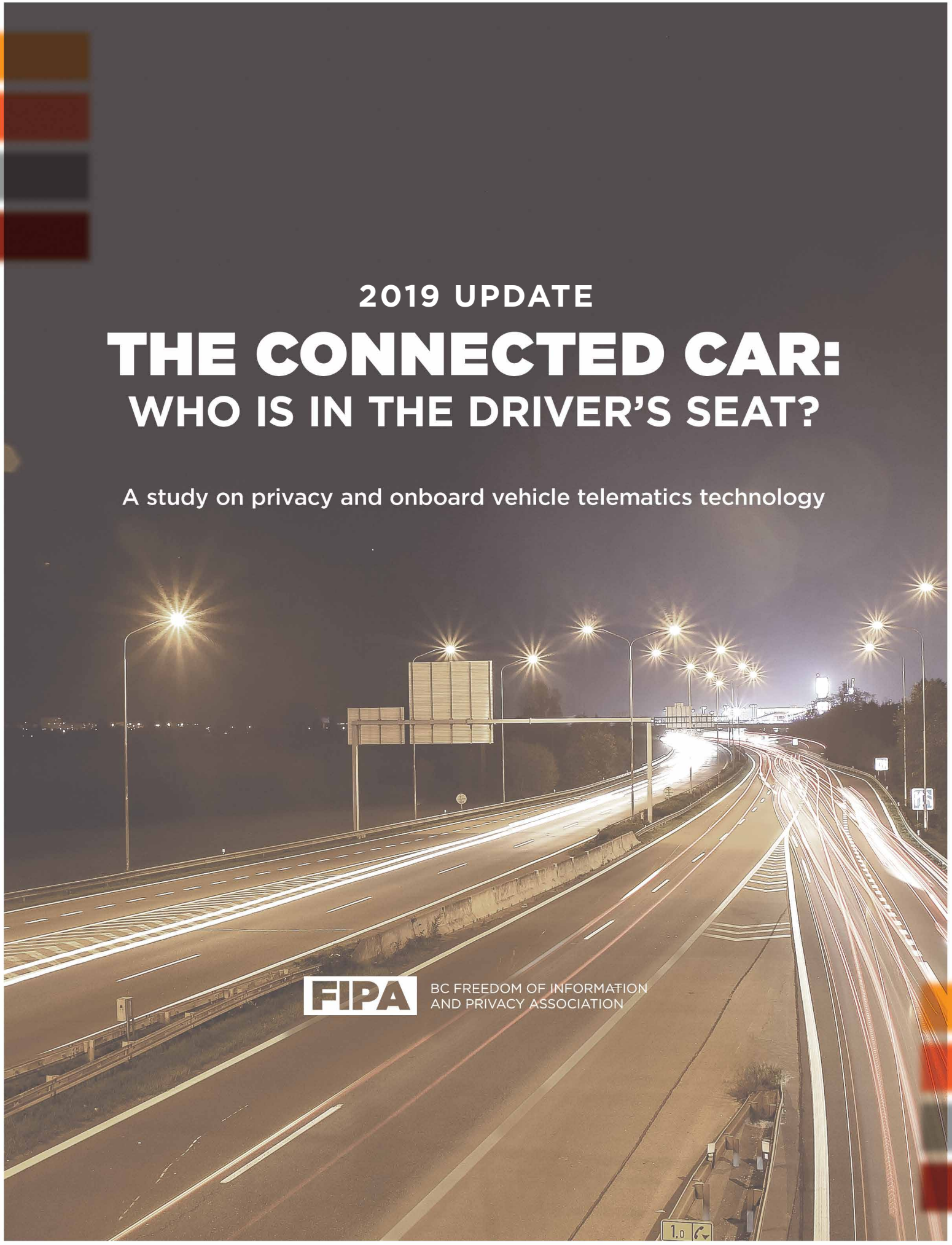
2019 UPDATE

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

A study on privacy and onboard vehicle telematics technology



FIPA
BC FREEDOM OF INFORMATION
AND PRIVACY ASSOCIATION

2019 UPDATE

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

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

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

Researched and written by Vincent Gogolek; many thanks to Rachel Chan for her research assistance on the privacy policies and a special thanks to Philippa Lawson for her review of the report and to Tamir Israel (CIPPIC) for his assistance in the early stages of the research.

FIPA BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

CONTENTS

EXECUTIVE SUMMARY

This report updates FIPA's 2015 ground-breaking report *The Connected Car: Who is in the Driver's Seat?*

As may be expected, there have been major developments both in technology and policy since our first Connected Car report.

Technology that was once exclusively available in high end vehicles has become commonplace. According to one estimate, 98 per cent of vehicles in North America and Europe will be connected by 2021. Car companies are constantly seeking new ways to profit from the collection of data taken from their vehicles, often in partnership with large technology companies like Apple and Google.

As technology advances, there have been more studies undertaken on what these changes mean for privacy rights. There have been pushes for stronger and more comprehensive legislative activity. Perhaps the most significant legislative change to date is the General Data Protection Regulation in the European Union. Other jurisdictions have also been mooting improved legislation as well as codes or standards to govern particular sectors of the economy or society, including Canada.

The privacy policies of the various car companies have also changed since 2015, generally for the better. One major improvement over what we found in 2015 was that with two exceptions, companies selling connected cars in Canada had their privacy policies available on their Canadian websites.

This allowed us to do a comparison of the privacy policies of the various companies (Original Equipment Manufacturers or OEMs) selling large numbers of cars and trucks in Canada (more than 1000 sales per annum).

We reviewed the privacy policies of 36 different vehicle brands of manufacturers from all over the world. The scope of the research focused on the policies' treatment of protected data, the openness and accountability of protected data, the accountability to third party processors, whether the policy recognizes the right of access for an individual to his or her own data, the accuracy and security of the data, the purpose specification and notice of changes, the limitations of the use, collection and retention of data, and the types of consent mechanisms that are being used by the manufacturers. In addition, we considered if there are any options for the individual to opt-out. We compared our findings to our 2015 findings in our original Connected Car report to see what had changed.

We found that OEMs' terms of service and privacy policies respecting connected car services showed significant improvement over 2015. Still these policies are still inadequate when compared to all major data protection principles and requirements under Canadian data protection law.

Although some manufacturers have made an effort to be specific about their uses of personal data and to explain their policies more clearly, key elements of OEM policies are still often unclear or expressed in very broad language. The worst examples are the very broad purposes OEMs continue to provide for collecting, using and sharing personal information, sometimes alongside specifics and sometimes not. While there is now a wider disparity among OEMs in terms of the adequacy of their connected car privacy policies, certain gaps and problems remain across the board.

In light of these shortcomings, and the federal Privacy Commissioner's repeated statements that he has not received a complaint about this issue, we have decided to remedy this situation. A complaint to Commissioner Therrien is attached to this report, and we hope it will give him the opportunity to bring clarity in an authoritative ruling on this issue.

INTRODUCTION

In 2015, the BC Freedom of Information and Privacy Association (FIPA) released a report, with funding from the Office of the Privacy Commissioner of Canada, entitled *The Connected Car: Who is in the Driver's Seat?* The report has been cited on numerous occasions and, most notably, was cited in both applicant and respondent's arguments in the 2016 Supreme Court of Canada leave application *Wayne Rodney Fedon v R* (14 July2016), 36970 (SCC).[1] In addition, Canada's Privacy Commissioner, Daniel Therrien, has stated that the report has "helpfully informed" his thinking on the privacy issues surrounding connected cars.[2]

The report's recommendations were:

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.*

In the three years following the *Connected Car* report, Canadians' continue to have serious concerns about their privacy in relation to the vehicles they drive. According to the CAA National Opinion poll:

- 38% of Canadians have found a previous user's personal information stored on the in-car system of a rented or shared vehicle.[3]
- 88% of Canadians believe the consumer should be able to decide with whom their in-car data is shared.[4]
- Nearly three quarters of Canadians (73%) are unaware that they had consented to the collection and use of their data by their vehicle manufacturer when they purchased their vehicle.[5]
- 83% of Canadians believe that clear, enforced rules are needed to protect their privacy and personal information when it comes to in-car data.[6]

Given the rapid advancement of technology, and the continued concern of Canadians about their privacy related to Connected Cars, FIPA decided to update the report.

