Canadian Journal of Law and Technology

Volume 17 | Number 2 Article 6

12-1-2019

Developing a Privacy Code of Practice for Connected and Automated Vehicles

Rajen Akula
Assistant Professor, Faculty of Business and IT, OntarioTech University

Developing a Privacy Code of Practice for Connected and Automated Vehicles

Rajen Akalu*

1. INTRODUCTION

Connected and autonomous vehicles ("CAVs") can collect, store, process and transmit vast amounts of data.[1] Understanding the use (and potential misuse) of this data, particularly when that data is about an identifiable individual within the meaning of data protection law, is regarded critical to the success of this new mode of transportation.[2] However, what constitutes personal information in relation to connected and automated vehicle data on a case-by-case basis. This presents a policy challenge for the government and creates uncertainty for businesses wishing to make use of this data.

Canadian law does not, however, have specific data protection rules that apply directly to connected vehicles.[3] It is has been argued by some commentators that sector specific legislation is what is needed to remedy this problem.[4] Crucial stakeholders, such as automakers, have asserted by contrast that any prescriptive unique to Canada's regulation with respect to privacy and CAVs would result in increased costs that would be passed on to consumers.[5] This paper explains how a privacy code of practice for CAVs developed using the

---

* PhD. Assistant Professor, Faculty of Business and IT, OntarioTech University, 2000 Simcoe Street, North Oshawa, Ontario L1H 7K4 Canada, rajen.akalu@uoit.ca. This project received funding support through the Office of the Privacy Commissioner of Canada's Contributions Program. The opinions expressed are those of the author and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada. The author acknowledges the helpful contributions of the privacy code of practice working group consisting of privacy and consumer advocates as well as academics and government officials involved in privacy regulation in the development of the code.

1 It is estimated that modern cars have the computing power of 20 personal computers, features about 100 million lines of programming code, and processes up to 25 gigabytes of data an hour. See McKinsey (2014) What's driving the connected car. Online at <www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car>.

2 Dorothy J. Glancy, "Privacy in autonomous vehicles" (2012) 52:4 Santa Clara L. Rev. 1171.

3 Jed Chong, "Automated and Connected Vehicles: Status of the Technology and Key Policy Issues for Canadian Governments" (2016) Library of Parliament Background Paper Publication No. 2016-98E, online: <www.lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/BackgroundPapers/PDF/2016-98-e.pdf>.

4 Philippa Lawson, *The Connected Car: Who is in the Driver's Seat?* (Vancouver: BC Freedom of Information and Privacy Association, 2015), online: <www.fipa.bc.ca/wordpress/wp-content/uploads/2018/01/CC_report_lite.pdf> [Lawson].

5 Rajen Akalu, "Paving the way for Intelligent Transport Systems (ITS): The Privacy

Canadian Standards Association Model Code ("CSA Model Code") might address privacy protection with respect to this emerging technology.

It will be argued that the development of a code of practice for CAVs can serve as a learning process that can address privacy concerns in a manner that is both holistic and systematic. A code of practice can also provide much needed guidance for organizations with respect to personal data as well as communicate to consumers the data they are entitled to control. As codes of practice vary widely in terms of their scope and orientation, it will be important to establish this at the outset.

Unlike privacy policies or statements, codes of practice apply to more than one organization.[6] Codes of practice in particular sectors have the potential to provide predictability and certainty for companies in terms of understanding their obligations around meaningful consent and appropriate limits on data processing. The automotive ecosystem involves a considerable number of market participants. Although automakers may be regarded as incumbents, there are numerous organizations seeking access to CAV data. These range from software developers, to municipalities as well as insurance companies and law enforcement.

The draft code of practice as developed in this paper serves as a statement of best practice for compliance with PIPEDA principles. The code should be used in combination as a quasi-legal compliance code with the *Personal Information Protection and Electronics Document Act* ("PIPEDA")[7] along with substantially equivalent laws in Alberta, Quebec, and British Columbia.[8] PIPEDA is a federal law that incorporates a national privacy standard (the "CSA Model Code"). The CSA Model Code outlines ten principles that form the basis of central obligations that any organization in the commercial sector needs to address when dealing with personal data.[9] The ten principles of the CSA Model Code were intended to serve as a template that could be adapted to unique circumstances. Commercial organizations are legally required to consider the ten principles when developing their privacy management program.[10]

Implications of Vehicular Infotainment Platforms. Online: < www.privacyandtheconnectedcar.com > .

6 Colin Bennett & Deirdre K. Mulligan, "The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy" (Paper prepared for the Privacy Law Scholars Conference at George Washington University, June 2012) [unpublished], online: < www.papers.ssrn.com/sol3/papers.cfm?abstract_id = 2230369 > [Bennett & Mulligan].

7 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*].

8 See the Alberta Personal Information Protection Act, the British Columbia Personal Information Protection Act and, in Quebec, An Act respecting the Protection of Personal Information in the Private Sector.

9 These principles are discussed in greater detail below.

10 See Schedule 1 PIPEDA.

The code is aimed at providing greater clarity regarding how individuals' (defined as a driver or the passenger of a vehicle)[11] personal information is handled. It purports to outline the responsibilities of users of personal data in the context of connected or autonomous vehicles. The aim is to offer industry guidance while educating automakers, regulators, consumers, and other members of the automotive sector regarding the implications of security risks in handling personal information. The term "user of personal information" refers to those entities that directly involve vehicles in their businesses (i.e. original equipment manufacturers, automotive suppliers, repair and maintenance companies, vehicle dealers and rental car companies).[12]

In the next section a brief overview of connected and automated vehicle technology is provided. This is followed by a discussion of the current approach to privacy protection, together with the limitations of that approach. The remainder of the paper will discuss the codes of practice generally and their specific application in to CAVs. A draft model code is provided as an appendix to this paper.

2. CONNECTED AND AUTOMATED VEHICLE TECHNOLOGY

Most passengers and goods in Canada travel by road. In 2016, more than 24.6 million road motor vehicles were registered in Canada, up 1.2% from 2016 and 19.3% from a decade ago. 92% were vehicles weighing less than 4,500 kilograms, mainly passenger automobiles, pickups, sport utility vehicles and minivans. 4.4% were medium and heavy trucks weighing 4,500 kilograms or more, and 3.3% were other vehicles such as buses, motorcycles and mopeds.[13] It is estimated that ninety percent of motor vehicle crashes are caused at least in part by human error.[14]

Connected vehicles utilize wireless technology to enable a diverse range of consumer convenience and infotainment applications. They also permit vehicles to send and receive information to other cars, the transportation infrastructure and a range of other wireless devices.[15] Automated vehicles by contrast make use of sensors and computer analytics to assess the external environment and

---

[11] See Appendix — A Code of Practice for Connected and Automated Vehicles.

[12] *Ibid.* — see also Deloitte (2018) Connected and autonomous vehicles in Ontario Implications for data access, ownership, privacy and security. Online: < www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-EN-CVAV-Research-Final-Data-Privacy-Security-Report-20180425-AODA.PDF >

[13] Transport Canada, "Transportation in Canada: Overview Report 2018" (2018), online: < www.tc.gc.ca/eng/policy/transportation-canada-2018.html > .

[14] Bryant Walker Smith, "Human Error as a Cause of Vehicle Crashes" *The Center for Internet and Society* (blog) (18 December 2013), online: < www.cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes > .

[15] Saif Al-Sultan et al., "A Comprehensive Survey on Vehicular Ad Hoc Network" (2014) 37 J. Network & Computer Applications 380.

perform numerous driving tasks instead of a human driver. This might include steering, braking and acceleration and monitoring the driving environment.[16]

The Society of Automotive Engineers defines six levels of automation.[17] These levels range from no automation to full automation.

> Level 0 No automation: The human driver performs all aspects of the driving task.
>
> Level 1 Driver assistance: The vehicle's driver assistance features support the driver with either steering or acceleration/deceleration under specific conditions. The human driver is expected to perform all remaining aspects of the dynamic driving tasks, including monitoring and responding to the driving environment.
>
> Level 2 Partial automation: The vehicle's driver assistance features support the driver with both steering and acceleration/deceleration under specific conditions. The human driver is still expected to perform all remaining aspects of the dynamic driving tasks, including monitoring and responding to the driving environment.
>
> Level 3 Conditional automation: The vehicle's automated driving system (ADS) features perform all aspects of the dynamic driving task, including monitoring and responding to the driving environment, under specific conditions. The human driver must be alert and ready to perform the dynamic driving task when the system requests the human driver to intervene.
>
> Level 4 High automation: The ADS-equipped vehicle performs all aspects of the dynamic driving task, including monitoring and responding to the driving environment, under specific conditions. The vehicle is designed to respond safely without human action to all situations, including when it reaches the limits of its operating environment.
>
> Level 5 Full automation: The ADS-equipped vehicle performs all aspects of the dynamic driving task, including monitoring and responding to the driving environment, in all conditions.

Vehicles in Canada have automation ranging from levels 0 to 2. Testing of automated vehicle technologies at levels 3 and 4 is underway in many countries, including Canada.[18] However, regardless of the level of automation, the

---

[16] Transport Canada, "Automated and Connected Vehicles" online: <www.tc.gc.ca/en/services/road/innovative-technologies/automated-connected-vehicles.html>.

[17] SAE International (2019). International standard J3016 taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. Online <www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic>. — for Terms Related to Driving Automation Systems for On-Road Motor Vehicles" (SAE Recommended Practice #J3016_201806, revised 15 June 2018), online: <www.sae.org/standards/content/j3016_201806/>.

[18] Transport Canada, "Automated and Connected Vehicles 101" (last modified 18 July

distinction between connected and automated vehicles is becoming increasingly blurred.[19] This is because advanced driving automation requires high levels of connectivity for some purposes such as downloading maps and updating software. It is the level of connectivity and data sharing that is the greatest source of potential privacy harms given the sensitivity and volume of personal information implicated in this context.

Data generated from connected vehicles fall into two main categories. "Telematics" data is generated from vehicles' sensors that makes use of information about a vehicle's internal systems. This type of data is used for car diagnostics and emergencies as well as to enable roadside assistance. Connected vehicles also process and store "infotainment" data. This data consists of non-vehicular information that provides drivers functions such as hands-free calling, text messaging and Internet capability.[20]

The data generated by connected vehicles has a great number of benefits such as reducing accidents, alleviating traffic congestion and product design improvement.[21] In order to accomplish this, it is necessary for vehicles to communicate with each other and the infrastructure. Thus, they need to exchange neighborhood information on a regular basis. As a result, connected vehicles broadcast unencrypted messages that contain a vehicle identifier together with the vehicle's location, speed and direction.[22] From this information, a driver profile may be developed that may be used for legitimate reasons such as providing emergency services and law enforcement, as well as a range of illegitimate reasons such as surreptitious surveillance by employers, insurance companies or criminals. The inferences that can be derived from driver profiles can reveal sensitive locations, such as home, office and places frequently visited. It should be noted, however, that the need for location privacy can often conflict with authentication requirements since safety critical information also needs to be received.[23]

As discussed in the next section, current solutions to protecting personal data rely on customer consent. As a consequence, the data handling practices of a

---

2019), online: < www.tc.gc.ca/en/services/road/innovative-technologies/automated-connected-vehicles/av-cv-101.html > .

19 Canada, Standing Senate Committee on Transport and Communications, *Driving Change: Technology and the Future of the Automated Vehicle*, 1st Sess., 42nd Parl. (January 2018) at 23, online: < www.sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_e.pdf > .

20 Lawson, *supra* note 4 at 5.

21 Araz Taeihagh & Hazel Si Min Lim, "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks" (2019) 39:1 Transport Reviews 103.

22 Florian Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks" in George Danezis & Philippe Golle, eds., *Privacy Enhancing Technologies* (Cambridge, U.K.: Springer, 2006) 197, online: < www.link.springer.com/chapter/10.1007/11767831_13 > .

23 *Ibid.*

given service provider are set out in the company's privacy statement. Since it is up to the service provider to determine how privacy policies and controls should be meaningfully conveyed to users, there are strong incentives to discharge privacy obligations via a corporate privacy statement.

3. THE CURRENT APPROACH TO PRIVACY PROTECTION

PIPEDA has been described as a "compromise both as to substance and as to form" since its aim is to protect individual privacy but also recognize the commercial need of businesses to collect personal data.[24] Privacy regulation in this area is essentially about reconciling this internal contradiction. Central to the operation of the Act is the definition of personal information. The Act states "personal information" means "information about an identifiable individual, but does not include the name, title, business address or telephone number of an employee of an organization."[25]

If PIPEDA is applicable to the organization, then section 5(1) requires that it comply with the obligations set out in Schedule 1 of the Act. This Schedule incorporates the CSA Model Code for the Protection of Personal Information (the Model Code). The Model Code includes ten principles: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use, Disclosure, and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance. These obligations are further qualified by stating that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[26] The requirement that information practices be reasonable has become a *de facto* balancing test employed by the Office of the Privacy Commissioner of Canada (OPC) to determine whether there has been implied consent.[27]

PIPEDA assumes that individuals control information about themselves and can choose to disclose their information.[28] Once disclosed, consent is required to use the personal information in ways not originally intended i.e. for secondary purposes. The approach is aimed at empowering individuals by fostering mechanisms, both legal and technical, that enhance individual control of data.[29] Individuals have autonomy over their data and organizations have obligations to respect rights to notice, access and consent regarding the collection, use and disclosure of personal data. Solove refers to this approach to privacy protection

---

[24] *Englander v. Telus Communications Inc.*, 2004 FCA 387, 2004 CarswellNat 4119, 2004 CarswellNat 5422 (F.C.A.) at para. 39.

