Developing a Code of Practice for the Connected Car

IT.CAN 21st Annual Conference

October 23, 2017

Abstract

Although notice and consent can be used in the context of connected vehicles, it is of limited application as a mechanism for protecting privacy. Presenting drivers with notional 'control' over their personal information as contemplated in the privacy legislation is problematic for a number of reasons. Firstly, the marketplace for connected vehicles is evolving rapidly and many market participants play multiple and often overlapping roles. Secondly, warnings, choices and interruptions regarding privacy are more likely to be confusing rather than helpful to drivers. And thirdly, people systematically under-estimate the long-term privacy risks associated with the sharing of personal information. 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 in this area though not an 'optimal' solution can at least serve as a learning process by which privacy concerns in a complex information environment may be addressed in a holistic way.

Introduction

In a recent discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act[1] (PIPEDA) the Office of the Privacy Commissioner of Canada (OPC) examined alternatives to the consent model as currently formulated. The discussion was 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."[2] 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"[3] of the Act. The OPC remarks in its paper that "[w]e have not yet fully explored this provision."[4]

While privacy codes of practice have been used both in Canada and internationally, there is little consensus regarding the meaning of this term. This paper examines the role a code of practice might play in the context of PIPEDA and connected car. It does so by first clarifying the meaning of codes of practice in relation to PIPEDA. The paper then outlines the key features of vehicular ad hoc networks (VANETS). VANETS are central to the deployment of connected vehicles and present significant challenges to the current regulatory framework for privacy protection. The final part of the paper discusses current efforts to develop a code of practice for connected vehicles in Canada.

Part 1 PIPEDA and Codes of Practice

PIPEDA regulates the collection, use, and disclosure of personal information within the course of commercial activity.[5] The Act has been described as a "compromise in both substance and form" since its aim is to protect individual privacy but also recognize the commercial need of businesses to collect personal data.[6] The Act states that "personal information" means

---

[1] S.C. 2000, c. 5.

[2] Office of the Privacy Commissioner of Canada (2016). "Consent and Privacy" https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

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

[4] See n. 2.

[5] S 4(1) provides that PIPEDA applies to every organization in respect of personal information that the organization "collects, uses or discloses in the course of commercial activities" or "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."

[6] Englander v. Telus 2004 FCA 387.

"information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[7]

If PIPEDA is applicable to the organization then s. 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 "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[8] The requirement that information practices be reasonable has become a de facto balancing test employed by the OPC to determine whether there has been implied consent.[9] However given the current administrative structure of PIPEDA which is based upon an informal dispute resolution model, OPC interpretations of reasonableness cannot be relied on as precedent.

PIPEDA is premised on the notion that individuals control information about themselves and can choose to disclose their information. Once disclosed, consent is required to use the personal information in ways not originally intended i.e. for secondary purposes. The approach is viewed as empowering individuals by fostering mechanisms, both legal and technical that enhance individual control of data. Individuals are said to 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 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.[10] Proponents of this approach to privacy protection argue that "removing consent from the equation risks undermining fundamental individual rights, protections and freedoms."[11] This approach, also referred to as informational self-determination has been the subject of criticism by privacy scholars. Empirical findings in behaviour 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.[12] While companies attempt to convey their data

[7] s. 2(1) PIPEDA.

[8] s. 5(3) PIPEDA.

[9] Austin, L. (2003). "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices"." Canadian Business Law Journal **44**: 21.

[10] Solove, D. J. (2013). "Privacy self-management and the consent dilemma." Harvard Law Review **126**.

[11] Cavoukian, A. and K. El Emam (2014). "The unintended consequences of privacy paternalism." Information and Privacy Commissioner Ontario Canada **5**.

[12] Acquisti, A., et al. (2013). "Gone in 15 seconds: The limits of privacy transparency and control." IEEE Security & Privacy(4): 72-74.

handling practices there is considerable evidence to support the view that "corporate privacy policies obfuscate, enhance and mitigate unethical data handling practices and use persuasive appeals to increase companies' trustworthiness."[13]

1.2 Codes of Practice

For the most part corporate privacy statements are drafted for the benefit of the organization rather that the consumer. This defensive approach to privacy protection is understandable given that companies are required to 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 copious detail knowing that these documents are unlikely to ever be read.