In this update to the *Connected Car* report, we will look in greater detail at the privacy

---

[1]https://cbabc.org/BarTalk/News/Tips-from-Courthouse-Libraries/Tips-from-Courthouse-Libraries-BC/August-2017
[2]https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20170328/
[3]CAA National Opinion Poll July 2018
[4]CAA National Opinion Poll December 2018
[5]CAA National Opinion Poll July 2018
[6]Ibid.

policies of the various companies selling large numbers of cars and trucks in Canada (more than 1000 sales per annum). We are able to do this because most manufacturers now post their privacy policies online. This is different from the situation as it existed in 2015. Although this change provides better insight into the policies the companies have in place, it is important to note that we do not have the capacity to audit actual practice. As in 2015, this update will only examine and compare policies as opposed to actual practices.

SCOPE AND METHODOLOGY

BC FIPA reviewed the privacy policies of 36 different vehicle models from manufacturers from all over the world. The scope of the research focused on the policies treatment of protected data, the openness and accountability of protected data, the accountability to third party processors, whether the policy recognizes the right of access for an individual to his or her own data, the accuracy and security of the data, the purpose specification and notice of changes, the limitations of the use, collection and retention of data, and the types of consent mechanisms that are being used by the manufacturers. In addition, we considered if there are any options for the individual to opt-out. We compared our findings to our 2015 findings in our original *Connected Car* report to see what had changed since 2015.

BACKGROUND

Since BC FIPA's 2015 report, time and technology have continued to advance. In fact, within months of the *Connected Car* report's release, continued research and investigations from others showed the situation is actually worse than we had reported.

Less than six months after the release of the original Connected Car report in 2015, a journalist from *Wired* magazine filed a chilling report on how he was behind the wheel when two white hat hackers took control of the Jeep he was driving - from 10 miles away.

This is how journalist Andy Greenberg described the experience. It is important to note that he was fully aware in advance that the hackers would take control at some point, just not when or to what extent.

"As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission.

Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun."[7]

Fortunately, the hackers had been in communication with the manufacturer, Fiat Chrysler, concerning what they had found, and the company released a patch shortly after the article appeared. The patch had to be downloaded and installed either by the owner using a USB stick or by a Fiat Chrysler dealer.[8]

The hackers were able to gain access to these systems through the car's Uconnect's cellular connection, provided they knew the vehicle's IP address. The hackers then attacked a chip in the car's entertainment unit hardware (head unit) which then allowed them to use the vehicle's internal computer network (BUS) to take control of the car itself.

---

[7]https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[8]http://media.fcanorthamerica.com/newsrelease.do?&id=16827&mid=1

"When Miller and Valasek first found the Uconnect flaw, they thought it might only enable attacks over a direct Wi-Fi link, confining its range to a few dozen yards. When they discovered the Uconnect's cellular vulnerability earlier this summer, they still thought it might work only on vehicles on the same cell tower as their scanning phone, restricting the range of the attack to a few dozen miles. But they quickly found even that wasn't the limit. "When I saw we could do it anywhere, over the Internet, I freaked out," Valasek says. "I was frightened. It was like, holy fuck, that's a vehicle on a highway in the middle of the country. Car hacking got real, right then."[9]

The same hackers were back a year later with more remote takeovers.[10]

Interestingly, Canadian Chrysler vehicles did not have the cellular connectivity that allowed the Wired hack to happen, so no patch was needed in the FCA vehicles in this country.[11]

---

[9]Wired article, op cit.
[10]http://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
[11]http://torontosun.com/2015/07/22/jeep-hackers-couldnt-do-it-in-canada/wcm/bdb1e34c-4a93-4365-8200-0375df99dd3a

TECHNOLOGICAL AND MARKET DEVELOPMENTS SINCE 2015

Connected car technology and the applications it enables have continued to develop since the FIPA report was released. If anything, the race to bring automated vehicles to market—and to enhance connectivity in order to attract consumers—has accelerated. According to one estimate, there are 78 million cars on the road with an embedded cyber connection. By 2021, 98 percent of new cars sold in the United States and in Europe will be connected.[12] What were in 2015 new features on higher end vehicles (lane control, braking, etc.) have now become common, and car companies continue to work on new ways to profit from the data collected by their increasingly connected vehicles.

One example is GM Marketplace, which was launched in 2017 and is now installed on more than four million GM vehicles. It allows drivers to use the touch screen in the vehicle to buy coffee, doughnuts, make restaurant and hotel reservations, and prepay for gasoline.[13] The app is free to consumers (who register with Marketplace vendors directly), but GM shares data about drivers' buying patterns (not financial information) with the vendors, who pay GM either a flat rate or a monthly fee based on the number of consumer "impressions" they receive.[14]

Other companies offer, or are developing, similar apps. Audi, Mercedes Benz, BMW and Nissan offer services that connect the car to the driver's phone, allowing for in-vehicle connectivity in order to offer additional services. As an analyst at Kelley Blue Book put it: "So everyone is trending in this direction and part of it is because we will look at mobility as a service. When we're in our car space, we're going to expect that it's a continuation of our phones."[15]

Some car companies are developing options with a view towards compliance with privacy laws as well as satisfying customer desire for control over their data. For example, BMW started rolling out a service called "CarData" in Europe in 2017.[16] This service, which operates on top of BMW's "Connected Drive" system[17], appears to be an opt-in process by which BMW and MINI owners can agree to share telematics data with third parties. If they opt in, customers are provided with a summary of the data sent by their vehicle to BMW ConnectedDrive system, and a view of the latest version of their data.

While industry alliances continue to shift, there is significant cooperation as well as competition among players. For example, GM acquired Cruise Automation, a US driverless car start-up, in 2016 and partnered with Honda two years later. For its part, Ford has partnered with Argo AI, an artificial intelligence/robotics company

---

[12]http://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/?noredirect=on&utm_term=.fb7f33ae755a
[13]http://www.freep.com/story/money/cars/general-motors/2018/11/13/gm-buying-market-place/1977649002/
[14]Ibid.
[15]Ibid.
[16]http://www.press.bmwgroup.com/global/article/detail/T0271366EN/bmw-group-launches-bmw-cardata:-new-and-innovative-services-for-customers-safely-and-transparently?language=en
[17]http://www.bmw-connecteddrive.ca/app/index.html?bmw=grp:bmw_ca:Store#/portal/store

founded by former Google and Uber leaders, to develop autonomous vehicles.[18] Meanwhile, Google's[19] Waymo arguably leads the development of fully autonomous vehicles.

On the cybersecurity front, in August 2015 automakers established a global information-sharing community to address vehicle cybersecurity risks. Members of the "Automotive Information Sharing and Analysis Center" ("Auto-ISAC") include virtually all manufacturers of light-duty vehicles in North America, as well as over 30 global automakers and suppliers.[20]

Android Auto and Apple CarPlay Operating Systems

In 2016 Google introduced an updated version of its "Android Auto" software that allows automakers to operate the entire vehicle infotainment system (as opposed to just applications) as well as heating and cooling, opening and closing windows and some instruments, on Android.[21] This was a turning point for manufacturers who have traditionally used specialized operating systems (e.g., QNX) to run vehicle infotainment as well as telematics systems. Although not as advanced as Android Auto, Apple has also turned its "CarPlay" software into a competing operating system for automobile infotainment systems.

