A Code of Practice for Connected Vehicles

Discussion Paper

1. Introduction

Privacy protection typically addresses isolated transactions between individuals and organizations. This approach to privacy protection, which relies on individual consent regarding the collection, use, and disclosure of data, fails to take into account the increasingly interdependent nature of privacy and the complex nature of information networks. As a result, the over-reliance on consent as the mechanism by which consumer control access to their personal information has become increasingly untenable.

While prescriptive rules in the connected vehicle context would be easy to justify if the uses of data had little or no benefit or were otherwise harmful, there are many socially desirable uses of connected car vehicle data such as location-based services or vehicular diagnostics.

The aim of this discussion paper is to develop a privacy code of practice for the connected car in order 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.

The expectation is that a code of practice could provide an added measure of predictability and consistency for companies in terms of understanding their obligations around meaningful consent and appropriate limits on data processing as well as provide greater clarity for individuals regarding how their data is being processed.

By placing boundaries on the sharing of location data by third parties, for example, as well as softer default rules on the use of non-personally identifiable information would make it easier for individuals to appreciate how their privacy is being protected. It would also enable individuals to demand services to be provided in more minimally intrusive ways.

2. Background

Governments recognize that consumers have neither the time nor resources to compare different car safety features when making a purchasing decision. This being the case, detailed regulations are established in order to ensure that minimum standards of vehicle safety are being maintained.[1] These regulations cover all aspects of vehicle manufacture from the installation of seatbelts, to the size of tire rims. Vehicle safety standards are highly prescriptive such that automakers have limited discretion on how to interpret a given standard. This approach ensures that vehicles purchased by consumers are reasonably safe.

Decisions regarding the sharing of data by consumers, by contrast, are not prescribed. In data protection law, generally speaking, it is the individual that exercises control over their personal information. This approach to individual control over personal data plays an important role in limiting the collection, use, and disclosure of personal information in the highly influential OECD Fair Information Principles (FIPs).[2] The FIPs stipulate that the reasons for the collection, use and disclosure and retention of personally identifiable information should be determined at or before the time of collection. Personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as authorized by law. The FIPs also specifies that individuals should be enabled by organizations to play a participatory role in the lifecycle of their own personal data and should be made aware of the practices associated with its use and disclosure.[3] While the FIPs are a mainstay of data regulation, their specific implementation is subject to nuanced interpretation that is context-specific. Moreover, advances in technology have enabled the shifting of information between contexts and while scholarship in this area has typically focused on sensitive information as a primary concern, there has been a trend toward recognizing the relationship between information that is neither sensitive nor intimate but is culled from public spheres. [4]

Developments in information technology and business practice have meant that: "a) there is virtually no limit to the amount of information that can be recorded, b) there is virtually no limit to the scope of analysis that can be done – bounded only by human ingenuity, and c) the information can be stored virtually forever."[5] Thus careful attention must be paid to attempts to reconcile various business imperatives associated with personal data with individual rights associated with privacy.

---

[1] The Motor Vehicle Safety Act S.C. 1993, c. 16 and Regulations and Orders Pursuant to the Act regulates the manufacture and importation of motor vehicles and motor vehicle equipment to reduce the risk of death, injury and damage to property and the environment.

[2] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Annex to Recommendation of the Council (23 September 1980).

[3] The OECD guidelines refer to Openness Principle and Individual Participation Principle concerning practices and policies with respect to personal data.

[4] Helen Nissenbaum, "Protecting Privacy in the Information Age: The Problem of Privacy in Public", *Law and Phil.* 17 (1998) p. 559 at p. 585.

[5] *Ibid*. at p. 576

Questions for discussion

1. **What are the strengths of the present approach to privacy protection with respect to connected vehicles?**
2. **Do you think data protection in connected vehicles requires prescriptive rules in order to be effective?**

3. The Connected Car

In the case of the connected car, modern vehicles are equipped with telematics systems that make use of vehicular information about a vehicle's internal systems that are used for diagnostics and emergency situations in order to provide roadside assistance service, for example.[6] They are also equipped with infotainment systems that use non-vehicular information, providing drivers with convenient onboard functions when driving, such as hands-free calling, text messaging and internet capability etc. The connected car forms an integral part of the vehicular ad hoc network (VANET).

