PAVING THE WAY FOR

INTELLIGENT TRANSPORT SYSTEMS (ITS):

The Privacy Implications of Vehicular Infotainment Platforms

PAVING THE WAY FOR

INTELLIGENT TRANSPORT SYSTEMS (ITS):

REPORT AUTHORS:

Rajen Akalu, Ph.D., Principal Investigator
Khalil El-Khatib, Ph.D., Co-Investigator
Steve Marsh, Ph.D., Co-Investigator
Tosan Atele-Williams, Senior Researcher
Kushal Jaisingh, Research Assistant

Rajen Akalu, Ph.D.
Assistant Professor
Faculty of Business and IT
University of Ontario Institute of Technology
2000 Simcoe Street North Oshawa, Ontario L1H 7K4 Canada
905 721 8668 x 5438 | rajen.akalu@uoit.ca | www.privacyandtheconnectedcar.ca

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. Submitted March 31, 2016.

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Contents

Summary

This project is titled: "Paving the way for Intelligent Transport Systems (ITS): The Privacy Implications of Vehicular Infotainment Platforms." The aim of this project is to determine the privacy implications of vehicular digital forensics as applied to car infotainment systems. We aim to assess the information stored in an infotainment unit as well as what this discloses about an end user and his or her actions. The project involved tracking personal information as it passes through a typical infotainment system. Infotainment logs are analyzed in order to determine driver usage patterns and identify possible secondary uses of the information as well as strategies that consumers might employ to safeguard their privacy while driving. A survey was conducted in order to gauge user perception of privacy in the use of vehicle infotainment and telematics systems. This was done in order to identify the factors that motivate information sharing and privacy concerns with respect to the use of vehicle information systems. Privacy information officers of leading car manufacturers were also interviewed as part of the project in order to determine how they are currently addressing privacy concerns regarding infotainment systems to their customers. The project concludes by providing recommendations for reform.

Introduction

The Intelligent Transportation System (ITS) and Vehicular Ad Hoc Networks (VANETs) are paving the way for an efficient, safer and user-friendly roadside and transportation system. The ITS and VANETs utilize 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.[1]

Modern vehicles are equipped with infotainment systems that are integrated with the ITS and VANET infrastructure. This constitutes 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.[2] Telematics data can be used to reconstruct accidents and determine their cause, or used by law enforcement to predict a suspect's behaviour.[3] Scassa et al. argue that "while ITS may offer significant benefits for safety, security, and environmental sustainability, it also raises considerable informational privacy risks."[4] The aim of this project is to assess the privacy risks associated with ITS with respect to infotainment platforms currently deployed in the transportation market.

Previous work by Lawson concluded that connected car service providers are not compliant with Canadian data protection law in various respects. Her review of "publicly available terms and policies suggests widespread disrespect for the privacy of customers by companies offering connected car services."[5]

The applicable federal data protection law in this context is the Personal Information Protection and Electronic Documents Act (PIPEDA).[6] This legislation provides individuals with a certain degree of control over their personal information by imposing obligations on organizations that collect, use and disclose that information in the course of commercial activities.[7] However, as Austin notes, "[c]ontrol is not a sufficient condition for the protection of privacy, as individuals may be provided with control and consequently choose to give up their privacy."[8] It has been 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.[9]

---

1 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.

2 Y. Kopylova, C. Farkas, and W. Xu, "Accurate accident reconstruction in VANET," in Data and Applications Security and Privacy XXV, Springer, 2011, pp. 271–279.

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

4 Scassa, T., Chandler, J. A., & 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. at p. 2.

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

6 S.C. 2000, c. 5.

7 PIPEDA s. 4 (1).

8 Austin, L. (2003). "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices"." Canadian Business Law Journal 44: 21. See also Allen, A. L. (1999). "Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm." Conn. L. Rev. 32: 861.

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

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."[10] Lawson's account of the privacy policies of connected car automakers demonstrates that they are clearly not remarkable in this regard. Moreover creating simpler or more usable privacy controls and notices might not improve users' decision-making regarding the sharing of personal information. It has been argued that such an approach to privacy protection might paradoxically increase riskier disclosure by assuaging privacy concerns while controlling data flows through simple framing or mis-directions.[11]

The approach of holding automakers accountable for compliance with PIPEDA as well as their stated privacy policies leaves a number of questions unanswered, notably: 1. How can control of data or consent to use data be considered meaningful in circumstances where the individual is unable to assess the risk associated with disclosing personal information? 2. Who should bear the risk associated with the privacy harms that were unforeseen by the service provider or the user when a new technological feature is implemented?