Some automakers have already replaced QNX with Android Auto and/or Apple CarPlay infotainment operating systems. It is expected that more will do so given the millions of Android and iOS application developers keen to come up with new apps for cars as long as security concerns are adequately addressed.[22] As Google and Apple continue to move into the automotive sphere, it remains to be seen whether QNX or other specialized OS providers will survive,[23] and what impact these changes will have on data privacy and security.

Driver monitoring

Volvo has recently announced that it plans to install interior cameras and sensors that will have the ability to detect an intoxicated or erratic driver. If the driver doesn't obey warning signals, the car could limit its speed, alert an assistance service or, "as a final course of action," slow down and park.[24] In addition, the European Commission has just announced it will require the mandatory installation of a number of interactive safety measures by 2022, including intelligent speed assistance (ISA), advanced emergency braking and lane-keeping technology.[25]

Government surveillance

In China, the government requires that manufacturers of electric cars, as a prerequisite to receiving government subsidies, provide it with the data the

---

[18]http://medium.com/swlh/the-race-to-fully-autonomous-cars-8212ff73aad
[19]Google was restructured in late 2015, such that Alphabet is now the parent company of Google, Waymo and other subsidiaries. We continue to use the more recognizable name "Google" although "Alphabet" is now more accurate.
[20]http://www.automotiveisac.com; See also Mark Nantais testimony June 7 2017 Senate Transport and communications cttee. https://sencanada.ca/en/Content/SEN/Committee/421/trcm/19ev-53410-e
[21]http://www.theverge.com/2017/5/17/15650938/android-car-google-io-
[22]http://seekingalpha.com/article/4074431-can-blackberrys-qnx-compete-googles-android-automotive-infotainment-space
[23]http://https://www.forbes.com/sites/lianeyvkoff/2015/11/02/king-of-infotainment-qnx-isnt-afraid-of-google-but-it-should-be/#78ab077043cf
[24]*Volvo's next cars will come with cameras to detect if its drivers are drunk Niclas Rolander, Bloomberg March 20, 2019* https://driving.ca/volvo/auto-news/news/volvos-next-cars-will-come-with-cameras-to-detect-if-its-drivers-are-drunk-and-stop-them-driving
[25]Road safety: UK set to adopt vehicle speed limiters BBC News March 27, 2019 https://www.bbc.com/news/business-47715415

cars collect.[26] Chinese officials claim that the data is used to improve public safety, facilitate industrial development and infrastructure planning, and to prevent fraud in the government subsidy programs. The automakers say they are merely complying with local legal requirements.

With the arrival of new Smart Cities programs and other types of infrastructure which will connect to autonomous and connected vehicles (such as Sidewalk Labs Toronto pilot project), there will undoubtedly be more of this type of data sharing in future, further challenging efforts to protect individual privacy and data security.

Data intermediaries

Otonomo, a data analytics company created in 2015, describes itself as "the first connected car data marketplace". Automakers give Otonomo access to their raw driver data.[27] Otonomo takes that data, analyzes it, "cleans it up," and then sells it to third parties, helping automakers commercialize their data. Although the 2014 automakers' pledge commits signatories not to sell data to an outside company without customers' consent, this voluntary self-regulatory standard doesn't stop them from using that data for their own benefit.[28]

Otomoto has formed an alliance with a company called Brightbox, which collects "terabytes of data" from connected cars and provides it to Otomoto. When asked what privacy protections are in place, Brightbox stated:

> "The connected car is a very sensitive environment associated with consumer safety. OEMs, car importers and dealership groups care about their customers and work to improve cybersecurity. Customers today have high requirements for cybersecurity, and one of the strategic focuses of our company's practical activity is to counter cyber-threats. Bright Box has taken steps to ensure security and data privacy. Our Data Privacy Policy covers all geographical areas where the connected vehicle solution Remoto is available, and it guarantees that all the new personal data protection elements of the [European Union's General Data Protection Regulation — GDPR] are adhered to and fully assured."[29]

---

[26]http://www.ctvnews.ca/autos/if-your-tesla-knows-where-you-are-china-may-too-1.4197133
[27]http://washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/?noredirect=on&utm_term=.0cb08fbc904a
[28]Ibid. It is also important to note that the pledge is a US voluntary initiative rather than a legal obligation, known as the 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
[29]http://news.itu.int/bright-box-otonomo-data-connected-cars/

SUBSEQUENT STUDIES ON PRIVACY AND CONNECTED CARS

The work that began in FIPA's *Connected Car* report has been picked up by a number of respected organizations in other countries, whose research has uncovered similar problems, and who have voiced similar concerns.

US Government Accountability Office report - 2017

In July 2017, the US Government Accountability Office (GAO) released a report to the subcommittee on Research and Technology of the Committee on Science, Space and Technology of the House of Representatives.[30]

The report's framework was based on the FIPA *Connected Car* report[31] and as Commissioner Therrien told the Senate Transport committee,

> "The selected experts interviewed for this project opined, in particular, that the existing Consumer Privacy Protection Principles do not provide sufficient guidance to inform automakers' actions or protect consumers' privacy, and should thus be improved. These findings are similar to those of a study by the British Columbia Freedom of Information and Privacy Association."[32]

To determine the types of data collected from connected vehicles and how, if at all, these data are used, the GAO interviewed representatives from 16 automakers and three other industry stakeholders. It also examined the online privacy policies of these organizations. Here are the conclusions of the GAO regarding the explanations of automakers in comparison to six leading privacy practices:

Transparency: The GAO managed to find all 13 original equipment manufacturers (OEMs) privacy policies, but concluded that they were not clearly written. Only two of them included a list of all the actual purposes for which the auto maker collects the data, and only one included a list of all the types of personal data collected.[33]

Focused Data Use: Although all automakers told the GAO that they "do not typically share collected data with unaffiliated third parties", none of the privacy notices said the data would not be used for reasons other than those listed in the policy, and only one set out the data retention timeframe.[34] Furthermore, fewer than half the policies stated that data would not be shared with third parties like data brokers, or that location and driving behaviour data would not be shared without first obtaining consent from the consumer.

Data Security: The majority of automakers reported conducting privacy risk assessments, and most or all participate or conduct security testing of various kinds. Almost all of the policies explained safeguards used to protect data.

---

[30] *Vehicle Data Privacy Industry and Federal Efforts under Way, but NHTSA Needs to Define Its Role* US Govt Accountability Office 2017 https://www.gao.gov/assets/690/686284.pdf
[31] Footnote 18 "We used data categories similar to those used in P. Lawson, B. McPhail, and E. Lawson, The Connected Car: Who is in the Driver's Seat? A Study on Privacy and Onboard Vehicle Telematics Technology (Vancouver, British Columbia: British Columbia Freedom of Information and Privacy Association, 2015), accessed April 19, 2016, https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf."
[32] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_sub_171122/
[33] GAO report, PP17-18
[34] Ibid., p.19

Data Access and Accuracy: Although most automakers reported offering customers various ways to access their personal account information, most policies were unclear about methods used to ensure the accuracy of that data.[35]

Individual Control: The GAO found that although automakers reported obtaining explicit consent before collecting personal information, they offered consumers a binary choice between consenting and receiving the services, or refusing consent and being denied the services. Only three automakers told the GAO that they offered consumers the option of opting out of sharing some types of data without losing access to all connected car services.[36]

Accountability: Most automakers were found to have measures in place to require third-parties to follow the automaker's privacy policy, or to have data handling requirements in their contracts with those third parties. A majority of policies outlined requirements the third parties must meet before receiving data from the automaker.