[25] *PIPEDA*, *supra* note 7 at s. 2(1).

[26] *PIPEDA*, *supra* note 7 at s. 5(3).

[27] Lisa Austin, "Reviewing *PIPEDA*: Control, Privacy and the Limits of Fair Information Practices" (2006) 44:1 Can Bus. L. J. 21 at 29.

[28] *Ibid.*

[29] *Ibid.*

as "privacy self-management" since the goal is to provide individuals with control over their personal data so that they can decide how to evaluate the benefits and costs of collection, use and/or disclosure of their information.[30]

Proponents of this approach to privacy protection view personal autonomy as paramount. They argue that "removing consent from the equation risks undermining fundamental individual rights, protections and freedoms."[31] This approach, also referred to as informational self-determination, has been the subject of criticism by privacy scholars.[32] Empirical findings in behavioural economics literature, for example, has clearly demonstrated that people often overvalue the immediate benefits they obtain from revealing information and underestimate the cumulative risks associated with the cost of privacy loss.[33] While companies attempt to convey their data handling practices in their privacy statements, linguistic analysis undertaken by Pollach has "shown that companies obscure privacy infringements by downplaying their frequency, mitigating or enhancing questionable practices and omitting references to themselves when they talk about unethical data handling practices."[34]

For the most part, corporate privacy statements are drafted for the benefit of the organization rather that the consumer.[35] This defensive approach to privacy protection is understandable given that companies are required to comply with all the obligations of the CSA Model Code once personal information is involved. As a result, companies are inclined to state their data handling practices in obtuse language knowing that even though this document will not be read, it will nevertheless be binding on the consumer.[36]

To constitute personal information, data must be attributed to an identifiable individual. However, the information need not be collected directly by the company for it to be "about" an identifiable individual. In the vehicle context, if a company keeps record of a vehicle identification number and registered owner, the information will be deemed to be personal information.[37] It does not matter who "owns" the information or whether the information was

---

30 Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv. L. Rev. 1880 at 1880 [Solove].

31 Ann Cavoukian, Alexander Dix & Khaled El Emam, "The Unintended Consequences of Privacy Paternalism" (Toronto: Information and Privacy Commissioner of Ontario, 2014) at 7, online: < www.ontla.on.ca/library/repository/mon/28003/326077.pdf > .

32 Lisa Austin, "Privacy and the Question of Technology" (2003) 22:2 Law & Phil 119; Lisa Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006) 56:2 U.T.L.J. 181; Solove, *supra* note 30.

33 Alessandro Acquisti, Idris Adjerid & Larua Brandimarte, "Gone in 15 Seconds: The Limits of Privacy Transparency and Control" (2013) 11:4 IEEE Security & Privacy 72.

34 Irene Pollach, "What's Wrong with Online Privacy Policies?" (2007) 50:9 Communications of the ACM 103 at 107.

35 *Ibid.*

36 *Ibid.*

37 Teresa Scassa, Jennifer A. Chandler & Elizabeth F. Judge, "Privacy by the Wayside: The

generated by the company. The courts have held that personal information means *any* information about a specific person, subject only to specific exceptions.[38] Information will be about an 'identifiable individual' where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.[39]

However, whether object-oriented information constitutes personal information is currently unsettled in Canadian law.[40] It was held for example that information about an object is not personal information.[41] The Privacy Commissioner of Alberta has argued that information about an object *is* personal information.[42] Lastly, it has been argued that information which is identifiable and is being used for a purpose relating to that individual is personal information.[43]

Until the issue of object-oriented personal information is settled by Canadian courts, there will continue to be uncertainty regarding the appropriate remit of privacy law with respect to connected and automated vehicles. Since the current privacy code of practice stems from PIPEDA, data that cannot be reasonably linked to an individual and is regarded as anonymous is out of scope of PIPEDA and by extension the code of practice.

3.1 Limitations on the current approach

Determining whether a company is dealing with identifiable and therefore personal information and whether the information is anonymous is the source of considerable uncertainty for parties dealing with connected vehicle data. Suppliers of connected vehicle services typically state that they cannot supply the services customers want without accessing vehicle information, including location information.[44] This view focuses on individual consent to data sharing and links obtaining consent to benefits offered by connected cars in terms of safety and convenience.

New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems" (2011) 74:1 Sask. L. Rev. 117.

38 *Dagg v. Canada (Minister of Finance)*, 1997 CarswellNat 870, 1997 CarswellNat 869, [1997] 2 S.C.R. 403 (S.C.C.).

39 *Gordon v. Canada (Minister of Health)*, 2008 FC 258, 2008 CarswellNat 522, 2008 CarswellNat 6510 (F.C.).

40 John Beardwood & Mark Bowman, "The Internet of Things and Privacy: An Analytic Framework," (2016) 17:5 Computer Law Review International 140.

41 *Leon's Furniture Ltd. v. Alberta (Information Privacy Commissioner)*, 2011 ABCA 94, 2011 CarswellAlta 453 (Alta. C.A.), leave to appeal refused 2011 CarswellAlta 1938, 2011 CarswellAlta 1939 (S.C.C.) [*Leon's*].

42 *Alberta Health, Re*, 2012 CarswellAlta 1983 (Alta. I.P.C.) [*Alberta Health*].

43 *Schindler Elevator Corp., Re*, 2012 BCIPC 25, 2012 CarswellBC 4283 (B.C. Information Privacy Commr.) [*Schindler Elevator*].

44 Akalu, *supra* note 5.

When presented with a privacy statement, the customer has essentially two options: take it, or leave it. However, as discussed above, people systematically under-estimate long-term privacy risks associated with the sharing of personal information in the first place. This has led some commentators to argue for mandated privacy regulation in relation to connected vehicles. For example, Lawson argues that "[j]ust 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."[45] However, at the present time there is little consensus about what an appropriate standard should be. Adopting a standard too early in the development of connected vehicles may restrict productive uses of the data generated by connected cars.

This being said, it is difficult to provide examples of the adverse effect that imposing a data protection standard might cause since all the potential uses of the data are not known. This being the case it becomes necessary to consider the values of data collection, use and disclosure that should guide the development of CAVs. As the Canadian Standards Association model code is incorporated by reference to PIPEDA, even in the absence of widespread industry support, a code of practice developed pursuant to the ten model principles can still inform data handling practices. In order to develop such a code, decisions need to be made regarding its aim, scope and application. It is to this exercise we now turn.

4. CODES OF PRACTICE AND CAVS

In a discussion, a paper exploring potential enhancements to consent under PIPEDA, OPC examined alternatives to the consent model as currently formulated.[46] The OPC states that its paper is motivated by a "concern that technology and business models have changed so significantly since PIPEDA was drafted as to affect personal information protections and to call into question the feasibility of obtaining meaningful consent."[47] One of the proposed enhancements to consent under PIPEDA are codes of practice. The OPC's role in the development of codes of practice is contemplated in section 24(c) of PIPEDA which requires the OPC to "encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10" of the Act.[48] The OPC remarks in its paper that "[w]e have not yet fully explored this provision."[49]

---

[45] Lawson, *supra* note 4 at 6.