To constitute personal information data must be attributable 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.[14] It does not matter who "owns" the information or whether the information was generated by the company. The courts have held that personal information means *any* information about a specific person, subject only to specific exceptions.[15] 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.[16] Whether there or not there is a 'serious possibility' that an individual could be identified with information alone or in combination with other information is an open question. The emphasis on individual control of personal data and personal information as the threshold for the application of all of the obligations set out in PIPEDA creates conditions for lack of transparency for consumers and uncertainty for businesses. Nowhere is this more prevalent than in corporate privacy policies.

Unlike privacy policies, codes of practice apply to more than one organization. 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. Codes of practice can also afford greater clarity for individuals information is being processed and whether this is being done in a manner that is transparent and fair manner in line with their expectations.

---

[13] Pollach, I. (2007). "What's wrong with online privacy policies?" Communications of the ACM **50**(9): 103-108.

[14] Scassa, T., et al. (2011). "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems." Sask. L. Rev. **74**: 117.

[15] Dagg v. Canada (Minister of Finance) [1997] 2 SCR 403.

[16] Gordon v. Canada (Health), 2008 FC 258.

Bennett and Raab distinguish privacy codes of practice based on their scope and application: organizational, sectoral, functional, technological and professional.[17] Private and typically large multi-national organizations have developed privacy codes of practice in order to apply the same data handling processes by any of the company's entities. Codes of practice have developed at the sectoral level such as healthcare, insurance telecommunications etc. However, as discussed below, where the connected vehicle sector begins and ends is difficult to determine. Where codes of practice cut across traditional sectors and activities, they may be better described in functional terms. Mobile marketing for example is broadly defined as including advertising, apps, messaging, mCommerce and CRM on all mobile devices including smart phones and tablets. The mobile marketers association states that "[C]urrent internet marketing and privacy standards do not adequately address the specific challenges faced by marketers when marketing through the mobile channel. Strong mobile industry privacy principles will protect the mobile channel from abuses by unethical marketers, and limit consumer backlash and additional regulatory scrutiny."[18] Codes can also apply to specific technologies such as the use of Radio Frequency Identification Devices (RFID).[19] A final category of codes relates to professionals that are heavily involved with information processing activities. These range from computer professionals[20], to librarians[21] and health professionals.[22] Enforcement of these codes will often take the form of disciplinary action at an individual level.

Part 2 Connected cars and vehicular ad hoc networks (VANETs)

Government initiatives for the Intelligent Transport System (ITS) rely on the successful deployment of Vehicular ad hoc networks (VANETs) The ITS utilizes advanced information processing (computers), communications, sensor and control technologies and management strategies in an integrated manner in order to improve the functioning of the transportation system.[23]

---

[17] Bennett, C. J. and C. D. Raab (2006). The governance of privacy: Policy instruments in global perspective.

[18] See http://www.mmaglobal.com/policies/code-of-conduct

[19] OECD (2008) OECD Policy Guidance on Radio Frequency Identification available at http://tinyurl.com/y95s27yr

[20] See ACM Code of Ethics and Professional Conduct, http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

[21] See IFLA Code of Ethics for Librarians and other Information Workers, https://www.ifla.org/publications/node/11092

[22] College of Physicians and Surgeons of Ontario (the CPSO) Privacy Code, http://www.cpso.on.ca/About-Us/Privacy-Code

[23] See Transport Canada Canada, "An Intelligent Transportation Systems (ITS) Plan for Canada: En Route to Intelligent Mobility" (November 1999) Available at http://www.irfnet.ch/files-upload/knowledges/Canda_its_plan.pdf.