The GAO also consulted with outside experts about these policies. Those experts determined that the policies alone would not guarantee protection of privacy, primarily because of the issue of lack of informed consent due to incomprehensibility of the policies, or excessive paperwork or other reasons.[37] Furthermore, 13 of the 16 experts consulted by the GAO were concerned that automakers' policies, and the joint Consumer Privacy Protection Principles agreed to by the automakers in 2014 did not "provide sufficient guidance to inform automakers' actions or protect consumers' privacy."[38]

Privacy International - 2017

In 2017, UK-based NGO Privacy International conducted a study into the privacy aspects of connected rental cars and car sharing services.[39]

Their report *Connected Cars: What happens to our data in Rental Cars?* examined the data practices of these companies and what they found was very disturbing.

"We asked a number of rental companies, car-share schemes, and manufacturers about the data collected and stored on the infotainment systems when cars are returned. As we detail below, the unanimous responses were, not only is it the individual's responsibility to delete their data when they return the rental car, the individual is further responsible for informing other passengers who connect their devices to the car that their data is being stored on the car, and not necessarily deleted. We are concerned at the abrogation by both manufacturers and rental companies of responsibility as to whom is the data controller."[40]

Privacy International made the following recommendations:

1. Rental companies and car-share schemes must provide clear and explicit information to customers in relation to what data is retained on the infotainment systems and how to delete it.

---

[35]Ibid. p.20
[36]Ibid. p.21
[37]Ibid., p.22
[38]Two of the experts were unsure if these were adequate. Only One expert said the principles provided sufficient guidance. GAO report, p.26
[39]Connected Cars: What Happens To Our Data On Rental Cars? Privacy International, 2017 p.4 https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf
[40]Ibid., p6

2. Manufacturers must provide the equivalent of a delete button enabling customers to quickly and easily remove their personal data from infotainment systems.

Finally, we have referred our research to the UK Information Commissioners Office (ICO). We believe there needs to be clarity about data controller and data controller roles in relation to rental vehicles.

The concerns raised by Privacy International were also reflected in testimony before the Canadian Senate Transportation and Communications Committee.

A senior executive with Enterprise, Alamo and National rental car agencies responded to a question about how people renting vehicles can remove their data as follows:

> "What we are faced with today is a range of steps and processes from every different manufacturer, and it's not even just between manufacturers but between models, trim levels and which entertainment systems are in the car. They all produce a different method for how to "factory reset" a vehicle to default condition. When we look at this, there are literally thousands of different methods to get that data cleared."

> "What we are doing as an industry is to start to have those discussions with the manufacturers. We've made maybe light of it in asking for an easy button. Obviously, we don't anticipate the car would have a button, but some standardized method within a couple of steps that would return vehicles to a default situation. Yes, we are engaged in it, and I think maybe making some progress there, but we need the manufacturers to make it possible."[41]

There are also problems with used cars and the data they collect on their past, present and future owners. As connected cars move from dealers' showrooms to used car lots and private want ads, the issue of what happens with all the data they have collected becomes a real concern. In some cases, previous owners have continued to be registered as the person having control over the data, resulting in confusion and possible privacy breaches.[42]

A senior executive with General Motors Canada described his company's policy in testimony to the Senate Transport committee in this way:

> "If the [used] car was sold through one of our dealerships, it would be cleaned. If the car was sold from individual to individual, then that individual making the sale of the vehicle has the responsibility. That's set out in our guidelines and terms and conditions that you would have a responsibility to do that. Certain cars do have that capability to be able to store that data, but if you are doing a personal sale and pushing it on, then there is nobody that's doing that for you per se."[43]

International Data and Privacy Commissioners - 2017

In 2017, the 39th International Conference of Data Protection and Privacy Commissioners passed a Resolution on Data Protection in Automated and Connected Vehicles.[44]

---

[41]Tomi Gerber, Assistant Vice President, Government and Public Affairs, Enterprise Holdings, Senate Transport Cttee Oct 4, 2017 https://sencanada.ca/en/Content/SEN/Committee/421/trcm/23ev-53527-e

[42]https://www.theregister.co.uk/2018/08/21/connected_car_data_handover_mess/

[43]David Paterson GM Canada VP

[44]39th International Conference of Data Protection and Privacy Commissioners Hong Kong, 25-29 September 2017 Resolution on Data Protection in Automated and Connected Vehicles https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf

The resolution called upon all relevant parties to "fully respect the users´ rights to the protection of their personal data and privacy and to sufficiently take this into account at every stage of the creation and development of new devices or services," and outlined a number of concerns with how data was being collected, used and disclosed by connected vehicles. It also urged parties to undertake 16 actions and activities to further this end.[45]

Senate Transport Committee study and Federal Government response - 2018

At the request of the federal Minister of Transport, the Standing Senate Committee on Transport and Communications undertook a study in 2016-17 on the regulatory and technical issues related to the deployment of automated (i.e. driverless) and connected vehicles.

The report, *Driving Change: Technology and the Future of the Automated Vehicle*, was released in January 2018. It examined a number of economic, labour and other issues as well as privacy and security aspects of connected and autonomous vehicles.[46]

The Committee heard from 78 witnesses, including the lead researcher, Philippa Lawson for FIPA's *Connected Car* report, and FIPA's then-Executive Director, Vincent Gogolek.

The report made 16 recommendations in total, three of which deal directly with privacy. The federal government has responded positively to those recommendations but it remains to be seen what measures will actually be taken.[47]

Of those 16 recommendations, three are particularly relevant to privacy and security. They are outlined below.

RECOMMENDATION 8:

The Government of Canada table legislation to empower the Office of the Privacy Commissioner to proactively investigate and enforce industry compliance with the Personal Information Protection and Electronic Documents Act.

The government said it supported this recommendation "in principle", but then went on to list multiple caveats, and cited the need for extensive examination of all possible options for action.[48]

RECOMMENDATION 9:

The Government of Canada continue to assess the need for privacy regulations specific to the connected car.

In particular, the Senate Committee concluded: "The Committee believes that it is too early in the development of the AV and CV industry to determine whether voluntary guidelines will suffice or whether privacy regulations will be required to protect Canadians' privacy in the era of AVs and CVs."[49] Hence their hedging of this recommendation.

In response, the federal government again said it supported the recommendation "in principle" but noted the need for flexibility in regulation, while acknowledging that AV/CVs stand to play a central role in the lives of Canadians, and that the resulting

---

[45]It should be noted that the U.S. Federal Trade Commission abstained from this resolution.
[46]https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf
[47]https://sencanada.ca/content/sen/committee/421/TRCM/reports/MinisterGarneau_GovResp_b.pdf
[48]ibid
[49]ibid

potential risks to privacy are significant, and "... increase significantly where a lack of clarity or understanding exists among industry and consumers about the rules for how personal information can be collected and used by AV/CVs."

In addition, the government's response stated there was "broad acknowledgement that the flow of information in an AV/CV ecosystem is both complex and opaque to owners and operators of such vehicles, but the government's preferred option was "development of an industry-specific code of best practices for privacy protection" rather than regulations.[50]

RECOMMENDATION 10:

Transport Canada bring together relevant stakeholders – governments, automakers, and consumers – to develop a connected car framework, with privacy protection as one of its key drivers.

The federal government responded with support for this recommendation, and in late 2018 quietly established an advisory group to advise it on the various issues raised by autonomous and connected vehicles. The "Car of the Future Advisory Group" includes expert sub-groups addressing five themes including data privacy and security. The other four themes are safety, innovation and competitiveness, digital and physical infrastructure, and social and environmental factors. The Advisory Group is expected to report to the government by the end of 2019.

[50] Ibid.

POLICY DEVELOPMENTS IN CANADA

In addition to the study conducted by the Senate Committee on Transport, and the "Car of the Future" Advisory Group that was recently established by the federal government, Canada's federal and provincial governments have been working together on a policy framework for connected and automated vehicles. Privacy and data security is just one of several challenges being addressed.