[46] Office of the Privacy Commissioner of Canada, "Consent and Privacy: A Discussion Paper exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act" (2016), online: <www.priv.gc.ca/media/1806/consent_201605_e.pdf> [OPC Report].

[47] *Ibid*. at 1.

[48] See below for discussion of key sections of PIPEDA.

[49] OPC Report, *supra* note 46 at 21.

While privacy codes of practice have been used both in Canada and internationally, there is little consensus regarding the meaning of this term. Given the fact that codes of practice have no formal definition, it is important to clarify the definition of codes as a policy instrument. It has been noted that codes are often a response to consumer or competitive pressure, or real or threatened regulatory sanctions.[50] When comparing voluntary codes with regulation, he notes that "it is important to remember that neither regulatory nor voluntary approaches are flawless in their design or operation. While it is true that voluntary approaches may not always achieve their objectives, full compliance with regulatory regimes is also rare."[51]

Codes of practice can provide greater clarity for an individual's information in being processed and whether this is being done in a manner that is transparent and fair in line with their expectations. This being the case, efforts to facilitate codes of practice are said to "promote 'governance' rather than 'government'; it is less about encouraging organizations to move in the right direction than it is about regulation and compliance."[52]

Codes of practice operate on various levels of compulsion with sanctions on one end of the spectrum and voluntarism on the other. However, the power to initiate and enforce codes of practice in the commercial sector lies primarily in the marketplace. This is in contrast to regulatory systems where governments establish and enforce mandated laws. At their best, codes of practice bring in a level of specificity and sophistication to the implementation of privacy in practice that would be difficult to achieve with mandated legislation.

There are a number of limitations inherent to the use of codes of practice, however. It has been noted that: "[p]oorly designed or implemented codes can frustrate or mislead their intended audience. As well, codes not backed by action can have legal consequences under deceptive advertising regulations and through contract and tort law actions."[53] Secondly, there is the issue of enforceability and consequence for non-compliance. A weak code of practice, lacking support from major stakeholders may result in delays for necessary regulatory interventions. Lastly, there is the issue of getting the right stakeholders involved in developing and overseeing compliance with the code of practice.

Thus an ongoing challenge "is to know when voluntary codes are most likely to succeed and to establish solid development and implementation processes that are fair, effective and efficient."[54] Codes can shape the content of legislation and

---

[50] Industry Canada, "A Framework for Evaluating Voluntary Codes" (2002) at 9, online: <www.ic.gc.ca/eic/site/oca-bc.nsf/vwapj/EvaluationFramework.pdf/$file/Evaluation-Framework.pdf>.

[51] *Ibid.*

[52] Bennett & Mulligan, *supra* note 6 at 3.

[53] Industry Canada & Treasury Board Secretariat, "Voluntary Codes: A Guide for Their Development and Use" (1998) at 6, online: <www.ic.gc.ca/eic/site/oca-bc.nsf/vwapj/volcodes.pdf/$FILE/volcodes.pdf>.

[54] *Ibid.*

inform regulatory and court interpretation of adequate compliance. Codes of practice therefore "should be process rather than an output oriented. And they should entail a systematic effort to determine and manage legal, reputational, economic and social risk."[55]

5. DEVELOPING A CANADIAN PRIVACY CODE OF PRACTICE FOR CONNECTED VEHICLES

The issues raised above in relation to codes of practice are particularly salient in the case of CAVs. The marketplace for connected vehicles consists of a wide range of private sector stakeholders from car manufacturers to internet service providers and insurance agencies. It is also of interest to all levels of government. This section outlines current efforts to develop a Canadian privacy code of practice for connected vehicles.

5.1 Where to start?

The CSA Model Code was intended to be technology neutral and provide generic guidance as to how consumer personal data should be treated. Examples of personal data obtained from connected and/or autonomous vehicles include but are not limited to i) information about an individual (i.e. individual's location or itinerary), ii) information that can be used to identify, contact or locate an individual, and iii) information used by an individual to identify himself or herself.[56]

The code provided in the appendix to this paper makes important distinctions between sensitive and non-sensitive personal data. Location data is, for example, highly sensitive and should require explicit opt-in and opt-out consent. Appropriate standards for establishing anonymity could also be set enabling third parties to make use of data without consent.

Of central importance to the development of a code is the intended audience. Defining the scope of the code is a challenge as there is such a wide range of stakeholders. The code in its present form refers to those entities that directly involve vehicles in their businesses (i.e. original equipment manufacturers, automotive suppliers, vehicle dealers and rental car companies). These businesses would fall under the legal remit of PIPEDA or those provinces where substantially similar legislation is in place.

It should be noted therefore that this code does not have legal effect. The code is a process by which the substantive merits of specific data handling practices in the CAV sector can be meaningfully explored. This is important since

---

[55] Bennett & Mulligan, *supra* note 6 at 12.

[56] Leslie Jacobson, "Vehicle Infrastructure Integration Privacy Policies Framework" (Paper presented to the National Surface Transportation Infrastructure Financing Commission, Washington, D.C., on 17 April 2008, dated 16 February 2007), online: <www.financecommission.dot.gov/Documents/April2008Meetings_Hearings/VII_-Privacy_Policies_Framework-Approved_by_ELT.pdf>. [Jacobson]

CAV technologies are evolving rapidly in ways that are difficult to anticipate. This code is aimed at providing advisory guidance as opposed to endorsing legal compliance with Canadian privacy law, specifically PIPEDA.

Despite its shortcomings in terms of enforcement, the development of a code of practice is helpful insofar as it highlights particular areas of concern and questions that need to be addressed with respect to the protection of personal information. The exercise forces both specificity and clarity regarding the appropriateness of data handling practices as well as the sensitivity of that data.

In the code provided in the appendix below, each CSA privacy principle is taken in turns and interpreted to show how it applies to CAVs. This is done with the use of case scenarios. The code outlines the responsibilities of users of personal data and any third parties involved in data sharing in the context of connected or autonomous vehicles. In doing so, it offers guidance while educating automakers, regulators, consumers, and other members of automotive sector regarding the implications of security risks in handling personal information.

6. CONCLUSION

While a code of practice is not an 'optimal' solution and there are limitations to this approach, it should be noted at the outset that all policy instruments are sub-optimal in the face of technological change. A code of practice is no different in this regard. Its advantage, however, is that it can provide a principled response to an emerging technological trend. It also forces a substantive conversation concerning the relative merits of information handling practices with respect to CAVs.

Under the current regulatory regime there are incentives for automakers and other market participants to regard privacy protection as an abstract problem that can be solved with a well drafted privacy policy. The development of privacy codes of practice can serve as a learning process by which privacy concerns in a complex information environment may be addressed in a holistic way.

