COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy, consent and vehicular ad hoc networks (VANETs)

Rajen Akalu *

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

Keywords:
Privacy
Vehicular networks
Law and policy

A B S T R A C T

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.

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.[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.

* 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
0267-3649/

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 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).[2] 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.[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 rather culled from public spheres.[4]

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."[5] 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.[6] 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). 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. 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.[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. 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.[10] 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.[11] 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.[12]

---

[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.

[6] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. and Zedan, H. 2014. A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications*, 37, 380–392.

[7] Hartenstein, H. and Laberteaux, K. P. 2008. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine,* 46, 164–171.

[8] Scassa, T., Chandler, J. A. and Judge, E. F. 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.

[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. Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce, 2004. ACM, 21–29.

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

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

The focus on individual consent as a model for privacy protection 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 of formulating a substantive and normative position on what constitutes a reasonable expectation of privacy in the circumstances, 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. 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. Individuals, not organizations, decide how to evaluate the benefits and costs of collection, use and or disclosure of their information and act accordingly.[13]

This paper argues that the privacy issues raised by VANETs are unlikely to be solved in this way. 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. The next section explores the relationship between privacy, consent and personal information in relation to the connected car. This is followed by a description of VANETs and a survey of the technical proposals aimed at protecting privacy. 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.

2. Protecting personal information with individual consent

The notion that individuals control their personal data and can assess for themselves the risks associated with collection, use and disclosure of their information is deeply rooted in current policy approaches to privacy protection. We observe this at the conceptual level with Westin's influential formulation of privacy as "the claim of individuals and groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[14] Similarly, Fried saw privacy as "control we have over information about ourselves".[15] These individual-centric and control-based conceptions of privacy emphasize personal autonomy regarding the sharing of personal data. They also exemplify a distinction between public and private information implying that individuals control information about themselves and could choose to disclose their information.[16] Once disclosed, consent would be required to use the personal information in ways not originally intended, i.e. for secondary purposes. Privacy regimes based on individual control are attractive because they provide a sense of individual empowerment. Such an approach to privacy protection conveys a sense of neutrality about the data being collected, used, and disclosed and universality regarding the context in which this takes place. Austin notes that while such regimes are important for legal policy, they avoid many of the definitional difficulties surrounding the idea of privacy.[17]

Without addressing the substantive and normative questions concerning the need to protect privacy, policy makers can assert that greater privacy protection can be realized if measures that strengthen consent and individual control over personal data are introduced. It follows that organizations should provide greater transparency regarding their data handling practices and enhance individual control of personal data.[18]

However this approach to privacy protection has also been challenged in light of the vast, complex nature of information flows in modern computing environments. It has for example been argued that:

> *Our digital information society depends and thrives on the ability to generate, collect, aggregate, link and use information, including personal data, through increasingly complex technologies and global processes. Understanding how our personal information is being used in this environment is becoming increasingly difficult if not impossible for the average person. Thus, expecting individuals to take an active role in deciding how their personal information is used in all instances is increasingly unrealistic.*[19]

In addition to the complexity associated with data collection and processing, it should be recognized that there are many instances where the consent of the individual can be overridden by competing interests such as business interests, law enforcement or threats to the life, health and security of an individual. As a result, whether a privacy violation has occurred or not depends on whether a reasonable person would consider collection use and disclosure of personal data appropriate in the circumstances. Austin argues however that if consent provides the central protection of privacy then reasonable purposes become too easily the site for the consideration of countervailing values such as business interests. What is needed she argues "is a nuanced and normative approach to privacy that is then incorporated into a test for 'reasonable purposes'".[20] Developing a test for reasonable purposes implies that we must make substantive decisions about the merits of certain forms of collection, use and disclosure

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

[14] Westin, A. F. 1967. Privacy and Freedom, Atheneum. New York, 7.

[15] Fried, C. 1984. Privacy: A Moral Analysis. Philosophical Dimensions of Privacy: An Anthology. Schoeman, FD Editor. Cambridge University Press, Cambridge.

[16] Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life*, Stanford University Press.

[17] Austin, L. M. 2006. Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA. *University of Toronto Law Journal,* 56, 181–215.