Modern vehicles are equipped with communication systems that are integrated with the ITS infrastructure and constitute critical sources of consumer data. Infotainment systems in these vehicles log information relating to the driver's behaviour, location, contacts, and intended destinations. Such information has the potential to be used to analyze driving patterns for user profiles and is of particular interest in vehicular forensics.[24] Telematics data can be used to reconstruct accidents and determine their cause or used by law enforcement to predict a suspect's behaviour.[25] Scassa et al. argue that "while ITS may offer significant benefits for safety, security, and environmental sustainability, it also raises considerable informational privacy risks."[26]

Central to the deployment of the ITS are vehicular ad hoc networks (VANETs). VANETs are a general class of mobile ad hoc networks that enable wireless communication between vehicles or with fixed equipment. The network facilitates both vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication and as such VANETs are used for a range of safety applications such as collision warnings and roadside assistance as well as non-safety applications such as navigation and infotainment. A VANET consists of (1) on board units (OBUs) built into vehicles and (2) roadside units (RSUs) deployed along highways and sidewalks.[27]

There are a wide range of applications for VANETs. Infotainment applications for example offer convenience and comfort to drivers and passengers by providing on-demand location based services such as travel information and traffic conditions, distance learning and media streaming. Road safety applications have focused on reducing the number of accidents by communicating traffic conditions, to drivers. There are also traffic monitoring and management applications which have focused on maximizing road capacity and minimizing traffic congestion via intersection management. Vehicle platooning is one such application which allows vehicles to travel closely together eliminating the stop-and-go traffic behaviour.[28]

---

[24] Kopylova, Y., et al. (2011). Accurate accident reconstruction in VANET. Data and Applications Security and Privacy XXV, Springer**:** 271-279.

[25] See M. Wall "Is your car spying on you" http://www.bbc.com/news/business-29566764 November 4, 2014.

[26] Scassa, T., et al. (2011). "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems." Sask. L. Rev. **74**: 117.

[27] Cheng, H. T., et al. (2011). "Infotainment and road safety service support in vehicular networking: From a communication perspective." Mechanical Systems and Signal Processing **25**(6): 2020-2038.

[28] Fernandes, P. and U. Nunes (2012). "Platooning with IVC-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow." IEEE Transactions on Intelligent Transportation Systems **13**(1): 91-106.

Part 3 Privacy codes of practice and the connected car

It is important to observe that VANETs are not controlled by a single sector such as the automotive manufacturing sector. Automakers operate in highly complex information environment that covers multiple and often intersecting, relationships. It is similarly important to note that for the vehicles to communicate with each other and the infrastructure, vehicles in VANETs broadcast unencrypted messages that contain a vehicle identifier together with the vehicle's location, speed and direction. 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.

Location privacy has been held to be personal information about an identifiable individual within the meaning of PIPEDA. Determining whether a company is dealing with identifiable and therefore personal information and whether the information is anonymous and therefore non-personal information that is not caught by the Act is the source of considerable uncertainty for parties dealing with VANET data. Suppliers of connected vehicle services typically state that they cannot supply the services customers want without accessing vehicle information, including location information. 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. By relying the notion that individuals control their data, a privacy statement can be presented to the consumer that will explicitly set out the organization's data handling practices, but that the customer is in no position to comprehend. Automakers for example tend to be of the view that it is necessary to share personal information with service providers, that this is explained this in the privacy statement which customers agree to.[29] However previous law and policy research has demonstrated a widespread disrespect for the privacy of customers by companies offering connected car services.[30]

To remedy this problem sector specific legislation has been called for to protect personal information. However this approach is likely to place limitations on valuable business uses of data that may not in fact violate privacy. The development a privacy code of practice for the connected vehicles has the potential to draw attention to inappropriate data handling practices that may otherwise go unnoticed and assist individuals in understanding the data they are entitled to control. This approach would place boundaries on the sharing of location data by third parties, as well as provide softer default rules on the use of non-personally identifiable information. This would in turn make it easier for individuals to appreciate how their privacy is being protected. It

[29] Akalu, R. (2016). Paving the way for Intelligent Transport Systems (ITS): The Privacy Implications of Vehicular Infotainment Platforms.", University of Ontario Institute of Technology and Office of the Privacy Commissioner of Canada.

[30] Lawson, P. (2015). The Connected Car: Who is in the Driver's Seat? British Columbia, BC Freedom of Information and Privacy Association.

would also enable individuals to demand services to be provided in more minimally intrusive ways.

There are number of limitations inherent to the use of codes of practice. A central concern whether privacy protection will be enhanced by a code. 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"[31]

Second there is the issue 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.