The federal/provincial Council of Ministers responsible for Transportation and Highway Safety ("CoMT") created a working group on connected and automated vehicles through its Policy and Planning Support Committee. Participating jurisdictions include Canada, New Brunswick, Ontario, Quebec, Alberta, and British Columbia. That working group issued a report in January 2018 entitled *The Future of Automated Vehicles in Canada*.[51] Endorsed by the Council of Ministers, the report identifies and discusses ten key issues, of which data privacy is one. On the issue of privacy, the report questions existing legal standards in the context of road travel and suggests that they will change in the future:

> "**Significant privacy and security issues need to be addressed.**
>
> Once AVs are fully deployed, vehicles will be broadcasting real-time travel data, raising a number of privacy and security concerns. Institutional, legal, privacy, and cybersecurity issues will need to be considered.
>
> For security, drivers and vehicle systems will need the assurance that incoming and outgoing data is dependable and secure. Although AV developers are, in general, very motivated to prevent hacking, in the rush to keep up in the race to bring AVs to market, some developers may try to deploy AVs which are not adequately secure. Ensuring and enforcing minimum security standards is a key job for regulators.
>
> Even with security in place, there are significant privacy issues at play. It is presently not yet clear what the ownership rights of travel data, or privacy rights of users, will be. Even "anonymous" data can be used to gain information about private individuals. The question that regulators need to answer is: Is anonymous travel a right? And to what degree?
>
> Regulators should be seriously thinking about privacy and security issues now. As a starting point, transportation regulators can engage with other regulatory bodies, such as those in health care, to learn best practices around privacy and address any clear gaps. In the medium-term, regulators should begin assessing shifts in the legal landscape regarding privacy rights in road travel."[52]

In the year after its 2018 report, the same working group issued a follow-up report entitled "Automated and Connected Vehicles Policy Framework for Canada".[53] Calling for a "strategic and aspirational vision for AV/CVs" and noting Canada's opportunity to be a world leader in this field, the report sets out six guiding principles focused on safety, security, public

[51]https://comt.ca/reports/autovehicle2018.pdf
[52]Pp.16-17.
[53]https://comt.ca/reports/avcv-policy-e.pdf

awareness, policy and regulatory alignment and continuous collaboration. The report also identifies roles and responsibilities for each of the three levels of government (federal, provincial/territorial and municipal). With respect to privacy, the report calls for an industry-specific code of best practices, stating:

> "AV/CVs stand to play a central role in the lives of Canadians, and the resulting potential risks to privacy are significant. These risks increase where there is a lack of clarity or understanding among industry and consumers about the rules for collecting and using personal information. Canada's existing privacy laws clearly apply, but we still face a lack of clarity as to how the Personal Information Protection and Electronic Documents Act (PIPEDA) principles translated to best practices in the automotive industry. Given the broad acknowledgement that the flow of information in an AV/CV ecosystem is both complex and opaque to owners, passengers, and operators of such vehicles, it is clear that initiatives to increase understanding of risks and obligations must be a multi-stakeholder effort. Governments will need to work with our partners to develop an industry-specific code of best practices for privacy protection."[54]

In brief, policy development in Canada with respect to AV/CVs seems to be focused on safety, intelligent transportation systems and making Canada a world leader in AV/CV technology. It is encouraging that the federal government has made privacy and data security one of five issue areas for its advisory group to address, but privacy concerns do not appear to be receiving the same level of attention by other governmental or industry groups working intensively in this area.

[54] P.14.

RELEVANT REGULATORY DEVELOPMENTS

Since the FIPA report and its analysis of privacy law compliance by automobile manufacturers, there have been some significant developments in respect of privacy law and regulation, putting further pressure on the industry (in Canada and the EU at least) to take steps to address the privacy issues arising from their new products and services.

EU GENERAL DATA PROTECTION REGULATION (GDPR)

There has been a major revision of privacy law in the European Union with the new General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. Some of the more notable changes include:[55]

Increased Territorial Scope (extraterritorial applicability)

- Penalties have been increased and organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.
- Conditions for consent have been strengthened.
- Breach notifications are now mandatory.
- Data subjects can now obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose.
- The GDPR introduces data portability – the right for a data subject to receive the personal data concerning them which they have previously provided in a 'commonly used and machine readable format' - and to transmit that data to another controller.
- GDPR has incorporated Privacy by Design principles more clearly than did the previous EU Directive.

The GDPR does not have a direct effect on Canadian consumers, but does set a standard for the industry. Indeed, guidelines for meaningful consent recently issued by the OPC are interestingly similar to those adopted by the EU.[56]

French Data Protection Authority compliance package

In October 2017 the French data protection authority (CNIL) put out an official guide for connected vehicles and personal data.[57] This document was created after extensive consultations with stakeholders, including the two major French automakers, and provides a roadmap for understanding how the requirements of both the French data protection law and the GDPR should be interpreted in the domain of the connected vehicle.

As the CNIL document puts it, the guidelines "constitute the CNIL's interpretation of the French Data Protection Act, as applied to connected vehicles. They reflect the analytical frameworks used by the CNIL to assess possible breaches of the law, and they constitute an element of legal security for data controllers."[58]

---

[55]https://eugdpr.org/the-regulation/
[56]https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
[57]https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf
[58]Ibid., p.2

In addition to setting out the requirements of French law and the GDPR, the compliance package provides recommendations for measures to meet the legal requirements.

For example, in terms of informing consumers of their information rights CNIL recommends:

> concise and easily-understandable clauses in the contract of sale of the vehicle and / or in the contract for the provision of services; and
>
> by using distinct documents (e.g. the vehicle's maintenance record book or manual) or the onboard computer; and using standardised icons in vehicles.

Automaker responses to the GDPR

The umbrella group for the European auto manufacturers has responded to the GDPR, taking the position that in order to make vehicles cyber secure, individuals should not have a right to access their personal data. Others have taken issue with this position, pointing to the need for data portability in a competitive industry and how limiting individual access rights would undermine competition. Among those opposed to the car companies are the rental car companies, who have stated that "vehicle ownership should convey the right of access to the data that is generated by the vehicles that are owned."[59]

USA - FEDERAL TRADE COMMISSION AND NATIONAL HIGHWAY TRAFFIC SAFETY AUTHORITY

There have been policy developments in the United States as well, but mostly in the form of guidance or discussion papers rather than concrete legislative action. This is not encouraging given the integration of the Canadian and American auto sectors.

In the US, the Federal Trade Commission (FTC) has primary responsibility for consumer protection including privacy rights, and has issued some statements dealing with the issue of connected and autonomous vehicles[60] including that "... consumers should be provided with clear, easily understandable information about if and how their information is being collected, stored, or transmitted and how they can access or delete that information" if that information is not related to the safety of the vehicle.[61] The FTC's work in this area includes a catalogue of the concerns people have with their data being collected by their vehicles. The FTC did not, however, sign on to the Data Protection Commissioners' resolution on connected cars.

The US Department of Transportation released a report in October 2018 entitled *Preparing for the Future of Transportation - Automated Vehicles 3.0*. This paper is primarily centred on self-driving cars, and is mostly related to safety, interoperability

---

[59]Tomi Gerber, Assistant Vice President, Government and Public Affairs, Enterprise Holdings, Senate Transport Cttee Oct 4, 2017 https://sencanada.ca/en/Content/SEN/Committee/421/trcm/23ev-53527-e

[60]https://www.ftc.gov/reports/connected-cars-workshop-federal-trade-commission-staff-perspective

[61]http://www.ftc.gov/news-events/blogs/business-blog/2018/01/ftc-staff-offers-perspectives-connected-car-workshop

and cybersecurity. Its main statement is about the importance of privacy along with the need to protect "proprietary and confidential business information":[62]

> "While advanced safety technologies have the potential to provide enormous safety, convenience, and other important benefits to consumers, stakeholders frequently raise data privacy concerns as a potential impediment to deployment. U.S. DOT takes consumer privacy seriously, diligently considers the privacy implications of our safety regulations and voluntary guidance, and works closely with the Federal Trade Commission (FTC)—the primary Federal agency charged with protecting consumers' privacy and personal information— to support the protection of consumer information and provide resources relating to consumer privacy. The Department suggests that any exchanges of data respect consumer privacy and proprietary and confidential business information."[63]

At present, American legislators are struggling to introduce national level privacy protections laws, but to date have been unable to agree on which approach to take.[64] A major stumbling block has been debate over whether a federal law should override existing state laws, most notably that California's strong consumer protection laws.