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

[19] Center for Policy Leadership. "The role of enhanced accountability in creating a sustainable data-driven economy and society. https://www.informationpolicycentre.com/.

[20] Ibid., n. 17 at p. 183.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

of data. In the context of connected vehicles there are a host of countervailing values ranging from law enforcement and safety to commercial value and consumer convenience. If our acceptance of automakers' data handling practices turns entirely on whether or not consent has been obtained, this is likely to undermine privacy rather than protect it.

As a general rule for data protection law to apply the data must be attributed to an identifiable individual. The requirement of an identifiable individual 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.[21] To constitute personal information the data must be attributable to an identifiable individual.[22] 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.[23] 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.[24] 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.[25] 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 that lies at the heart of any discussion of personal information in the context of connected vehicles.

2.1. *Personal information and the connected car*

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.[26] Video imaging may constitute personal information to the extent licence 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.

The emphasis on making privacy protection contingent on personal information is problematic in the connected vehicle context because it is the case that individuals drive in the same vehicle most of the time. As Cottrill argues:

> *[a]lthough various countries have taken a number of approaches to address the question of general privacy protection, little has been done from a policy standpoint to address the specific question of private information in a mobile environment.*[27]

Considerable privacy harms can result from the inferences that can be made from knowing a vehicle's identity and while location privacy may be protected, it can only be deemed personal information if it can be attributed to an identifiable individual. 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 connected data. Moreover, it has been noted that automakers operate in a highly complex information environment that covers multiple, often intersecting, relationships.[28] The benefits of connected cars regarding safety will consistently outweigh the potential privacy concerns if our focus is on individual consent regarding the sharing of personal information. Having said this privacy protection is seen as a key enabler of the willingness of consumers to share personal information. This being the case there have been numerous technical proposals aimed at protecting privacy. The next section provides description of vehicular ad hoc network (VANET) architecture and a survey of the technical proposals aimed at protecting privacy in this context.

3. Vehicular ad hoc networks

Vehicular ad hoc networks (VANETs) are a general class of mobile ad hoc networks that enable wireless communication between vehicles or with fixed equipment.[29] Specifically, a VANET consists of (1) onboard units (OBUs) built into vehicles and (2) roadside units (RSUs) deployed along highways and sidewalks.[30] 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

[21] 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*.

[22] McIsaac, B., Shields, R. and Klein, K. 2004. *The law of privacy in Canada*, Scarborough [Toronto], Ont.: Carswell.

[23] Scassa, T., Chandler, J. A. and Judge, E. F. 2011. Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems. *Sask. L. Rev.*, 74, 117.

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

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

[26] PIPEDA Case Summary #2006-351. Use of personal information collected by Global Positioning System considered available online. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-351/ [accessed March 13, 2017].

[27] Cottrill, C. 2009. Approaches to privacy preservation in intelligent transportation systems and vehicle-infrastructure integration initiative. *Transportation Research Record: Journal of the Transportation Research Board*, 9–15 at p. 11.

[28] Ibid., n. 10.

[29] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. and Zedan, H. 2014. A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications*, 37, 380–392.

[30] Cheng, H. T., Shan, H. and Zhuang, W. 2011. Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mechanical Systems and Signal Processing*, 25, 2020–2038.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

such as navigation and infotainment.[31] Cheng et al. divide potential applications in a vehicular environment into three main categories, namely (1) infotainment delivery, (2) road safety and (3) traffic monitoring and management.[32]

Infotainment applications 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.[33] Road safety applications have focused on reducing the number of accidents by communicating traffic conditions to drivers. Traffic monitoring and management applications have focused on maximizing road capacity and minimizing traffic congestion via intersection management.[34] An example of this application is vehicle platooning which allows vehicles to travel closely together eliminating the stop-and-go traffic behaviour as well as reducing crash instances that are the result of driver error. Platooning is expected to contribute to higher energy efficiency by dynamically adjusting vehicle speed and reducing aerodynamic drag.[35]

