A PRIVACY CODE OF PRACTICE FOR THE

CONNECTED CAR

RAJEN AKALU, Ph.D.
Assistant Professor
Faculty of Business and IT

OntarioTech University
2000 Simcoe Street North Oshawa, Ontario L1H 7K4 Canada | 905 721 8668 x 5438 | rajen.akalu@uoit.ca

SUMMARY

This code of practice relates to privacy with respect to connected and automated vehicles (CAVs). As codes of practice vary greatly in terms of their regulatory scope and CAVs encompass a wide range of emerging technologies, it is important to establish the aim and scope of this document at the outset and outline how this code was developed.

This project began with the aim of building consensus among stakeholders regarding the development of a code that would provide enhanced privacy protection for Canadians with respect to CAVs. It also intended to provide clearer and more predictable rules for CAV organizations with respect to the collection, use and disclosure of personal information.

However, the project encountered resistance among key stakeholders such as the automotive associations and original equipment manufacturers. The reasons these stakeholders were reluctant to engage in the code development process is important and worthy of mention. Several automakers argued for example that Canadian privacy law, namely The Personal Information Protection and Electronic Documents Act (PIPEDA) already provided a strong privacy framework. Any additional unique to Canada prescriptive regulations they argued, would result in increased cost to consumers. If an organization complies with PIPEDA, a code of practice would be unnecessary.

However, compliance with PIPEDA is by no means a settled issue and levels of privacy protection can vary widely among organizations. In the absence of key stakeholder involvement, the project shifted towards how organizations related to the provision of CAVs might demonstrate compliance with the Act as well as educate consumers regarding the types of data involved with CAVs.

It is worthwhile to note that the Act that is now PIPEDA itself began as a code of practice – the Canadian Standards Association (CSA) model principles. The ten principles, which are incorporated as a schedule to the Act, provide guidance to organizations on appropriate data handling practices.

The ten principles of the CSA model code form the basis of central obligations that any organization in the commercial sector needs to address when dealing with personal data. This code therefore derives its legitimacy from existing legislation rather than being the product of stakeholder consensus.

It should be clearly noted therefore that this code does not have legal effect. It should rather be viewed as a process by which the substantive merits of specific data handling practices in the CAV sector can be meaningfully explored. This is important since that 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. Developing a privacy code of practice for CAV is well and truly where

the ‘rubber meets the road’. It is essentially an orienting process. By interpreting and applying the CSA model code to CAVs we may better direct regulatory and technical efforts to provide adequate privacy protection in the face of a fast-changing technological landscape.

As mentioned, this code takes as its starting point the CSA model code and PIPEDA. PIPEDA is a federal law and it should be noted that other provinces have enacted substantially similar legislation. This code is thus broadly applicable throughout Canada.

The scope of this code is limited to entities that directly involve vehicles in their business. As such, private entities that use vehicle data indirectly, e.g. insurance companies are excluded. That is not to say that insurance companies have reduced obligations with respect to privacy protection, but rather their involvement is tangential to a discussion on how privacy protection will be directly implemented in CAVs

This code of practice contributes to the discussion of privacy protection in CAVs by outlining the specific types of data generated by CAVs namely telematics systems and infotainment systems. The data involved in these systems vary with respect to its level of sensitivity. Location data for example has a greater degree of sensitivity compared to vehicle health data. It should be understood that data from multiple devices may be combined and generate a detailed profile of a given individual. Having a sense of the degree of sensitivity associated with data provides insight into the types of privacy safeguards will be required.

Correlated to the issue of data sensitivity is relationship between data that is personal information and anonymous information. Central to this question is the extent to which object-oriented information constitutes personal information. If personal information can be vested in objects the organizations will become responsible for safeguarding this data. If not, the organization may potentially use this data in order without consumer consent. 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(s) and is regarded as anonymous is out of scope of PIPEDA and by extension this code of practice.

The development of this code was funded by the Office of the Privacy Commissioner of Canada Contributions Program. It has taken place with the effort of a small (but dedicated) working group consisting of privacy and consumer advocates as well as academics and government officials involved in privacy regulation. It has also been the subject of numerous class discussions at OntarioTech University. The views contained in this code do not necessarily reflect those of the OPC or specific working group members. Mistakes in the code are my own.

Rajen Akalu, Ph.D.

WORKING GROUP MEMBERS

Colin Bennet, Professor, University of Victoria

Philippa Lawson, Barrister & Solicitor, Consultant, Researcher/Writer

Eric Lawton I&T Division, Risk Management, Cyber Security & Compliance (RMCS&C)

Gregg Loane, Manager, ITS Capital Delivery, City of Toronto

Ian Jack, Canadian Automobile Association

Jason Kerr, Canadian Automobile Association

Brenda McPhail, Director, Privacy, Technology & Surveillance Project at the Canadian Civil Liberties Association

Sharon Polsky, President of the Privacy and Access Council of Canada

Murad Wancho, Research Assistant, University of Ontario Institute of Technology

CONTENTS

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 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 Colombia. 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.

[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[1]. In order to align itself with the legislation, the Code is limited to that of the commercial activity 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.[2] 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.

[1] *Personal Information Protection and Electronic Documents Act* (s.c. 2000, c.5)
[2] Ibid.

[3] This Code focuses on personal information, which can be described as any type 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.[3]

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.[4] 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.

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

[3] Jacobson, L. (2007). Vehicle Infrastructure Integration Privacy Policies Framework: The Institutional Issues Subcommittee of the National VII Coalition, 1-32.

[4] It should be noted that usage based insurance is governed provincially by the Financial Services Commission See FSCO Usage-Based Automobile Insurance Pricing in Ontario, Bulletin No. A-05/13 See https://www.fsco.gov.on.ca/en/auto/autobulletins/2013/Pages/a-05-13.aspx

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.[5] 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 vehicle The behavior of drivers can be monitor 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 in first look, seems not so harmful.[6] This type 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.[7] 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

[5] U. Shafi, A. Safi, A. R. Shahid, S. Ziauddin, and M. Q. Saleem, "Vehicle Remote Health Monitoring and Prognostic Maintenance System," Journal of Advanced Transportation, vol. 2018

[6] Kaplun, V. & Segal, M. Telecommunications Systems 2019.

[7] M. Swan, "Connected car: quantified self becomes quantified car," *Journal of Sensor and Actuator Networks*, vol. 4, pp. 2-29, 2015

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

[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.[8] The privacy commissioner of Alberta has argued that Information about an object is personal information.[9] Lastly, it has been argued that information which is identifiable and is being used for a purpose relating to that individual, is personal information.[10]

[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.

[8] *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner*) 2011 ABCA 94 (CanLII)
[9] Alberta IPC in *Order F2012-14*
[10] Schindler Elevator Order P12-01 2012 BCIPC No. 25.

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 in which allows for the flow of information with other vehicles through VANETs.

Vehicle to Infrastructure (V2I): a communication system in 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 of 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 use of these systems are 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

Vehicle dealers 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 are 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.[11]

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

[11] Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (1996).

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[12] companies should Obtain explicit consent for collections, uses or disclosures 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

[12] Office of the Privacy Commissioner of Canada, Guidelines on obtaining meaningful consent https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ May 2018.

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 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

Being 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 firstly rental agencies should verify if data and 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 the 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.