The CSA Model Code is beneficial when considering connected and automated vehicles because it forms part of PIPEDA and is intended to be technology neutral. By (re)interpreting the principles contained in the code it is possible to both comply with the spirit of PIPEDA as well as form the basis of common understanding regarding the protection of personal information among a diverse set of organizations associated with providing CAV products and services.

APPENDIX — A CODE OF PRACTICE FOR CONNECTED AND AUTOMATED VEHICLES

1. Introduction

1.1 There are many potential benefits of driverless and automated vehicle data, particularly the potential to create new business opportunities, improve road safety and facilitate consumer convenience and choice.

1.2 The publication of this Code of Practice is intended to help car manufacturers and users of connected and automated vehicle (CAV) data by providing guidelines and recommendations for measures that should be taken to protect the use of personal data used in the course of commercial activity.

1.3 This Code of Practice is non-statutory but has been developed in order to give expression to existing Canadian legislative requirements with respect to the protection of personal data. The aim of the Code is to promote responsible information practices in the CAV sector as well as inform consumers of their privacy rights. It should be used by organizations in conjunction with detailed knowledge of Canadian privacy law, in particular, the Personal Information Protection and Electronic Documents Act.

1.4 Failure to follow the Code may be relevant to liability in any legal proceedings. Similarly, compliance with the Code does not guarantee immunity from liability in such circumstances.

2. Aim, scope and definitions

Aim

2.1 While this Code of Practice outlines individual rights and user responsibilities with respect to personal information collected, used and disclosed by connected and automated vehicles in the private sector, this Code is not intended to apply to workplace privacy.

Commentary

[1] This Code of Practice serves as a statement of best practice for compliance with PIPEDA principles. The Code should be used in combination as a quasi-legal compliance code with the *Personal Information and Electronics Document Act* (PIPEDA) along with substantially equivalent laws in Alberta, Quebec, and British Columbia. PIPEDA is a Federal law that incorporates a national privacy standard (the CSA model code). The CSA model code outlines ten principles that form the basis of central obligations that any organization in the commercial sector needs to address when dealing with personal data.[57]

[57] SCHEDULE 1 (Section 5) Principles Set Out in the National Standard of Canada

[2] The ten principles of the CSA model code were intended to serve as a template that could be adapted to unique circumstances. Commercial organizations are legally required to consider the ten principles when developing their privacy management program. The ten principles of the CSA model code are: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use; Disclosure and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance. These principles are elaborated on and applied in this Code of Practice to connected and autonomous vehicles engaged in commercial activity Individuals are entitled to expect that commercial organizations comply with CSA principles since they are enshrined in law.

[3] The term user of personal information refers to those entities that directly involve vehicles in their businesses (i.e. original equipment manufacturers, automotive suppliers, repair and maintenance companies, vehicle dealers and rental car companies).

[4] The Code is aimed at providing greater clarity in how individuals' (defined as a driver or the passenger of a vehicle), personal information is being handled. It purports to outline the responsibilities of users of personal data in the context of connected or autonomous vehicles. The aim is to offer industry guidance, while educating automakers, regulators, consumers, and other members of the automotive sector regarding the implications of security risks in handling personal information.

Scope

2.2 This Code of Practice is intended to apply whenever personal data is collected, used and disclosed in the course of commercial activity by connected and automated vehicles in Canada.

Commentary

[1] The Code of Practice is intended to supplement the Personal Information Protection and Electronic Documents Act (PIPEDA). Subsequently, any data or organizations that could be categorized under the legislation will be within scope. According to PIPEDA, an organization(s) that collects and controls personal information is accountable for ensuring its use, storage, and disclosure comply with legislative requirements and protect personal privacy[58]. In order to align itself with the legislation, the Code is limited to that of the commercial activity

Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 Online < www.laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html > .

[58] *PIPEDA*, *supra* note 7.

within the private sector.

[2] Pursuant to section 2(1) of PIPEDA "commercial activity" refers to any transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.[59] This would include information collected as a function of the way the data collection mechanisms of the car or its applications work, which may not be immediately monetized but which are collected with commercial interest in mind. Certain examples include data sharing between automakers and third parties (as defined below), or the transaction of purchasing, renting, and/or car sharing a connected vehicle or autonomous vehicle along with any subsequent flow of personal information.

[3] This Code focuses on personal information, which can be described as any type of data that is collected, disclosed, summarized or extrapolated, in a way that can be associated or linked with an identifiable individual. Examples of personal data obtained from connected and or autonomous vehicles include but are not limited to; i) information about an individual (i.e. individual's location or itinerary), ii) information that can be used to identify, contact or locate an individual, and iii) information used by an individual to identify himself or herself.[60]

2.3 This code is intended to apply to entities that directly involve vehicles in their business. As such entities that use vehicle data indirectly, e.g. insurance companies use vehicle data, but do not directly involve vehicles in their business.[61] A description of the entities to which this code applies is found in section three.

2.4 The Code is not intended to apply to non-consumer or public sector activity.

Definitions

2.5 For the purposes of this document the following definitions should be understood:

Automated vehicle: This means a vehicle in which a driver is not necessary. The vehicle is designed to be capable of safely completing journeys without the need for a driver in all traffic, road and weather conditions that can be managed by a competent human driver.

---

59 *Ibid.*

60 See Jacobson, *supra* note 56.

61 It should be noted that usage based insurance is governed provincially by the Financial Services Commission See for example Financial Services Commission of Ontario, "Usage-Based Automobile Insurance Pricing in Ontario" Bulletin No. A-05/13 (3 October 2013), online: < www.fsco.gov.on.ca/en/auto/autobulletins/2013/Pages/a-05-13.aspx > .

Connected vehicle: Connected vehicles consist of two types of technologies: telematics and infotainment, and vehicle-to-vehicle and vehicle-to-infrastructure communications.

Sensitive Information: refers to information that must be safeguarded from unauthorized access and that which a reasonable person would expect that only certain people would have access to, with consent.

Commentary

[1] There are two main systems that generate data in a connected and automated vehicle: Telematics systems and infotainment systems. The data involved varies with respect to its level of sensitivity and it should be understood that data from multiple devices may be combined and generate a detailed profile of a given individual.