The distributed and heterogeneous nature of VANETs makes security a significant technical challenge.[36] 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.[37] VANETs enable cars to become context aware. This implies that a vehicle is cognizant of its environment (including the activity and location of other vehicles).[38] In order for such a network to operate, it is necessary for vehicles to exchange information with each other on a regular basis. This creates numerous data breach points for personal information making the need for privacy protection more acute.[39]

3.1. *Vehicular communications*

There are two main categories of vehicular communications that create context awareness. The first consists of connected vehicle safety systems that use dedicated short range communications (DSRC). The second consists of connected vehicle mobility applications that make use of cellular wireless to communicate vehicle status to navigation and other non-safety related data such as infotainment.[40] DSRC enables highly secure, high speed wireless communication between vehicles and infrastructures. A key feature of DSRC is its low latency, which refers to the short time lag between transmission and acquisition of data, essential for active crash avoidance and vehicle sensing. For safety communications, DSRC transceivers are embedded in the electrical systems of modern cars and standardized for interoperability among all makes and models. Vehicles are constantly communicating basic safety messages to each other. This information consists of a given vehicle's status (speed, position, heading etc.). To protect privacy safety communications do not identify any particular vehicle as the source of communication. The unique identifier of the DSRC device (its MAC address) is change every three minutes in order to prevent the transceiver from being used as a tracking device.

In contrast to vehicle communications that serve the narrow purpose of safety and are standardized, consumer-oriented vehicle communications are highly diverse. Smartphone platforms offered by Apple and Google enable a plethora of phone functions that appear on the vehicle's display screen making use of the vehicles' controls. Vehicle manufacturers also install proprietary vehicular infotainment platforms that enable infotainment services. As the Internet of Things increasingly includes vehicles, the use of wireless connections to transmit vehicular data such as braking, transmission and tire pressure to manufacturers is also set to increase. Security risks are greater in this category of vehicle communication due to the sheer volume of data and inability to identify the source of communication.[41]

3.2. *Technical proposals for securing data*

In response to the need for privacy protection in connected vehicles there have been a number of technological approaches aimed at securing data collection.[42] The approach of Hoh et al. aims at protecting privacy by "separating the communication and authentication tasks (which rely on pseudonyms or identities) from data analysis and sanitation (which require access to detailed position information)".[43] The separation of communication from authentication privacy

[31] Huang, C.-J., Chen, Y.-J., Chen, I.-F. and Wu, T.-H. 2009. An intelligent infotainment dissemination scheme for heterogeneous vehicular networks. *Expert Systems with Applications,* 36, 12472–12479.

[32] Ibid.

[33] Gehlen, G. and Pham, L. Mobile web services for peer-to-peer applications. Second IEEE Consumer Communications and Networking Conference, 2005. CCNC. 2005, 2005. IEEE, 427–433.

[34] Jayapal, C. and Roy, S. S. Road traffic congestion management using VANET. 2016 International Conference on Advances in Human Machine Interaction (HMI), 2016. IEEE, 1–7.

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

[36] Panghal, A. K. and Rani, S. 2015. Vehicular Ad-hoc Network (VANET)-Privacy and Security. *International Journal of Advanced Research in Computer Science,* 6.

[37] Maglaras, L. A., Al-Bayatti, A. H., He, Y., Wagner, I. and Janicke, H. 2016. Social Internet of Vehicles for Smart Cities. *Journal of Sensor and Actuator Networks,* 5, 3.

[38] Hubaux, J.-P., Capkun, S. and Luo, J. 2004. The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine,* 2, 49–55.

[39] Glancy, D. J. 2012. Privacy in autonomous vehicles. *Santa Clara L. Rev.,* 52, 1171.

[40] Hill, C. Module 13 Connected Vehicles: Purposes and objectives (2013). Available at http://www.pcb.its.dot.gov/eprimer/documents/module13.pdf.

[41] Glancy, D. J. 2013. Sharing the Road: Smart Transportation Infrastructure. *Fordham Urb. LJ,* 41, 1617.

[42] Cottrill, C. 2009. Approaches to privacy preservation in intelligent transportation systems and vehicle-infrastructure integration initiative. *Transportation Research Record: Journal of the Transportation Research Board*, 9–15.

