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

A study on privacy and onboard vehicle telematics technology

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.***

For the complete report, visit ***https://fipa.bc.ca/connected-car***

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.