CANADA – OFFICE OF THE PRIVACY COMMISSIONER CONSENT GUIDELINES

Highly relevant to the issue of data privacy in connected cars are new guidelines on consent under PIPEDA, released jointly by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner of BC on January 1, 2019.[65] Undoubtedly responding to widespread non-compliance with PIPEDA's consent rules—including that found in the 2015 FIPA *Connected Car* report—the *Guidelines for Obtaining Meaningful Consent* set out seven guiding principles based on the legal requirements under PIPEDA, which are as follows:

1. Make privacy information readily available in complete form, emphasizing the key elements of the data involved.

2. Allow individuals to control the level of detail they get in respect of privacy policies, and when they get it.

3. Clearly outline which collection, use or disclosure is "...integral to the provision of that product or service and provide individuals with distinct options to refuse consent (if not to provide express consent)

4. Organizations should use a variety of communications strategies to explain their privacy practices

5. Organizations should take the consumer perspective into account, and ensure their consent policies are user-friendly

6. Users should be notified and their consent obtained before an organization introduces significant changes to its privacy practices.

---

[62]*Preparing for the Future of Transportation* - Automated Vehicles 3.0 p.18 https://www.transportation.gov/av/3/preparing-future-transportation-automated-vehicles-3
[63]Ibid.
[64]https://www.theglobeandmail.com/world/article-us-lawmakers-battling-to-regulate-tech-giants-including-facebook/
[65]https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

7. Organizations should be prepared to demonstrate compliance with the above six principles.

Canada – Digital Charter and Action Plan

This series of documents was released by Minister of Innovation, Science and Economic Development Navdeep Bains in May 2019, and reflects what the government heard during consultations on the digital economy conducted in 2018, and its plan for moving forward on a wide range of issues related to the digital economy, including privacy protection.

The plan is ambitious and wide-ranging, including ten principles for action on a variety of issues, several of which will be important for development of rules in the Connected Car sphere.[66] These include modernizing PIPEDA to include:[67]

- Reforming consent, including preventing bundling of consent into contracts
- Improving data mobility
- Creating data trusts to facilitate data sharing
- Incentivize use of codes or standards
- Improve enforcement, including providing the Privacy Commissioner with order-making power

It should be noted that although these proposals contain promises of action, they are not actual amendments to legislation. It remains to be seen if these initiatives move forward after the federal election taking place in October 2019.

---

[66]Canada's Digital Charter: Trust in a Digital World https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[67]Strengthening Privacy for a Digital Age: **Proposals to modernize the *Personal Information Protection and Electronic Documents Act*** https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

PRIVACY CHECKUP 2019: ARE AUTOMAKERS PROVIDING CONNECTED CAR SERVICES COMPLIANT WITH CANADIAN PRIVACY LEGISLATION?

Our 2015 review of connected car terms of service and privacy policies showed that automakers were failing to meet their legal obligations under almost every principle of data protection law. Four years later, we revisited applicable terms of service and policies and measured them against the applicable law in Canada.[68] The following is a summary of our findings.

Scope of Protected Information:

What the law requires: Canadian data protection law protects "personal information", which is defined as *"information about an identifiable individual"* PIPEDA s.2

What we found in 2015: 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.

What we found in 2019:

Some OEMs' privacy policies now expressly set out the many types of information covered by the policy, particularly in terms of data they collect.[69] As for anonymization, most policies state that data which has been anonymized "in a way which can no longer be associated with you or your vehicle and can be used for any legitimate business purpose."[70] However, the risk of re-identification is usually not referred to.[71]

Openness and Accountability Generally:

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 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

---

[68]A complete list of privacy policies with links can be found at Appendix A of this report.
[69]Eg: GM Canada Consumer Privacy Policy https://www.gm.ca/en/privacy.html
[70]Eg:GM Onstar Privacy Policy https://www.onstar.com/ca/en/privacy_statement/
[71]Eg: Fiat Chrysler Automobiles Canada privacy policy http://www.fcacanada.ca/privacy/privacy_statement.pdf

(e) what personal information is made available to related organizations (e.g., subsidiaries). (4.8.2)

What we found in 2015:

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 were so incomplete, vague or open-ended in certain respects that they were entirely unhelpful.

What we found in 2019:

Privacy policies covering connected vehicles are now generally available online, with a few exceptions.[72] They are also usually accessible through the company's Canadian website. However, it is important to note that many companies have more than one privacy policy; one is a general policy while the other deals specifically with Connected Car services.[73] It is not always evident which policy applies or that there is more than one that applies.

Most policies also now have an effective date or commit to posting the most recent version, and some post links to previous editions of the policy.[74]

Most policies now provide more context and/or detail than in 2015, although at least one is largely a simple restatement of the law, providing little information to consumers about the company's collection, use and disclosure of their personal data.[75]

Descriptions of the information being collected vary widely: on one hand, some companies now provide a list of contextualized examples, sometimes explaining why they collect each type of information.[76] FCA offers no more than a legal definition of "personal information" and makes no effort to connect types of personal data with particular purposes.

Some of the commonly stated purposes for collecting personal data are as nebulous as they were in 2015: e.g., "developing principles and solutions for the design of our products",[77] "conduct market and product preference research and analysis",[78] and the all-encompassing "meet internal business purposes"[79] or "other legitimate business purposes".[80]

---

[72]We were unable to locate privacy policies for vehicles sold by Kia, Mitsubishi and Smart, only their website privacy policies. ." Representatives of these companies were asked about this situation at the 2019 Vancouver International Auto Show, but were unable to provide any explanation of these brands' failure to provide a link to the policy or direct us to where those policies might be found. E mails were then sent to the addresses on the three companies' websites. Smart Canada stated in its response that "smart is a wholly owned and operated division of Mercedes-Benz Canada Inc" and linked to the parent company's privacy policies. Smart also stated that "... our smart vehicles do not have any connected capabilities." Mitsubishi stated equivocally that "We regret to learn that you are unable to find the privacy policy covering your connected vehicles as you mentioned, please be advised that all the information that is supposed to be available to the public is on our website." There was no response from Kia Canada.

[73]For example, GM has a general Consumer Privacy Policy https://www.gm.ca/en/privacy.html but also a specific statement for its OnStar program https://www.onstar.com/ca/en/privacy_statement/. Several other companies follow the same approach, requiring that the consumer be aware of both policies and read together.

[74]Eg: GM OnStar

[75]FCA

[76]Eg: GM Onstar, Ford, Acura/Honda, BMW/MINI.

[77]FCA

[78]Hyundai Canada

[79]Acura

[80]Hyundai

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 we found in 2015: 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.

What we found in 2019:

Many policies now state that they require third party processors to handle data in some privacy protective way. Some say that such third party protections are contractual in nature[81], while others use the less specific phrase "according to our instructions".[82] For example, Acura states that it "requires its third party service providers with access to Covered Information to protect and to keep this information confidential and they are only permitted to use Covered Information for the sole purpose of carrying out services for Acura." It is not clear from this wording whether the requirement is contractual, or what specific obligations third parties have beyond keeping information secure and confidential, and only using it in carrying out services for Acura. GM Canada states its third parties are subject to contractual requirements that meet "industry standards".[83] In contrast, MINI's policy states that "We contractually require any third party organization to use and protect the personal information disclosed to them in a manner consistent with our Privacy Policy."[84] Some policies are unclear as to whether they take any measures to ensure that contracted third parties protect customer data.[85]

Regardless, many policies state that the OEM is not responsible for third party actions regarding personal information.[86]

Many policies note that personal information may be stored outside Canada, and therefore may be subject to foreign legal and privacy regimes.