[43] Hoh, B., Gruteser, M., Xiong, H. and Alrabady, A. 2006. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing,* 5, 38–46.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

allows for one entity to know the vehicle's identity but not its position (and vice versa). While this approach minimizes privacy concerns, the usefulness of the collected data and its integrity would be called into question. Moreover, there is still the potential to re-identify individual vehicle through data mining and cluster analysis techniques.

Dötzer's approach to protecting privacy relies on the use of tamper-proof pseudonyms that can be changed in accordance with privacy threat model and mapped to real-world identities in special situations by a certification authority.[44] The trusted third party would be responsible for validating the authenticity of the entity sending the message while keeping its identity secret. This proposal depends on the creation of pseudonyms that are robust (so they cannot be spoofed) as well as a certification authority that is backed by statute (so that all manufacturers have to participate in the system). However establishing such an authority would be a considerable multi-jurisdictional undertaking (since cars are sold for a geographic region such as North America, rather than just Canada for example). And if the pseudonym is not changed often enough or becomes known the real-world identity of the traveler would be revealed. An additional issue is that in a sparse network "if you cannot hide in a crowd of pseudonym changing vehicles, you must assume that an observer can link your old pseudonym and your new one, making this process useless."[45]

A third technical approach to privacy protection is one that allows users to select the degree of privacy they wish to have.[46] The user is tasked with determining the acceptable trade-off between privacy and authentication as is assigned group membership based on that determination. Under this approach "the authentication requester need only be verified that it is a member of a group, and the authentication server treats every member in that group the same, because of the shared common information among all the group members make them indistinguishable from the authentication server's view".[47] However establishing the optimal group size to ensure that privacy is protected as traffic conditions change as well ensuring the efficacy of such a network remain outstanding issues with this approach.

Where the anonymity of the driver is revealed either through hacking of the network or through data mining techniques, the existing regulatory framework for privacy protection will be required to respond. Finding the appropriate balance between privacy protection and network effectiveness presents an ongoing regulatory challenge. This challenge as described in the next section is unlikely to be solved entirely by reliance on the personal information and individual consent model alone.

4. Privacy issues unsolved by consent and personal information in VANETs

As noted in the previous section the fact that vehicles are increasingly connecting with each other and with public networks (e.g. V2V, V2I) make it inevitable that nodes (i.e. cars) 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 dependent on other people since it is possible to determine information about a user from their contacts or driving patterns.[48] 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."[49] 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 to reveal the identity of an individual driver.

The fact that the tracking of vehicles can reveal sensitive locations, such as home, office and places frequently visited needs to be reconciled with the fact that privacy can often conflict with authentication requirements. This is because critical safety information must be sent to a trusted source. As the scope of privacy law turns on whether the personal information of an identifiable individual is involved, it is often assumed that if there is no personally identifiable information there is no privacy harm.[50] However, as the technical proposals for securing VANET data demonstrate, there are many circumstances in which non-personally identifiable information can be linked to individuals and transformed into personally identifiable information. On the other hand, placing strict limits on the collection, use and disclosure of personal data may result in the full benefits of VANETs going unrealized. Accounting for the potential risk of re-identification will necessarily involve a measure of regulatory guidance to establish appropriate safeguards in this context.

In addition to the problems of defining personal information, relying on individual consent in the VANET context is unlikely to provide meaningful privacy protection as there are powerful countervailing interests such as safety, economic efficiency and customer convenience. The concept of individual consent in the context of privacy protection in general and VANETs in particular is burdened by assumptions of individual autonomy to control personal information. The control of data cannot be considered meaningful in circumstances where the individual is unable to assess the risk associated with disclosing personal information. Without a clear articulation of what the individual is entitled to control, privacy rights can be presented in a way that provides individuals with no meaningful choice. This is achieved by assuming that the individual has agreed to the use of their personal data when service is first provided. Reducing the consent to an isolated transaction thus

[44] Ibid., n. 29.

[45] Dötzer, F. Privacy issues in vehicular ad hoc networks. Privacy enhancing technologies, 2005. Springer, 197–209.