[2] Telematics systems are devices that produce:

i.Vehicle Health Data: about the performance of the car's components; used for vehicle diagnostics. Sensors in the car monitor when a vehicle is on the move, both in faulty condition (when any failure in a specific system has occurred) and in normal condition. This data is transmitted to the server which analyzes the data. There are four main subsystems of the vehicle namely its fuel system, ignition system, exhaust system, and cooling system that are typically being monitored.[62] This type of data is typically used for fault detection and preventative maintenance. It is not particularly sensitive as it can rarely be linked to an identifiable individual.

ii.Driver Behavior Data: about how or when the driver is operating the vehicle. The behavior of drivers can be monitored by using the data that is collected from the connected vehicles. Risky driving behavior can be detected and the actual driving patterns of a vehicle operator to identify unsafe practices or policy violations. This can be used to determine whether the drive accelerated or braked harshly, speeding or fatigued driving. Vehicle fleet operations management and insurance companies can get powerful insights into customer vehicle usage and risk assessment.

iii.Location Data: GPS data generated by vehicles can be monitored and analyzed in order to provide certain services to the driver, i.e. usage-based insurance, entertainment services, navigation etc. It is possible to get additional private data, even if the basic data at first look, seems not so harmful.[63] This type

[62] Uferah Shafi et al., "Vehicle Remote Health Monitoring and Prognostic Maintenance System" (2018) J. Advanced Transportation, online: < www.downloads.hindawi.com/journals/jat/2018/8061514.pdf > .

of data can be regarded as highly sensitive.

iv.Driver Health & Biometric Data: heartbeat & head/eye movement
Biometrics is a technology that measures a person's fingerprints, facial features and other unique characteristics in order to verify one's identity. It can also determine physical well-being when they are driving; things like heart rate, blood pressure, drowsiness, increased levels of blood alcohol content, and warnings about a potential epileptic seizure.[64] This type of data is particularly sensitive given what it can potentially reveal about a given individual.

v. Information associated with electric vehicles: companies have the ability to monitor the use of charging stations which gives them information concerning the location and pattern use.

b.Infotainment systems: are devices that produce:

i.Personal Communications Data: voice/text/email/social networking data sent/received via in-car system

ii.Personal Contacts & Schedules

iii.User's choice of entertainment

Apple's CarPlay and Google's Android Auto are prominent examples of the trend towards integrated in-vehicle infotainment systems. Many car manufacturers have their own proprietary infotainment systems. The privacy and security risks associated with information exchange between the vehicle's infotainment platform and the user's mobile phone are not well understood. The lack of transparency concerning the exchange of data generated by the vehicle and third-party applications raises legitimate privacy concerns that fall outside the scope of this Code.

Personal Information: any information about an identifiable individual recorded in any form.

Anonymous Information: any information that is collected, disclosed, extrapolated in such a way that no longer provides any personal identifiers about an individual.

Commentary

---

[63] Vladimir Kaplun & Michael Segal, "Breaching the Privacy of Connected Vehicles Network" (2019) 70:4 Telecommunications Systems 541.

[64] Melanie Swan, "Connected Car: Quantified Self becomes Quantified Car" (2015) 4:1 J. Sensor & Actuator Networks 2.

[1] The relationship between personal information and anonymous information is an important aspect to consider in any discussion of connected and automated vehicles. Central to this question is the extent to which object-oriented information constitutes personal information. Canadian courts are conflicted on this rather fundamental issue. It has held for example that information about an object is not personal information.[65] The privacy commissioner of Alberta has argued that Information about an object is personal information.[66] Lastly, it has been argued that information which is identifiable and is being used for a purpose relating to that individual, is personal information.[67]

[2] Until the issue of object-oriented personal information is settled by Canadian courts there will continue to be uncertainty regarding the appropriate remit of privacy law with respect to connected and automated vehicles. For the purposes of the present Code, data that cannot be reasonably linked to an individual and is regarded as anonymous is out of scope of PIPEDA and by extension this code of practice. Information from a vehicle is collected in such a way, where it can no longer reasonably ascertain an individual's identity, and personal information as it would provide a level of anonymity and thus is out of scope under PIPEDA and this code of practice.

Individual: refers to a human occupant, owner or operator of an autonomous or connected vehicle.

Personal information user: Any entity, organization, or individual that collects, discloses or uses the personal information in the context of the autonomous or connected vehicle environment.

Third Party: Any entity, organization or individual other than the automaker which gains access to the personal information of an individual.

Telematics: systems which relay information regarding an individual's driving behavior which includes but not restricted to metrics such as; speed of traveling, location, and driving and navigation systems.

Infotainment systems: systems which combine entertainment and information delivery to an individual.

Vehicular ad hoc networks (VANETs): a general class of mobile ad hoc networks that enable wireless communication between vehicles or with fixed equipment.

Vehicle to Vehicle (V2V): a communication system which allows for the flow of information with other vehicles through VANETs.

---

65 *Leon's*, *supra* note 41.

66 *Alberta Health*, *supra* note 42.

67 *Schindler Elevator*, *supra* note 43.

Vehicle to Infrastructure (V2I): a communication system which allows for the flow of information between vehicles and roadside infrastructure

Public road: In this Code, public road means any highway or other road to which the public have access.

3. Application of the Code of Practice

This code is intended to apply to entities that directly involve vehicles in their business. As such entities that use vehicle data indirectly, e.g. insurance companies, or government agencies are excluded. A description of entities to whom this code applies is provided below.

Original equipment manufacturers

Original equipment manufacturers are a major participant of automobile production and thus are an important focus within this Code of Practice. Automakers have the responsibility to meet consumer needs, not only in terms of vehicle efficiency when it comes to fuel, safety, performance and design but also in creating an environment which allows individuals to maintain a level of connectivity. OEMs can either offer their own infotainment service content or choose to use the content through the individual's smartphone. Telematics are used in two ways. Firstly, to reduce OEM expenses through, for example the ability to remotely update software reduces recall and warranty costs. Secondly, to generate revenue through selling consumers telematics features within the vehicle or to monetize the personal information collected from these telematics systems. When such data is used, the data may be made available to third parties such as advertising companies, data mining companies, application providers among others. Such a use of these systems is at the center of operations for many automakers, in fact many of the large automakers have developed their own telematics/infotainment platform brand and will continue to implement such technology to offer differentiated connected car services.

Automotive suppliers

Automotive suppliers are entities that provide automakers with inputs which are necessary for the proper functioning of telematics and infotainment systems. Because of the diverse components of such systems, the specific organizations are various. They include but are not limited to entities which provide hardware components, user interface devices, mobile software management, short range mobile device connectivity, audio services and application providers. As such these third parties may have access to a wide array of personal and non-personal data and ambiguity remains surrounding the handling of such information.

Vehicle dealers

A Vehicle dealer can be described as an entity which sells new or used vehicles to consumers. To be considered under the application of this Code, the dealer must

be selling vehicles of autonomous, or connected nature. Dealers are important participants in the automotive industry as they act as intermediaries through providing a point of purchase where individuals receive automobiles indirectly from the manufacturers. Dealers are in control of personal information obtained directly from consumers.

Rental car companies

A car rental company can be described as an agency which loans out automobiles for a specified period of time to a consumer in exchange for a monetary amount. Among vehicles rented, the majority of these vehicles are newer models and so they are equipped with infotainment systems and/or telematics. Car rental agencies use vehicle data obtained from the stream of telematics in the task of fleet management. This is done to track real-time vehicle location, obtain behavior based alert information (speeding, acceleration), vehicle usage behavior and vehicle diagnostic information. In terms of infotainment systems, much of the personal data that is extracted from personal devices such as mobile phones remain on the vehicle even after it is returned. This in itself constitutes a privacy threat as the renter is vulnerable to information theft. The data handling procedures is ambiguous as it is unclear on how long such data is held, who the data is sold or given to, or who controls this data.