Policies have not changed significantly with respect to responsibility for dealership handling of personal data: OEMs still disclaim responsibility for their dealers' handling of personal data. Customers are, for the most part, simply advised that dealers are separate organizations and have their own privacy policies.[87]

---

[81]Infiniti Canada
[82]FCA
[83]GM Onstar
[84]MINI Canada
[85]Eg. Tesla https://www.tesla.com/en_CA/about/legal
[86]Eg: GM Onstar, Acura.
[87]ibid

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 we found in 2015:

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.

What we found in 2019:

Policies usually acknowledge the customer's right to access their own personal information but the scope of such access is typically unclear, with statements like: "You may review and update your Personal Information at any time by contacting us"[88]; "You can contact [Company X] at any time to discuss or update your personal information that [Company X] has on file."[89] Ford specifically limits the access right to "certain of your personal information which is easily accessible to our service representatives" and specifies the type of data that is accessible to its service representatives. Most policies are silent as to whether exercising one's access right will entail a fee, although some promise to respond at no cost[90] and others reserve the right to charge for access.[91]

Most policies focus on the customer's right to correct inaccurate information, sometimes directing the customer to do so via their online account if possible and otherwise calling a toll-free number. Some companies state that they will forward corrected information to third parties who have received the inaccurate information from them in the past.[92]

Accuracy:

What the law requires: 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)

What we found in 2015:

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

---

[88]Toyota
[89]Acura; GM makes a similar broad statement.
[90]FCA
[91]"We will respond to all requests for access to information within 30 business days from the receipt of request and at minimal or no cost to the individual. In the case where there is a cost associated with processing the request, we notify the customer in advance." Mercedes-Benz https://www.mercedes-benz.ca/en/legal-notices/privacy-policy
[92]FCA, Mercedes-Benz

What we found in 2019:

Although most companies make at least a general commitment to keeping accurate information, policies differ considerably in terms of how they will do this. All policies provide for correction of inaccurate data on the customer's initiative. Some (e.g. Mazda)[93] expressly place the onus on the customer to advise them of any changes in their personal information, while others (e.g. Ford) state that they take proactive measures to maintain accuracy of their information. Mercedez-Benz states that the efforts it makes to ensure accuracy of personal data depends on the use of the data and the interests of the customer.[94] Other than saying that they make "reasonable efforts" to ensure accuracy of personal data, most policies (other than Ford) do not specify how they do so.

Security:

What the law requires: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. (4.7)

What we found in 2015:

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.

What we found in 2019:

Policies vary greatly in respect of the level of detail provided regarding data security promised to customers. Some companies provide specifics as to the measures they take to safeguard personal data[95] – for example, Ford says it encrypts data being transmitted, and Toyota states it uses a "dedicated private and secure wireless network" for its connected car services. In contrast, other companies provide no elaboration regarding the "reasonable" and/or "adequate" steps they claim to take to protect customer data.[96]

With respect to security of personal data entrusted to third party telecommunications service providers, some companies purport

---

[93]"To the extent permitted by law, Mazda assumes no responsibility for verifying the ongoing accuracy of personal information. Once advised that personal information is inaccurate, Mazda will seek to amend the information and correct it with information provided by the customer." https://www.mazda.ca/en/privacy/

[94]"At MBC, we make reasonable efforts to ensure that personal information we use or disclose is as accurate, complete, and up-to-date as is necessary for the specified purpose. This depends on the use of the information and takes into account the interests of the customer. For example, accuracy of information is particularly important if Mercedes-Benz Financial Services Canada Corporation is using this information to make a judgment or evaluation about a customer, such as for credit checks."

[95]Eg: Audi, Ford, Toyota.

[96]FCA, GM Onstar.

to use contractual measures to ensure data security that meets industry standards;[97] others expressly disclaim responsibility for security of third party networks,[98] while still others simply do not address this point.[99]

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 we found in 2015:

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.

What we found in 2019:

Generally, car companies do not proactively advise their customers about changes to the purposes for which they use personal data but most commit to having the most recent version of their privacy policy posted on their website.

Although some OEMs have retained the broad and vague language we found in 2015, others now set out specific purposes and context for collection of personal information (see above, under Openness). Unfortunately, most automakers continue to use broad and ill-defined purposes similar to those we found in 2015, including "market products and services to you", "develop new products and services, including autonomous vehicle and car-sharing products and services"[100], and "legitimate business purposes."[101]

---

[97]GM Onstar: "We also require by contract (other than in an emergency situations) that third party services providers acting on our behalf or with whom we share your information also undertake to provide such security and confidentiality measures in accordance with industry standards."
[98]Toyota, Acura: "Because certain communications and information collected from your vehicle are provided through wireless and satellite networks, we cannot promise or guarantee that the communications will not be intercepted by others. You understand and agree that your use of the Connected Vehicle Technologies and Services is at your own risk and Acura will not be liable for any damages for any loss of privacy occurring in communication over such networks."
[99]FCA
[100]GM Onstar
[101]Acura

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 we found in 2015:

Some OEMs do not limit the purposes for which they collect, use and disclose personal customer data. OEMs treat marketing and product research and development (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.

What we found in 2019:

As in 2015, the 2019 policies typically include marketing and product R&D as one of several non-optional purposes of data collection for connected services. Examples of apparently non-optional purposes that could extend beyond those "that a reasonable person would consider appropriate in the circumstances" include to "meet internal business purposes",[102] "manage and administer our business",[103] "conduct market and product preference research and analysis",[104] "develop future services and/or products",[105] "develop new vehicles and features",[106] and "other marketing purposes".[107] Perhaps the broadest and vaguest purpose we found is "legitimate business interests".[108]

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 we found in 2015:

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.

What we found in 2019:

Some policies purport to limit their collection of personal data to that which is "necessary" or "reasonably necessary" for stated purposes.[109] Other policies do not specifically state that collection of personal data is limited to that necessary

---

[102] Acura
[103] Maserati
[104] Hyundai
[105] Acura
[106] Toyota
[107] FCA
[108] Hyundai
[109] Hyundai, FCA

for the purpose in question.[110] Interestingly, the policies that provide more information about the types of data collected, and the uses to which the data is put, tend not to expressly limit themselves to necessary collection, while those that purport to comply with the general rule above provide much less, if any, detail as to the data they collect and the uses to which it is put. No policy we reviewed specified whether the purposes for which they collect personal data could be accomplished with anonymized data.

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 we found in 2015:

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.

What we found in 2019:

Although most OEMs now address retention, typically stating that they will retain personal information only for as long as necessary to fulfil the purpose, some use vague language or qualifiers that undermine this commitment – e.g. 'as permitted by law'.[111] Very few commit to any specific retention period in their policies, although some now set out criteria for how they will determine how long to hold information.[112]

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 we found in 2015:

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.

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.

What we found in 2019:

Again, the use of very broad language in OEM privacy policies has the effect of undermining protections which those policies might otherwise afford.[113]

Some companies merely make a general commitment reflecting their legal obligation to obtain consent to any sharing of personal data with third parties,[114] while others are more helpful and provide a list of third parties with whom, and purposes for which, they may share personal information.[115]

In terms of secondary marketing and other optional services that require use or disclosure of personal data, many policies now incorporate some kind of

---

[110]Ford, GM
[111]For example, Mazda states "Mazda reserves the rights to otherwise retain your personal information as may be required or permitted by law."
[112]Ford Privacy Policy sets out criteria, and also states specifically that procedures are in place to destroy or anonymize 'in a secure manner' once the period expires.
[113]Eg: "to provide superior service", "to develop future services and/or products", "to perform market research"
[114]Eg: Hyundai; FCA; Subaru.
[115]Eg: Ford, GM Onstar, Mercedes

opt-out mechanism beyond simply not receiving marketing messages. Some now offer specific opt-out provisions, by activity/service, sometimes with detailed instructions (e.g., for removing cookies).[116]

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 we found in 2015:

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.