[46] Sha, K., Xi, Y., Shi, W., Schwiebert, L. and Zhang, T. Adaptive privacy-preserving authentication in vehicular networks. First International Conference on Communications and Networking in China, 2006. ChinaCom'06, 2006. IEEE, 1–8.

[47] Ibid., p. 4.

[48] Ibid., n. 29.

[49] Dötzer, F. Privacy issues in vehicular ad hoc networks. Privacy enhancing technologies, 2005. Springer, 197–209.

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

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

enables connected vehicle service providers to discharge their privacy obligations with a well drafted privacy statement.

Instead of focusing on consent, technology proposals aimed at enhancing security in VANETs have concentrated on the identity of the car, rather than the driver. It is assumed in the security literature that if the car is anonymous, no personal information is involved. However, the car's data log still has a value to third parties, in the same way that a net user's browsing history does.

There are also some issues where consent will be removed from the policy determination entirely. The pressure to adopt a general wireless authentication for example, specifically for advanced safety mechanisms, also raises privacy concerns as well as the potential for widespread surveillance.[51] This is particularly problematic under circumstances where the driver has no choice about participating in the connected vehicle safety system.[52] Decisions regarding the reasonableness of certain forms of data collection in the connected vehicle context will be crucial if technical solutions are to be developed in this area. In the next section, a code of practice in the connected vehicle context discussed a potential solution to the issues raised above.

5. Toward a privacy code of practice for the connected car

Codes of practice are designed to influence organizations to conduct themselves in ways that benefit both themselves and the community. They can also serve as a signal to consumers that the organization's product, service or activity meets or exceeds regulatory requirements. The development and codification of basic privacy norms in this sector can serve to both enhance consent in the short term and provide alternatives to consent (in the form of regulatory requirements) in the long term.

In the short term, a code of practice would draw attention to inappropriate data handling practices that may otherwise go unnoticed. This would assist individuals in understanding the data they are entitled to control. Individuals could demand services be provided in more minimally intrusive ways. In the long-term, a code of practices can assist in directing regulatory attention to systemic threats to privacy that result from the widespread deployment of VANET technologies.

A code of practice for connected vehicles has limitations inherent to 'soft-law' generally. First, there is the issue of whether consent and/or privacy protection will be enhanced by a sectoral 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.*[53]

Second there is the question of code enforceability and consequences 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. Given the fact that the stakeholders involved with VANETs consist of such a wide range of stakeholders from car manufacturers to Internet service providers and insurance agencies as well as government stakeholders. Thus identifying all the people and organizations that could be involved or affected by the code and taking their interests or concerns into account represents a significant challenge in code development. Finding consensus among such a broad range of stakeholders regarding issue identification and objectives as well as the potential costs, limitations and benefits would be difficult. It should be understood that personal data is a core asset of most businesses and so restricting its use limits strategic options.[54] While it has been argued that privacy breach can cause a media backlash[55] the alternative is being at a competitive disadvantage to companies with more consumer data. For many companies privacy is a variable rather than central in the business development of a service or product. It should also be noted that the adoption of codes of practice raises competition law issues to the extent that they substantially reduce competition or prevent non-participating firms from entering the market. They can also negatively affect consumers by significantly raising prices, reducing service or limiting product choice.

The challenges associated with safeguarding privacy in the connected vehicle context have lead some commentators to go as far as to call for sector-specific legislation that will protect privacy in the connected car context.[56] While such prescriptive rules would be easy to justify if the uses of data had little or no benefit from the widespread deployment of connected vehicles, there are many socially desirable uses of VANET data. A code of practice could create a set of default rules that could be waived in certain circumstances. Derogations from the code would not necessarily be privacy derogations, but it would make noticeable a given organization's departure from the code, requiring them to more clearly justify their information practices. A code of practices with respect to VANETs would have a substantive position on the appropriateness of certain forms of collection, use and disclosure of data. The development of a code is a learning process. The experience of developing a code can lead to the creation and establishment of substantive obligations, accountability structures and institutions.

Individual control and personally identifiable information will continue to play a central 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

[51] Hubaux, J.-P., Capkun, S. and Luo, J. 2004. The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine,* 2, 49–55.