4. Consumer Rights and Organizational Responsibilities

In this section a brief summary of each principle of the CSA model code (which mirrors the obligations in PIPEDA) is described together with how the principle is applied to the CAV context.

4.1 Principle 1 (Accountability): ''An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.''

Summary of Principle

The accountability principle contemplates appointing a ''designated individual(s)'' who is responsible for the oversight, compliance, and control of any personal information that an organization possesses. Such an individual' s identity must be available upon request which includes the title, and contact information. An ideal candidate would be one who is; (1) in a high level within the organization so that one has sufficient autonomy to ensure implementation of Code's principles, (2) has no employee duties which may place a conflict of interest between privacy policies and/or other job demands, (3) understands on how personal information is utilized, handled, distributed both within the organization, and to third parties.

Application of Principle 1 — Accountability

OEM

Being that most if not all OEMs are large organizations and that many high level positions have some type of overlap in terms of the responsibilities it is ideal to create a new position of a privacy officer who oversees activities (which involve telematics and infotainment systems). He or she would be obligated to uphold these ten principles concerning personal information. Alternatively, chief security officers could be given such responsibility. Regardless, it is vital that this individual possesses some technical knowledge or at a minimum the access to that knowledge.

Automotive Suppliers

Automotive suppliers vary with the inputs they provide to automakers, and so there may not be one ideal way to apply the accountability principle according to this principle. One must judge the most suitable candidate for a designated individual based on the organizational structure. However, the individuals could be selected from the following; a vice president of corporate services, a legal officer, a security manager, or corporate security officer.

Vehicle Dealers

Vehicle dealers obtain personal information from different individuals at various locations. Because of this, there should be a specified designated individual at each of these locations in charge of compliance.

Rental Agencies

Similar to vehicle dealers, rental agencies obtain personal information from consumers from various branches and as such a designated individual should be assigned to each of these locations. The main privacy concern is relative to infotainment systems which often occurs when a consumer connects their mobile device to the vehicle and such data remains after the automobile is returned.

4.2 Principle 2 (Identifying Purposes): "The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection."

Summary of Principle

Information that is collected by an organization should be viewed in terms of necessity. This implies that personal information that is requested should serve an essential purpose. Both information which is deemed necessary or secondary must be identified along with the policies concerning maintenance, the uses, and any source(s) which will gain access to the information, either before or at the time of collection. Individuals must be given the choice to accept or reject such uses. Handling of such information should conform to the definitions the

organization provided and should be documented in plain language if such documentation is highly technical or used within company sensitive material.

Application of Principle 2 — Identifying Purposes

OEM

OEMs have the capability to access a wide range of personal and non-personal information. Much of the information collected is personal, and is usually collected without the knowledge of consumers. Often, safety measures are cited as the reason for this practice. However, if such data collection measures are deemed as necessary for the safety of an individual, this data should be anonymized.

Automotive Suppliers

Automotive suppliers can collect both personal and non-personal data from consumers. For example, Advanced Driver Assistance Systems can obtain driving behavior data and hardware providers can receive information concerning the vehicle. The requirement to identify the purposes of data collection is particularly important in the case of automotive suppliers as there is a wide range of secondary uses of collected data.

Vehicle Dealers

There is often ambiguity when vehicle dealers collect personal information from consumers. Before any collection of the data occurs, the designated individual should ensure that consumers receive a plain-language document identifying the purposes of data collection.

Rental Agencies

Rental agencies provide a highly technical agreement at the point of sale. This agreement will typically outline the purposes for which personal data is being collected. Customers should be made aware of what information is collected and whether it is used for secondary purposes such as fleet management.

4.3 Principle 3 (Consent): The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Summary of Principle

Individuals must provide consent through express or implied terms when it comes to the uses of their personal information. Following the Office of the Privacy Commission of Canada guidelines on obtaining meaningful consent[68] companies should obtain explicit consent for collections, uses or disclosures

[68] Office of the Privacy Commissioner of Canada, "Guidelines on Obtaining Meaningful

which generally: (i) involves sensitive information; (ii) are outside the reasonable expectations of the individual; and/or (iii) create a meaningful residual risk of **significant** harm. Exceptions include situations where obtaining consent would be considered inappropriate or impossible. Such situations include; security or criminal investigations, individual is a minor, medical emergencies, cases of physical or mental incapacitation, or the interests of public supersede that of the individual. Express consent can be any action by which an individual explicitly authorizes the use of their personal information i.e. signature, checking off a box, verbal approval, or a method of agreement which is appropriate according to the situation. This method should be used when collecting forms of personal information. Implied consent are actions or inactions where which one can reasonably determine that consent has been achieved. Such a method is more ambiguous as the individual may have not understood what they have consented to or the lack of proof of such consent. Subsequently, implied consent should be avoided when it comes to obtaining sensitive personal information in CAVs.

Application of Principle 3 – Consent

OEM/ Automotive Suppliers

Individuals are often left to decipher this information as they are expected to hold autonomy over their data. However, since the information will be collected by the automakers they hold the responsibility to explain the intended uses and impact of their data in clear, simple and understandable language, and then it is acceptable to obtain the consent of the individual.

Rental Agencies/Vehicle Dealers

In the contractual agreements the acknowledgment that information is collected is stated, however, the intended sources, how it will be used, whom it is disclosed often is not clearly mentioned. Moreover, if consumers deny signing the contract, they may be denied access to the service.

4.4 Principle 4 (Limiting Collection): The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Summary of Principle

Organizations have an obligation to limit the uses and the gathering of information to which is necessary and defined as the specified purposes (at the time or before collection). As such, the method of collecting information should be conducted in an appropriate manner meaning, individuals must never be coerced, threatened, misled in providing information or should not be gathered

---

Consent" (May 2018), online: < www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ > .

from acquaintances without explicit consent of the individual in question. The consent to marketing should not be tied as part of the warranty process for example.

Application of Principle 4 — See Principle 5 below

4.5 Principle 5 (Limiting Use, Disclosure and Retention): Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Summary of Principle

Organization's should develop guidelines when it comes to retaining the data such as the minimum or maximum lengths they will be in possession of the information.

Application of Principle 4 and Principle 5 – Limiting Collection & Limiting Use, and Disclosure

OEM

Automakers sometimes use personal information in purposes which have not been identified to individuals. They can use such information to establish relationships with their intermediaries or other third parties in order to monetize such information. As such, automakers must only collect personal data which will only be directly used in terms of relevant purposes (i.e safety, direct information needed for a transaction).

Automotive Suppliers

Due to the wide applications automotive suppliers provide, the amount of information they can collect, retain, and disclose is considerable. However, each automotive supplier must limit their collection of information only to that which is relevant to the purposes of their input. For example, suppliers of a mobile interface should only collect information such as preferences or feedback on what the user likes or dislikes about the software in order to provide a refined product.