What we found in 2019:

Privacy policies often rely upon both express and implied consent without clearly identifying which services or activities require which type of consent.

There is still considerable reliance on implied consent by virtue of mere use of a product or service. For example, "...if Acura intends to use certain types of Covered Information (specifically, geolocation information, driver biometric information or driver behavior information) for marketing purposes or to provide such information to third parties for their own independent use, we will obtain your separate, express consent, either by affirmative statement or your enablement of certain vehicle functions, before doing so."[117] (underlining added)

Interestingly, many automakers require that customers telephone them in order to opt-out of secondary uses of their personal information.[118] It is unclear why email and/or other online methods of opting-out (or opting-in) are not made available – one could presume that companies want to be able to explain and possibly convince customers of the benefits of not exercising the opt-out. Indeed, the effort to which customers must go to understand their choices and how to exercise them is significant.

The default setting of connected car services remains, for the most part (if not across the board), privacy-unfriendly. Rather than defaulting all settings to the most privacy friendly and allowing customers to opt-in to data collection, use and disclosure, companies assume that customers consent to a wide range of data

[116]Eg: Acura, Ford, GM Onstar, Volvo, Tesla.
[117]Acura
[118]Ford, GM, Hyundai

uses without asking them, even where the use in question is optional. Silence is treated as consent, and the best that consumers can expect is the ability to refuse certain services or opt-out of certain unnecessary data collection, use or disclosure.

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)

What we found in 2015:

OEMs often require that customers agree to unnecessary collection, use or disclosure of their personal data in order to register for Connected Car services.

What we found in 2019:

As noted above, the ability to opt out of collection, use or disclosure of various types of personal information varies widely from company to company. Some companies have clearly gone to some effort to identify and categorize the various purposes for which they collect, use and disclose customer data, and to give customers more choice in the matter.[119] But while there has been progress on complying with the legal requirement to "explicitly specify" purposes for which companies require customer consent as a condition of service, it remains debatable whether all such purposes are "legitimate" – or more fairly stated, whether it is "legitimate" to make all such purposes non-optional.

Since the release of FIPA's Connected Car

[119]Eg: Ford, GMOnstar, Acura.

CONCLUSION

report in 2015, car manufacturers have been reluctant to acknowledge that there are any shortcomings in terms of privacy protection. Those willing to speak publicly usually say very little beyond that they believe they are compliant with Canadian law.[120]

Our 2019 review of OEMs terms of service and privacy policies respecting connected car services show significant improvement over 2015 but still widespread inadequacy in regards to all major data protection principles and requirements under Canadian data protection law.

Although relevant privacy policies and related information are now largely available to Canadian consumers on the manufacturer's website, and although some manufacturers have made an effort to be specific about their uses of personal data and to explain their policies more clearly, key elements of OEM policies are still often unclear or expressed in very broad language. The worst examples of this are the very broad purposes OEMs continue to provide for collecting, using and sharing personal information, sometimes alongside specifics and sometimes not. While there is now a wider disparity among OEMs in terms of the adequacy of their connected car privacy policies, certain gaps and problems remain across the board.

Privacy, while acknowledged by policy makers as an issue, tends to be overshadowed by other serious issues raised by the transformative impact of this technology. Coordinated federal/provincial government efforts tend to be focused on motor vehicle safety, intelligent transportation systems and making Canada a world leader in AV/CV technologies.

The federal Privacy Commissioner has expressed concerns about the state of privacy in this field, but has yet to receive an actionable complaint related to connected cars.[121] Given what we have found in our review of the privacy policies of the various car companies, and the likelihood that they are not meeting their obligations under PIPEDA, we have written to the Commissioner to request that he investigate this apparent non-compliance with Canada's privacy law.[122] That complaint is attached to this report, and we look forward to having the Commissioner state what needs to be done in order to ensure that these organizations are meeting their legal obligations.

List of Canadian Connected Car privacy

[120]David Patterson testimony.
[121]Senate report op cit p 56
[122]See Appendix B

APPENDIX A

policies available online

Acura
https://www.acura.ca/privacy

Honda
https://www.honda.ca/privacy/vehicledata

Alfa, Fiat, Chrysler, Dodge, Jeep
http://www.fcacanada.ca/privacy/privacy_statement.pdf

Maserati
https://www.maserati.ca/maserati/ca/en/others/privacy-statement

Audi
https://www.audi.ca/ca/web/en/tools/navigation/layer/legal/privacy.html

VW
https://www.vw.ca/en/tools/navigation/footer/links/privacy-policy.html

Porsche
https://connect-store.porsche.com/ca/en/t/privacy?reducedHeaderFooter=true

BMW
https://myc-profile.bmwgroup.com/api/gateway/contentserver/staticcontent/Angular/gdpr/v2/?target=bmw-browser#/legal-docs-content?version=2018.08.14&fileName=Bmw_cd_pp_ca-en.json

MINI
https://www.mini.ca/en/about/privacypolicy

Buick, Cadillac, Chevrolet GMC
http://www.gm.ca/gm/english/corporate/about/privacy/overview https://www.onstar.com/ca/en/footer-links/privacy-policy.html

Ford, Lincoln
https://www.ford.ca/help/privacy/

Hyundai
https://www.hyundaicanada.com/en/about/privacy-policy

Genesis
https://www.genesis.com/ca/en/privacy-policy.html

https://mybluelink.ca/support/terms

KIA
https://www.kia.ca/legal# (Website privacy policy only)

Jaguar, Land Rover
https://www.jaguar.ca/en/privacy-legal.html

Mazda
https://www.mazda.ca/en/privacy/

Mercedes
https://www.mercedes-benz.ca/en/legal-notices/connected-vehicle

Smart
https://www.smart.com/ca/en/index/footer/data-protection.html (Website only, Smart says it does not offer connected cars)

Mitsubishi
https://www.mitsubishi-motors.ca/en/legal/ (Website privacy policy only)

Nissan
https://www.nissan.ca/en/privacy.html#!

Infiniti
https://www.infiniti.ca/en/privacy.html

Subaru
https://www.subaru.ca/privacy

Toyota/Lexus
https://www.toyota.ca/toyota/en/privacy#/al/entune-privacy-content

Tesla
https://www.tesla.com/en_CA/about/legal

Volvo
https://www.volvocars.com/en-ca/footer/privacy

APPENDIX B

Complaint to Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

By Email

Dear Commissioner Therrien,

Please find attached a copy of an update on our 2015 report The Connected Car: Who is in the Driver's Seat, which examines the privacy policies of vehicle makers who sell more than 1000 vehicles in Canada each year.

As you can see, many of the problems which we identified in our original report remain unresolved. For example, purposes for collection of personal information remain vague and excessively broad in many instances. There are also ambiguities with regard to the protection of personal information, sharing with third parties and the ability to opt out of data collection.

Given the amount of time that has passed since we pointed out many of these problems, and the fact that many of these problems continue, we request that your office conduct an investigation into the compliance of these companies with the Personal Information and Protection of Electronic Documents Act (PIPEDA).

If you require any clarification or additional information, please feel free to contact me or my office.

Sincerely,

Sara Neuert, Executive Director

BC Freedom of Information and Protection of Privacy Association

FIPA BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

#103-1093 West Broadway
Vancouver B.C. V6H 1E2

p: 604.739.9788
e: fipa@fipa.bc.ca
w: fipa.bc.ca
tw: @bcfipa