[52] Ibid., n. 41.

[53] ISED. 2010. *Innovation Science and Economic Development – Codes Guide – Processes for Developing Effective Codes* [Online]. Available: https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00964.html#footnote2 [Accessed February 27, 2017].

[54] Spiekermann, S. 2012. The challenges of privacy by design. *Communications of the ACM,* 55, 38–40.

[55] Cavoukian, A. and Hamilton, T. 2002. The Privacy Payoff. How Successful Business Build Consumer Trust. *McGraw-Hill Ryerson Trade.*

[56] ISED. 2010. *Innovation Science and Economic Development – Codes Guide – Processes for Developing Effective Codes* [Online]. Available: https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00964.html#footnote2 [Accessed February 27, 2017].

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

regulation; without it there would be no limit on the scope of privacy law.[57] However, while necessary, individual control and personally identifiable information are an insufficient form of privacy protection in VANETs. This is because this approach to privacy protection addresses isolated transactions between individuals and organizations. A reliance on individual consent regarding collection, use and disclosure of data fails to take into account the increasingly interdependent nature of privacy and the complex nature of information networks. This implies a need to holistically address a set of wider social values that include, but are not limited to, privacy.

A notable effort to develop privacy codes of practice with respect to personal data in cars has been the joint Auto Alliance's and Global automakers consumer privacy protection principles for vehicle technologies and services.[58] Members of the Alliance and Global Automakers created a set of privacy principles to which members of the Associations agree to as a basic set of privacy commitments. The principles establish a framework that automakers and other participants in the automotive industry may choose to adopt when offering innovative vehicle technologies and services. The principles are based on the Fair Information Practice Principles but pay special attention to particularly sensitive information in the connected vehicle context, such as geolocation, driver behavior and biometric information. These forms of data require increased protection to be in place.

Central to the privacy protection principles is the concept of 'covered information' in the connected car context. Covered information is defined as:

(1) Identifiable information that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a participating member in connection with vehicle technologies and services; or
(2) Personal subscription information provided by individuals subscribing or registering for vehicle technologies and services.[59]

The principles are intended to cover new vehicles no later than Model Year 2017 and while the principles are not intended to replace or even supplement existing law, the fundamental data protection practices upon which the principles are based are sound. Although companies are free to implement the principles as they see fit, departure from the principles would need to be justified. Affirmative consent is required for the sharing of covered information by participating members with third parties when geolocation information, biometrics or driver behaviour information is being used for the basis of marketing, consumers are able to better assert and articulate their privacy concerns in these areas. However, affirmative consent is not required where safety or compliance issues are involved. A notable caveat is that affirmative consent is not required for internal research or product development. While this provision is self-serving, a substantive discussion of the merit of certain forms of data collection and the need to prioritize certain form of data as worthy of increased protection is at least taking place.

Defining covered information as 'information that is linked or linkable' is an important step toward the recognition that organizations are better placed than individuals to identify and mitigate the risks with respect to privacy. Identifiable information is defined as information that is liked or reasonably linkable to (i) the vehicle from which the information was retrieved, (ii) the owner of that vehicle, or (iii) the registered user using vehicle technologies and services associated with the vehicle from which the information was retrieved. In this way, the definition of protectable information from being about and identifiable information to being about a vehicle or individual associated with the vehicle (i.e. a passenger) is expanded. This broadening of the definition of identifiable information is helpful because it recognizes that personally identifiable information is too narrow to provided meaningful privacy protection in the connected vehicle context. It also aligns business practice with technical proposals aimed at securing data in connected vehicles.

The definition of covered information however contains an important caveat.

> *If participating member collects covered information and then alters or combine the information so that the information is no longer reasonably linked to the vehicle from which the information was retrieved, the owner of that vehicle or any other individual, the information is no longer covered information. If participating members attempt to link the information to specific, identified individuals or vehicles or share the information without prohibiting the recipients from attempting such linking, information becomes covered information.*[60]

Whether information can be reasonably linked is problematic to the extent that it has been demonstrated scientists can often 're-identify' or 'de-anonymize' individuals hidden in anonymized data.[61] Government regulation would be needed in order to provide clear guidance on acceptable risks to re-identification.

The focus of automakers' attention with respect to privacy protection is understandably on their customers. This is appropriate as they have a direct relationship with their customer. A privacy code of practice, unlike a privacy statement, represents a common set of privacy principles within a particular sector that is not contingent on the consent of a given customer. This being said, the complex nature of modern information networks makes defining the sector a particularly challenging task. It would be necessary going forward to incorporate a broader range of stakeholders as well as appropriately define the scope of the sector.

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

[58] Auto, A. 2014. *Consumer privacy protection principle for vehicle technologies and services* [Online]. Available: https://autoalliance.org/connected-cars/automotive-privacy-2/principles/ [Accessed March 24, 2017].

[59] Ibid.

[60] Ibid.

[61] Ohm, P. 2010. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

Sharing of consumer data raises significant privacy concerns that the user is unlikely to be aware of and therefore framing the discussion as one of consumer choices and control over personal information is unhelpful. The development of 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.

It is unrealistic to assume that consumers can be informed about data sharing via a privacy statement. The concept of control with respect to personal information has its limitations since individuals are unable to assess the risk associated with disclosing personal information. When data is shared among multiple recipients, it is appropriate that connected car companies provide information about their data sharing network and take responsibility for its conduct. A privacy management code of practice that establishes rules for all third parties that want to provide location services using a company's network can serve to promote shared network responsibility. Penalties for breaching the code such as contract termination, cost recovery and withholding payment are all mechanisms that could be used to enforce the code.[62] In this way, a company can not only take responsibility for its own practices, but it can also inform its customers about its data sharing practices and enforce privacy standards on its networks. While the Auto Alliance's and Global automakers consumer privacy protection principles make no mention of these sorts of enforcement mechanisms, it does contribute to the privacy protection process which can be further elaborated upon.

6. Conclusion

VANETs have the potential to greatly improve the transportation infrastructure by providing safety and convenience by enabling communication between vehicles, infrastructure networks and pedestrians. The data generated by the deployment of such networks are a critical source of consumer data which has the potential to significantly weaken privacy. The current focus on individual consent in data protection law, policy discussion and industry practice has the effect of leaving a broader set of privacy issues to go unaddressed. This paper has argued that while consent remains important, privacy law and policy cannot remain neutral with respect to data that is being collected, used and disclosed in this context. The development and codification of privacy norms in VANETs would assist in making substantive decisions making easier to understand regarding what is being protected (and what is not).

The development of a privacy code of practice for the connected vehicles would draw attention to inappropriate data handling practices that may otherwise go unnoticed and assist individuals in understanding the data they are entitled to control. It would also place boundaries on the sharing of location data by third parties and provide 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. While grappling with these issues will remain a challenge, avoiding these very real problems under the thin veil of consent will not make them go away.

[62] Spiekermann, S. and Cranor, L. F. 2009. Engineering privacy. IEEE Transactions on Software Engineering, 35, 67–82.

REFERENCES

Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on electronic commerce. ACM; 2004. p. 21–29.
Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular ad hoc network. J Netw Comput Appl 2014;37:380–92.
Austin LM. Is consent the foundation of fair information practices? Canada's experience under PIPEDA. Univ Tor Law J 2006;56:181–215.
Austin LM. Enough about me: why privacy is about power, not consent (or harm). In: Sarat A, editor. A world without privacy?: what can/should law do. (January 1 2014). Available at SSRN: https://ssrn.com/abstract=2524512. Forthcoming in.
Auto A. Consumer privacy protection principle for vehicle technologies and services [Online]; 2014. Available from: http://goodtimesweb.org/industrial-policy/2014/Consumer PrivacyPrinciplesforVehicleTechnologiesServicesFINAL.pdf. [Accessed 24 March 2017].
Cavoukian A, El Emam K. 2014. The unintended consequences of privacy paternalism. Information and Privacy Commissioner, Ontario, Canada, 5.
Cavoukian A, Hamilton T. The privacy payoff. How successful business build consumer trust. Whitby, Ontario Canada: McGraw-Hill Ryerson Trade; 2002.
Cheng HT, Shan H, Zhuang W. Infotainment and road safety service support in vehicular networking: from a communication perspective. Mech Syst Signal Process 2011;25:2020–38.
Cottrill C. Approaches to privacy preservation in intelligent transportation systems and vehicle-infrastructure integration initiative. Transp Res Rec 2009;9–15.
Dötzer F. Privacy issues in vehicular ad hoc networks. In: Privacy enhancing technologies. Springer; 2005. p. 197–209.
Fernandes P, Nunes U. Platooning with IVC-enabled autonomous vehicles: strategies to mitigate communication delays, improve safety and traffic flow. IEEE Trans Intell Transp Syst 2012;13:91–106.
Fried C. Schoeman FD, editor. Privacy: a moral analysis. Philosophical dimensions of privacy: an anthology. Cambridge: Cambridge University Press; 1984.
Gehlen G, Pham L. Mobile web services for peer-to-peer applications. In: Second IEEE Consumer Communications and Networking Conference, 2005 (CCNC 2005). IEEE; 2005. p. 427–433.
Glancy DJ. Privacy in autonomous vehicles. Santa Clara Law Rev 2012;52:1171.
Glancy DJ. Sharing the road: smart transportation infrastructure. Fordham Urban Law J 2013;41:1617.
Hartenstein H, Laberteaux KP. A tutorial survey on vehicular ad hoc networks. IEEE Commun Mag 2008;46:164–71.
Hoh B, Gruteser M, Xiong H, Alrabady A. Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Comput 2006;5:38–46.
Huang C-J, Chen Y-J, Chen I-F, Wu T-H. An intelligent infotainment dissemination scheme for heterogeneous vehicular networks. Expert Syst Appl 2009;36:12472–9.
Hubaux J-P, Capkun S, Luo J. The security and privacy of smart vehicles. IEEE Secur Priv Mag 2004;2:49–55.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006

ISED. 2010. Innovation science and economic development – Codes guide – Processes for developing effective codes [Online]. Available from: https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00964.html#footnote2. [Accessed 27 February 2017].
Jayapal C, Roy SS. Road traffic congestion management using VANET. In: 2016 International conference on advances in human machine interaction (HMI). IEEE; 2016. p. 1–7.
Lawson P. 2015. The connected car: who is in the driver's seat? British Columbia: BC Freedom of Information and Privacy Association.
Maglaras LA, Al-Bayatti AH, He Y, Wagner I, Janicke H. Social internet of vehicles for smart cities. J Sens Actuator Netw 2016;5:3.
McIsaac B, Shields R, Klein K. 2004. The law of privacy in Canada. Scarborough [Toronto], Ont.: Carswell.
Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life. Stanford University Press; 2009.
Ohm P. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Rev 2010;57.
Panghal AK, Rani S. Vehicular ad-hoc network (VANET) – privacy and security. Int J Adv Res Comput Sci 2015;6.
Pollach I. Online privacy as a corporate social responsibility: an empirical study. Bus Ethics 2011;20:88–102.
Scassa T, Chandler JA, Judge EF. Privacy by the Wayside: the new information superhighway, data privacy, and the deployment of intelligent transportation systems. Sask Law Rev 2011;74:117.
Schwartz PM, Solove DJ. Pii problem: privacy and a new concept of personally identifiable information. NYUL Rev 2011;86:1814.
Sha K, Xi Y, Shi W, Schwiebert L, Zhang T. Adaptive privacy-preserving authentication in vehicular networks. In: First international conference on communications and networking in China, 2006 (ChinaCom '06). IEEE; 2006. p. 1–8.
Solove DJ. Privacy self-management and the consent dilemma. Harv Law Rev 2013;126.
Spiekermann S. The challenges of privacy by design. Commun ACM 2012;55:38–40.
Spiekermann S, Cranor LF. Engineering privacy. IEEE Trans Softw Eng 2009;35:67–82.
Westin AF. Privacy and freedom. New York: Atheneum; 1967. p. 7.

Please cite this article in press as: Rajen Akalu, Privacy, consent and vehicular ad hoc networks (VANETs), Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.006