Rental Agencies

Frequently, personal information remains on rental vehicles after the individual returns the automobile to the agency. The retention of the data has no maximum or minimum periods, rather is held until another consumer erases the data to in order to connect their own personal mobile device.

4.6 Principle 6 (Accuracy): Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Summary of Principle

The personal information that is collected, must be an accurate representation of the individual in order to avoid risks of discrimination or any harm done by inaccurate or incomplete data. To achieve a satisfactory level of accuracy, entities should allow the individual to review and update the information, documenting purposes, and implementing a system in which regular corrections and updates occur.

Application of Principle 6 – Accuracy

OEM

If an OEM holds personal information about an individual they are required that such information is accurate, complete and up to date. To ensure data quality, any information should be available to review. After which the individual may make a written request to update inaccurate, incomplete or equivocal information. Automakers should use this as a model in order to allow for upholding the CSA Principle of Accuracy.

Automotive Suppliers

Once automotive suppliers have collected an amount of information which a reasonable person would deem relevant, they should strive to make the opportunity available to their consumers to review the compilation of data and make corrections. To the extent possible they should try and limit the amount of information gathered as when size of the collection increases so does the risk of collecting inaccurate data.

4.7 Principle 7 (Safeguards): Personal Information must be protected by appropriate security relative to the sensitivity of the information

Summary of Principle

Throughout the process of data collection, the organization should ensure sufficient security measures to avoid security breaches, or accidental disclosure of personal information. Such measures could include but are not limited to; evaluating existing measures and the suitability to protect the data, implementing physical, organizational and technological safeguards.

Application of Principle 7 – Safeguards

OEM /Automotive Suppliers

Given that automakers and automotive suppliers obtain a wide array of personal data, their responsibility to protect the individual is greater than other stakeholders. Firstly, they should access their current systems and identify any points of which could run the risk of breaches, thefts, or disclosure.

Vehicle Dealers

Vehicle dealers are primarily involved in repair and maintenance activities. They initially obtain personal information (through data sharing) and direct collection after they store it. To ensure sufficient security, vehicle dealers should restrict physical access so that only qualified individuals can retrieve personal information.

Rental Agencies

As mentioned earlier, information that is not deleted from onboard infotainment systems are available to those who are not qualified and in fact can be total strangers. Thus, rental agencies should first verify if data has been wiped from these systems and additionally should ensure staff members participate in regular training programs so that they are capable of clearing the information and instructing consumers on how to delete their information.

4.8 Principle 8 (Openness): An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Summary of Principle

An organization must be transparent in terms of their policies and procedures regarding personal information. Such openness is done in order to create a relationship of trust between the entity and the individual. An adequate level of openness would be considered wherein an individual can easily obtain materials concerning the retention, disclosure, and use of their personal information.

It can be argued that this principle is followed since almost all such entities post privacy policies on their websites. However, these policy statements are often very difficult to understand. It is crucial that policies are expressed in plain language.

Application of Principle 8 – Openness

OEM

Automakers across the industry are similar in terms of handling of personal information. Subsequently, a generic strategy of making available copies of industry sector policies that explains how such these practices are in compliance with the CSA Code Principles along with the PIPEDA can be used as the source of openness.

Automotive Suppliers

At the present time, automotive suppliers typically meet the openness requirement with a privacy statement. This statement is usually written in

technical language. Such resources should be made easily available, and readily accessible to individuals upon request.

Vehicle Dealers

Vehicle dealers obtain personal information through data sharing, and through telematics devices. This information can be used to create marketing databases, or for warranty, repair and or maintenance services. It is crucial for these entities to make a consumer privacy brochure available at major points of interaction along with the training of dealers (i.e. purchase of an automobile, renewal of the lease, change of agreement, etc.)

Rental Agencies

Rental agencies are varied in terms of the vehicles they offer however, there is the similarity that most if not all of these vehicles are of connected nature. So, the method in which personal information collected is analogous. Similar to vehicle dealers, it would be ideal to adopt a company specific brochure beyond that of the privacy terms and services which are given to the consumers at the times of interaction as each company may handle data in different but appropriate manners.

4.9 Principle 9 (Individual Access): Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and 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.

Summary of Principle

If requested, an individual must be provided with the information concerning the use, purposes, maintenance, retention and disclosure of their personal data. To meet the principle of individual access one must achieve four steps which are outlined in the CSA Code:

- A request by the individual for the kind of personal information the organization maintains, its substantive nature, its uses, and the third parties to which it has been or may have been disclosed.
- Timely response from the organization, either providing the information requested or written reasons why that information cannot be provided, preferably citing a specific exemption that is documented within the organization‘s privacy code. If information is withheld, the individual should be informed about redress procedures.
- If information is provided, the individual may challenge its factual accuracy, as well as its completeness and relevance
- The correction or deletion of any information that is successfully challenged and a

- Communication of that correction to every internal data user and external third party who may have received it.

Application of Principle 9 — Individual Access

OEM/ Automotive Suppliers

Beyond the standard application that OEMs and automotive suppliers must be able to provide a detailed, accurate file concerning the personal information they must provide communication of any correction or deletion of any information that been shared with other parties.

Rental Agencies

Although it may be the case that rental agencies often do not receive any requests from consumers regarding their information, they must adopt a system in which if such an event occurs the individual will be informed of the existence, the disclosure, the uses, and the access to the information itself.

4.10 Principle 10 (Challenging Compliance): An individual shall be able to challenge an organization's compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Summary of Principle

Although an entity can introduce the ten listed principles, this does not ensure compliance can be challenged. Organizations must allow for inquiries, complaints, and challenges regarding compliance and should handle such complaints in a manner consistent with principle 8 - Openess.

Application of Principle 10 — Challenging Compliance

OEM

The automotive industry is represented by two associations, the Canadian Vehicle Manufacturers' Association and the Global Automakers of Canada. It should be the responsibility of these associations to establish uniform procedures to receive and handle complaints and inform consumers about their opportunities for redress/making complaints. It can be to require each automaker to have specific privacy departments, or possibly assign this responsibility to an existing employee.

Automotive Suppliers

Due to the nature of the relationship, automotive suppliers usually do not come in direct contact with consumers and dealing with complaints may not be a straightforward process. However, if consumers have an issue with the compliance, a system must be created where which these organizations have

front line customer service staff which are positioned with the partnering original equipment manufacturer to relay such concerns.

Vehicle Dealers

Consumers primarily interact with sales representatives of vehicle dealerships. This occurs for example when initially purchasing an automobile, or follow-up correspondence concerning vehicle services. Therefore, the most appropriate manner to handle complaints is through sale representatives. The organizations can simply expand the responsibilities held in these positions to include responding to inquiries and complaints concerning their information handling policies and practices.

Rental Agencies

Individuals for the most part deal with front line employees when they wish to rent a vehicle. To facilitate an appropriate process of compliance, the organization must first ensure their front level staff are trained and kept updated with changing privacy requirements. Secondly, the front-line customer service staff must be trained in an appropriate manner to receive and react to individual complaints.