VANETs enable communication between vehicles, infrastructure networks, and pedestrians. The information generated by VANETs constitutes a critical source of consumer data which can be stored at low cost and subject to analytical techniques such as data mining.[7] Vehicles log information relating to the driver's behaviour, location, contacts, and intended destinations. 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. Thus while VANETs may offer significant benefits for safety, security, and sustainability, it also raises considerable informational privacy risks since the data being shared is potentially accessible to a wider set of adversaries.[8] Providers of connected car services have asserted that the automotive industry cannot supply the services customers want without accessing vehicle information, including location information.[9] The emphasis on vehicle safety on the part of automakers, while understandable, threatens to undermine privacy rather than protect it. This is because safety concerns will almost always be deemed reasonable when pitted against privacy concerns.

[6] Al-Sultan, S., et al. (2014). "A comprehensive survey on vehicular Ad Hoc network." Journal of network and computer applications **37**: 380-392.

[7] Hartenstein, H. and K. P. Laberteaux (2008). "A tutorial survey on vehicular ad hoc networks." Communications Magazine, IEEE **46**(6): 164-171.

[8] 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.

[9] Personal correspondence with GM.

However, this approach relies heavily on individual consent and this has a tendency to obscure rather than clarify the privacy issues at stake.

At present, car manufacturers and dealerships typically satisfy their privacy obligations to consumers by communicating information handling practices with users via user agreements, privacy statements, and software terms.[10] The data handling practices of a given service provider are usually provided to consumers in a corporate privacy statement. Whether the consent of the consumer is meaningful is an open question since the terms of these agreements are often obtuse and subject to change without notice. Given the fact that behavioural studies have consistently 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.[11]

Nevertheless, the organization would argue that it is compliant with its regulatory obligations because customer consent was obtained. Privacy statements in the connected vehicle industry provide a good example of overemphasis on individual consent providing inadequate privacy protection. Such practices raise concerns of whether privacy statements, rather than representing an organization's commitment to safeguarding customer data are in fact an ostensible effort to increase an organization's trustworthiness, obscuring, rather than promoting, transparency of its corporate data handling practices.[12]

Questions for discussion

1. **Is obtaining individual consent sufficient in the context of connected vehicle services?**
2. **Do you agree that privacy statements are obscure rather than promote transparency of corporate data handling practices?**

4. The over-reliance on consent in policy and practice

The focus on the individual consent model is attractive for policy-makers and automakers because it has the effect of glossing over conceptual ambiguities that are latent in definitions of privacy they do not wish to grapple with. Instead, 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

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

[11] Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce, ACM.

[12] Pollach, I. (2011). "Online privacy as a corporate social responsibility: an empirical study." Business Ethics: A European Review **20**(1): 88-102.

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.[13]

As a general rule for data protection law to apply, the data must be linked to an identifiable individual. This is problematic for a number of reasons. Firstly, as Austin notes, the fair information practices (FIPs) represent an all-or-nothing model where FIPs apply in relation to the collection, use, and disclosure of personal information but not otherwise.[14] To constitute personal information, data must be attributable to an identifiable individual.[15] However, the information need not be collected directly by the company for it to be 'about' an identifiable individual. If a company keeps a record of a vehicle identification number and registered owner, the information will be deemed to be personal information.[16] 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.[17] Moreover, 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.[18] Whether there is or there is not a 'serious possibility' that an individual could be identified with information alone or in combination with other information is an open question that lies at the heart of any discussion of personal information in the context of VANETS.

Personal information includes information that is directly linked to an identifiable individual (e.g. driver's license, license plates, and registration, name and address etc.). It can also include information that when combined can lead to an identifiable individual. GPS data gathered during a workday has been held to constitute the personal information of employees. Video imaging may constitute personal information to the extent license plate and image can result in the identification of an individual. However, in most cases, it will not be possible to determine who was driving a vehicle at a particular moment in time thus not satisfying the requirement of being personal information warranting regulatory protection. However, this belies the reality that individuals will drive in the same vehicle most of the time and therefore considerable privacy harms can result from the inferences that can be made from knowing a vehicle's identity. Thus, while location privacy may be protected, it can only be deemed personal information if it can be attributed to an identifiable individual.

---

[13] Solove, D. J. (2012). "Privacy self-management and the consent dilemma."

[14] Austin, L. M. (2014). "Enough About Me: Why Privacy is About Power, Not Consent (or Harm)." Forthcoming in Austin Sarat, ed., A World Without Privacy.

[15] McIsaac, B., et al. (2004). The law of privacy in Canada, Scarborough [Toronto], Ont.: Carswell.

[16] 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.

