Privacy, consent and vehicular ad hoc networks (VANETs)

Rajen Akalu*

University of Ontario Institute of Technology, Oshawa, Ontario, Canada

Abstract

The consent model of privacy protection assumes that individuals control their personal information and are able to assess the risks associated with data sharing. The model is attractive for policy-makers and automakers because it has the effect of glossing over the conceptual ambiguities that are latent in definitions of privacy. Instead of formulating a substantive and normative position on what constitutes a reasonable expectation of privacy in the circumstance, individuals are said to have control over their data. Organizations have obligations to respect rights to notice, access and consent regarding the collection, use and disclosure of personal data once that data has been shared. The policy goal becomes how to provide individuals with control over their personal data in the consent model of privacy protection. This paper argues that the privacy issues raised by vehicular ad hoc networks make this approach increasingly untenable. It is argued that substantive rules that establish a basic set of privacy norms regarding the collection, use and disclosure of data are necessary. This can be realized in part via a privacy code of practice for the connected vehicle. This paper first explores the relationship between privacy, consent and personal information in relation to the connected car. This is followed by a description of vehicular ad hoc networks and a survey of the technical proposals aimed at securing data. The privacy issues that will likely remain unsolved by enhancing individual consent are then discussed. The last section provides some direction on how a code of practice can assist in determining when individual consent will need to be enhanced and when alternatives to consent will need to be implemented.

© 2017 Rajen Akalu. Published by Elsevier Ltd. All rights reserved.

Keywords:
Privacy
Vehicular networks
Law and policy

1. Introduction

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, the government establishes detailed regulations in order to ensure that minimum safety standards are being maintained. 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.

* University of Ontario Institute of Technology, Faculty of Business and Information Technology, 2000 Simcoe St. N., Oshawa, ON L1H 7K4, Canada.
E-mail address: rajen.akalu@uoit.ca.

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. http://dx.doi.org/10.1016/j.clsr.2017.06.006
By contrast, decisions regarding the sharing of data by consumers are not prescribed in the same manner. As a general rule, in data protection law it is the individual that exercises control over their personal information. The approach of individual control over personal data places limitations on limiting the collection, use, and disclosure of personal information. They are a central tenet of the highly influential OECD Fair Information Principles (FIPs). The FIPs stipulate that the reasons for the collection, use, 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 specify that individuals should be enabled by organizations to play a participatory role in the lifecycle of their personal data and should be made aware of the practices associated with its use and disclosure. 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 rather culled from public spheres.

This trend has been accelerated by developments in information technology and business practice which 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. Given this trend of data retention of personal information and the commercial imperative for business analytics, careful attention must be paid to attempts to reconcile various business interests associated with personal data with individual rights with respect to privacy.

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 as well as enable roadside assistance. Modern vehicles also equipped with infotainment systems that use non-vehicular information, providing drivers convenient onboard functions when driving such as hands-free calling, text messaging and Internet capability. The connected car forms an integral part of the vehicular ad hoc network (VANET). VANET’s 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. Vehicles log information relating to the driver’s behaviour, location, contacts, and intended destinations. With 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, they also raise considerable informational privacy risks since the data being shared is potentially accessible to a wider set of malicious users. Providers of connected car services have asserted that the automotive industry cannot supply the services customers want without accessing vehicle information, including location information. 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. However, this approach relies heavily on individual consent which has a tendency to obscure rather than clarify the privacy issues at stake.

At present car manufacturers and dealerships satisfy their privacy obligations to consumers by communicating information handling practices with users via user agreements, privacy statement and software terms. The data handling practices of a given service provider are usually set out in copious detail to which customers consent. Whether the consent of the consumer is meaningful given the fact that numerous behavioural studies on privacy 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 is an open question. Nevertheless, the organization would argue that it is compliant with its regulatory obligations because customer consent has been obtained. Privacy statements in the connected vehicle industry are illustrative of the overemphasis on individual consent providing inadequate and illusionary 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.


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


5 Ibid. at p. 576.

دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات