle should display an indicator noticeable enough to the driver and passengers whenever vehicle tracking is in progress and cameras and microphones are on. For instance, an icon, light or other “at-a-glance” feedback mechanism could be displayed when the tracking or monitoring device is active, or when the data it is generating is accessible to installed applications. A simple means of switching between open (e.g., location-enabled) and private (e.g., location-blocked) modes might also be provided, such as a button or switch.9

**Recommendation #4D – Respect for User Privacy: Keep it User-Centric**

The principle of user-centricity requires that architects and operators keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. In the context of Privacy by Design generally, and this principle in particular, the notion of user-centricity is expanded to include the extent to which the system interface allows for informational choice in how personal information is used, as well as for communicating expectations and providing means to shape and clarify expectations.10

Operational aspects of this principle include measures to obtain informed user consent, provide rights of access and correction, and make effective redress mechanisms available. We are not suggesting that fulfillment of such measures needs to happen completely through vehicle-based mechanisms. Distracted driving obviously needs to be considered in the design of such measures. However, organizational policies and processes need to demonstrate a high degree of consideration for users at all touch points and interactions. Doing so results in a shift in the control over personal information in the custody of the organization from “organization-centric” to fully user-centric -- from “customer relationship management” (CRM) to “customer managed relationships” (CMR).

This PbD principle has important links to the fields of human-computer user interface design and systems architecture (OS / Platform design). From the perspective of user interface design, the privacy challenge is to make consumers aware of privacy controls without getting in the way of their experience. A privacy wizard displayed at the first startup of the car or an application could inform the user about the tracking capabilities, and allow them to set any initial blocking conditions. The usefulness of the privacy wizard could be extended by making it a persistent privacy tool available to the user throughout the lifespan of the car. It is also important that both end-of-life and loss-of-use (should the car be lost or

---


10 Ann Cavoukian, Ph.D. *Privacy by Design and the Emerging Personal Data Ecosystem*, (October 2012). Online: https://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf
stolen) protections be built in to allow car owners the option of securely deleting any personal or sensitive information on the car.

The Operating System and Platform of a mobile device are key enablers of privacy and security protections due to their central position in virtually all device interactions. We would therefore strongly recommend that industry players collaborate on research and development into Open Source, user-centric platforms and software components for automotive telematics systems. Doing so would enable web applications and services to be used and shared consistently and securely over a broad spectrum of converged and connected devices. The Webinos platform is one example of such an approach.\footnote{\url{http://webinos.org/about-webinos/}}

**Recommendation #4E – Work with device manufacturers, OS / Platform Developers, Network Providers, Application Developers, Data Processors to integrate controls and data minimization techniques.**

This recommendation reinforces the notion that all parties have a role to play, both on their own and in partnership with others. Privacy by Design is a collaborative effort. There are many privacy and security-related products, services, templates, best practices, and lessons learned that are needed by all parties and should be accessible on an open, equal basis, not through proprietary processes. These tools should be developed with input from Data Protection / Information and Privacy Commissioners.

For example, new user-centric privacy mechanisms, data protection standards, data minimization techniques, privacy principles and architecture requirements should be developed for the industry and be accessible to all parties. Boilerplate language for contracts, agreements and training materials could be made available. Risk assessment methodologies and templates should be developed for the automotive industry. Roles and responsibilities for Privacy Officer positions could be developed. Parties could collaborate on a harmonized Data Sensitivity Classification framework for the industry.

In summary, it is critical that protections not only be built directly into technologies but also into the culture of companies and the industry as a whole so privacy is recognized as a core functionality and not just a problem to be overcome.
**GLOSSARY**

**ADAS:** Advanced Driver Assistance Systems

**Aftermarket:** the automotive parts, service and repair industry that serves vehicles after they have been assembled. Aftermarket products can be added to a vehicle at the dealership before purchase or by authorized installers after purchase. Aftermarket devices may be integrated with vehicle systems via the OBD port. Alternatively, they may operate entirely independently of vehicle systems, through for example mobile cell phones.

**ALPR:** Automated Licence Plate Readers

**B2C:** Business to Consumer

**Bus:** the communications network that interconnects electronic components within a vehicle

**CAN bus:** Controller Area Network bus – a commonly used vehicle bus standard that allows ECUs to communicate with each other without a host computer

**Customer data:** information that is or can be linked to the customer

**ECU:** Electronic Control Unit - a small computer that operates a specific function or set of functions within a vehicle

**EDRs:** Event Data Recorders – an electronic device that records certain data about a vehicle’s operational performance in the seconds prior to and during a crash. Almost all vehicles sold in North America are now equipped with EDRs.

**Data processing:** collection, retention, use and/or disclosure of data

**Fobs:** small handheld electronic devices used for such purposes as remote locking/unlocking of vehicles

**GNSS:** Global Navigation Satellite System – global system for pinpointing the geographic location of a receiver, anywhere in the world; includes GPS (USA), GLONASS (Russia), Galileo (Europe)

**GPS:** Global Positioning System – US-based satellite system for pinpointing the geographic location of a GPS receiver.

**Head unit:** hardware interface for vehicle’s sound and entertainment system, typically located in the centre of the dashboard

**Infotainment:** combination of information and entertainment

**ITS:** Intelligent Transportation Systems

**M2M:** Machine-to-Machine. M2M communications can be defined as the flow of data between network connected devices, without the need for human interaction

**OBD:** On-Board Diagnostic

**OEM:** Original Equipment Manufacturer

**Processing:** see above, under “Data processing”

**RFIDs:** Radio Frequency Identification tags

**Telematics:** the application of both telecommunications and informatics in to deliver value-added services in the automotive context

**TCU:** Telematics Control Unit

**UBI:** Usage-Based Insurance

**V2V, V2I, V2P, V2X:** Vehicle-to-Vehicle; Vehicle-to-Infrastructure; Vehicle-to-Pedestrian; Vehicle-to-anything

**VANET:** Vehicular Ad-hoc Networks – an ever-changing mobile network made up of connected vehicles within app. 300 metres of each other
SELECTED REFERENCES

GENERAL INDUSTRY WEBSITES

http://analysis.tu-auto.com
https://connectedcarsworld.wordpress.com
http://www.telematics.com
http://telematicsnews.info

PUBLICATIONS


American Civil Liberties Union (“ACLU”), Location-Based Services: Time for a Privacy Check-in”, Nov. 2010.


The Economist, Smartphones on Wheels, Technology Quarterly, Q3 2014, Sept.6, 2014.


GSMA, Connected Car Forecast, Version 1.0, May 2013


Kleieman & Lyons, Vehicle Telematics: A Useful Litigation Tool For Attorneys, A Boon To Insurers And The Privacy Concerns Big Data Raises For Us All, Sept.20, 2014.


Ponemon Institute, *Exposing the Cybersecurity Cracks: Canada; Part I: Deficient, Disconnected & in the Dark*, June 2014.


U.S. Government Accountability Office (“GAO”), *In-Car Location-Based Services: Companies are taking steps to protect privacy, but some risks may not be clear to consumers*, GAO-14-81, December 2013.


**CANADIAN LEGISLATION**


Personal Information Protection and Electronic Documents Act (“PIPEDA”), S.C. 2000, c.5.

Act Respecting the Protection of Personal Information in the Private Sector R.S.Q. ch.P-39.1

Personal Information Protection Act S.A. 2003, c.P-6.5

Personal Information Protection Act S.B.C.2003, c.63