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

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

Questions for discussion

1. **Is there an over-reliance on consent in privacy policy and practice?**
2. **Are the inferences that may be made from knowing a vehicle's identity sufficient to warrant privacy protection?**

4. Personal information and the connected car

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 data protection law is the source of considerable uncertainty for parties dealing with VANET data. Moreover, it has been noted that automakers operate in a highly complex information environment that covers multiple, often intersecting, relationships.[19] The focus on individual consent to data sharing coupled with the benefits of the connected cars in terms of safety will consistently outweigh the potential privacy concerns. The narrow focus on protecting personal information, together with the reliance on individual consent to the sharing of data leaves a range of privacy concerns concerning VANETs unaddressed. The social connectivity of cars, for example, will enable interactions among vehicles, among drivers and between infrastructures and drivers/vehicles/pedestrians. This makes privacy dependent on other people since information about a user can be revealed by the user's friends or family.

Considerably more personal behaviour can be derived from the type of car a person drives than the phone they use, since cars in many countries are status symbols indicating an individual's wealth, income level etc. Cars are personal devices that are usually kept for a long time and they are increasingly storing considerable amounts of personal information that can be used alone or with other data in order to reveal the identity of an individual driver. Dötzer warns that "[a] very dangerous and often ignored fact about privacy is that innocent looking data from various sources can be accumulated over a long period of time and evaluated automatically."[20]

The fact that vehicles are increasingly connecting with each other and with public networks (e.g. V2V, V2I) make it inevitable that nodes will exchange neighbourhood information on a regular basis. Since VANETs enable interactions among vehicles, among drivers and between infrastructures and drivers/vehicles/pedestrians, privacy protection is also dependent on other people since information about a user can be revealed by the user's contacts or driving patterns.[21] The fact that tracking vehicles can reveal sensitive locations, such as home, office and places frequently visited needs to be reconciled with the fact that location privacy of connected cars can often conflict with authentication requirements since safety critical information needs to be sent by a trusted source. The fact that driver profiles may be developed that can be used for

[19] Ibid n. 10.
[20] Dötzer, F. (2005). Privacy issues in vehicular ad hoc networks. Privacy enhancing technologies, Springer.

[21] Ibid n. 29.

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 would also need to be addressed. Consent in such circumstances will not provide meaningful privacy protection as there are powerful countervailing interests militating against it.

Thus, the focus on individual consent obscures the difficult substantive decisions that need to be made about the merits of certain forms of data collection use and disclosure. This is crucial if technical solutions are to be developed in this area.

Questions for Discussion

1. **Does the focus on individual consent to data sharing coupled with the benefits of the connected cars in terms of safety outweigh the potential privacy concerns in public discussions of these issues?**
2. **Are there privacy concerns concerning connected vehicles are currently going unaddressed?**
3. **Are there certain forms of data collection use and disclosure with respect to connected vehicles that you think should be prohibited?**

5. Developing and Implementing a Privacy Code of Practice for the Connected Car

Individual control and personally identifiable information will continue to play an important role in privacy protection. Exercising control via consent enables individual choice regarding the sharing of personal data. Similarly, personally identifiable information establishes the boundaries of privacy regulation and without it, there would be no limit on the scope of privacy law.[22] However, while necessary, individual control and personal identifiable information are an insufficient form of privacy protection in VANETs. This is due in large part to the fact that this approach to privacy protection addresses isolated transactions between individuals and organizations. A reliance on individual consent regarding the collection, use, and disclosure of data fails to take into account the increasingly interdependent nature of privacy and the complex nature of information networks. The wider social values including privacy will, therefore, need to be assessed holistically.

While prescriptive rules would be easy to justify if the uses of data had little or no benefit or were otherwise harmful, there are many socially desirable uses of VANET data so it is important to be mindful of the economic costs associated with imposing data protection rules. If we are to develop a position on what constitutes reasonable purposes with respect to the collection, use, and disclosure of VANET data, the development and codification of basic privacy norms in the form of a code of practices would be a good place to start.

[22] Schwartz, P. M. and D. J. Solove (2011). "Pii problem: Privacy and a new concept of personally identifiable information, the." NYUL Rev. **86**: 1814.

Questions for discussion

1. **What are the merits of voluntary industry guidelines such a code of practice versus a regulatory approach?**
2. **In what ways could a code of practice provide enhanced privacy standards tailored to connected cars?**
3. **What would be the scope and objectives of a code of practice?**
4. **How should such a code be implemented?**
5. **What are the economic costs associated with implementing a code of practice?**