3. 2 Developing a code of practice for the connected car

The issues raised above are particularly prevalent in the case of connected vehicles. The marketplace for connected vehicles consists of a wide range of stakeholders from car manufacturers to internet service providers and insurance agencies as well as government stakeholders. Defining the sector or technology to establish the scope and application of a code of practice therefore represents a significant challenge. An alternative approach would be to develop principles around data categories or elements in the provision of connected car services. This would enable customers to better understand the data involved and their rights. It would also provide predictability for companies in terms of understanding their obligations regarding consent as well as the appropriate limits on data processing.

Connected vehicle generate six different types of data. 1. Infotainment data is generated by the infotainment system (such as music selection or mobile applications) 2. Personal communications data is generated by messages sent or received via the vehicle infotainment system (this is often done through a synched smartphone. 3. Location data concerns data about a vehicle's location at any given time 4. Driver behaviour refers to when and how a driver operates the vehicle 5. Biometrics and health concerns data gathered by health monitoring devices in or linked to the vehicle and 6. Vehicle diagnostics is data generated by a vehicle's internal systems on the performance of vehicle components.

By developing principles around categories of data rather than organizations or industry sectors, consumers can better understand the type of data involved. This approach would also assist with stakeholder engagement as certain organizations and sector deal with some data categories but not others. Development of a privacy codes of practice is not an 'optimal' solution, but it should be noted that privacy solutions are always sub-optimal in the advent of technological change.

[31] ISED (2010). "Innovation Science and Economic Development - Codes Guide - Processes for Developing Effective Codes." Retrieved February 27, 2017, from https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00964.html#footnote2.

The development of code of practices can at least serve as a learning process by which privacy concerns in a complex information environment in may be addressed in a holistic way.

Conclusion

Exercising control via consent enables individual choice regarding the sharing of personal data. However an over reliance on individual consent regarding collection, use and disclosure of data does little to take into account the increasingly interdependent nature of privacy and the complex nature of information networks. This paper examined the role that a code of practice might play in the context of PIPEDA and connected car. Despite their limitations, codes of practice have the potential to take into account wider social values including privacy in the deployment of connected car technologies. Using privacy codes of practice can also promote transparency on how privacy obligations are being addressed in a manner beneficial to both organizations and individuals.

Acquisti, A., et al. (2013). "Gone in 15 seconds: The limits of privacy transparency and control." IEEE Security & Privacy(4): 72-74.

Akalu, R. (2016). Paving the way for Intelligent Transport Systems (ITS): The Privacy Implications of Vehicular Infotainment Platforms.", University of Ontario Institute of Technology and Office of the Privacy Commissioner of Canada.

Austin, L. (2003). "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices"." Canadian Business Law Journal **44**: 21.

Bennett, C. J. and C. D. Raab (2006). The governance of privacy: Policy instruments in global perspective.

Cavoukian, A. and K. El Emam (2014). "The unintended consequences of privacy paternalism." Information and Privacy Commissioner Ontario Canada **5**.

Cheng, H. T., et al. (2011). "Infotainment and road safety service support in vehicular networking: From a communication perspective." Mechanical Systems and Signal Processing **25**(6): 2020-2038.

Fernandes, P. and U. Nunes (2012). "Platooning with IVC-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow." IEEE Transactions on Intelligent Transportation Systems **13**(1): 91-106.

ISED (2010). "Innovation Science and Economic Development - Codes Guide - Processes for Developing Effective Codes." Retrieved February 27, 2017, from https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00964.html#footnote2.

Kopylova, Y., et al. (2011). Accurate accident reconstruction in VANET. Data and Applications Security and Privacy XXV, Springer**:** 271-279.

Lawson, P. (2015). The Connected Car: Who is in the Driver's Seat? British Columbia, BC Freedom of Information and Privacy Association.

Pollach, I. (2007). "What's wrong with online privacy policies?" Communications of the ACM **50**(9): 103-108.

Scassa, T., et al. (2011). "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems." Sask. L. Rev. **74**: 117.

Solove, D. J. (2013). "Privacy self-management and the consent dilemma." Harvard Law Review **126**.