To begin to address these questions we need to better understand the nature of privacy in the context of connected cars as well as the nature of privacy concerns amongst consumers. Understanding consumer expectation, Canadian data protection laws, as well as the privacy risks associated with using infotainment and telematics systems will assist in the design of ITS privacy solutions that are appropriate in the circumstances.

Infotainment and telematics systems, like all information systems, typically perform one or more of the following tasks: data transfer, data storage and data processing. The focus of this project considers how this data is stored inside the vehicles, for how long and if forensic analysis can access to it.

It should also be noted that vehicles are increasingly communicating with each other and with public networks through V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure) and V2P (vehicle-to-pedestrian) interactions. This enables both collection and the real-time sharing of critical information about the condition on the road network. This social interaction, both among vehicles and among drivers, raises issues of security, privacy and trust that need also to be addressed.[12]

This report is composed of four parts. The first part involves analyzing infotainment logs using forensic techniques in an acquired Ford F-150 truck infotainment unit. This will enable us to track the flow of personal information as it passes through a typical infotainment system.

In part two of the report, we conduct a consumer survey on privacy concerns relating to infotainment systems. While the comfort, safety, security, and added services that infotainment

---

[10] Pollach, I. (2005). "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62(3): 221-235. See also Pollach, I. (2007). "What's wrong with online privacy policies?" Communications of the ACM 50(9): 103-108.

[11] Acquisti, A., I. Adjerid and L. Brandimarte (2013). "Gone in 15 seconds: The limits of privacy transparency and control." IEEE Security & Privacy(4): 72-74.

[12] Maglaras, L. A., A. H. Al-Bayatti, Y. He, I. Wagner and H. Janicke (2016). "Social Internet of Vehicles for Smart Cities." Journal of Sensor and Actuator Networks 5(1): 3.

systems bring into the driving experience are innovative, they also raise considerable concerns on the ability of consumers to decide when, what, and how information about them is collected, stored, used and disclosed to others.

In part three, we report on our discussions on our work with privacy information officers of car manufacturers. This is done in order to understand how they are currently addressing privacy concerns of their customers as well as their view on regulatory reform in the connected car sector.

The fourth and final part of this report provides our conclusions and recommendations for reform. We have grouped our recommendations for reform into two sections: theoretical and practical. At the theoretical level, we discuss the concept of privacy and highlight the need for a free-standing reasonableness requirement for third party co-operation with law enforcement. We then discuss practical recommendations as they relate to connected cars. Specifically, we recommend automakers adopt codes of practice with respect to the handling of customer data. Lastly, we outline the privacy requirements for ITS. This particular recommendation relies on establishing an independent credentialing authority that would need to be created by statute and trusted by customers, manufacturers, system operators, and service providers to manage pseudonymous data.

Part 1 – Tracking the Flow of Personal Information in the Connected Car

Infotainment and telematics components allow a vehicle to generate, log and exchange data about its surrounding and users in real time. The data logged hypothetically gives a third party the ability to analyze this data if accessed. Data about a driver could also be collected if he or she was suspected of criminal activities or for commercial purposes. Infotainment systems inside modern vehicles can potentially reveal a lot about the end user through his driving patterns, activities while driving and location. In this part, we explore the possibilities of vehicular digital forensics by identifying what can be stored in the memory of an infotainment system. This will in turn provide some inferences in terms of what actual information is stored and what it can disclose about an end user and his/her actions. To this end, we report on data acquired from an F-150 truck infotainment unit. A general description of VANET architecture is first provided.

1. Vehicle components and architecture

Vehicular ad hoc networks (VANETs) belong to a general class of mobile ad hoc network with fast moving nodes (i.e. vehicles). There are two main components to a VANET: 1) On-board units built into vehicles; and 2) Roadside units (RSUs) deployed along highways/sidewalks that facilitate V2V and V2I communication.[13] The potential VANET applications fall into three main categories: 1) Infotainment delivery; 2) road safety; and 3) traffic monitoring and management. In this section, we report on the infotainment system.[14]

Modern vehicles now make use of many computer buses within their internal components to send and receive operational messages. Electronic Control Units (ECUs) process this data then actuate mechanisms to accomplish tasks requested by the vehicle's user. Some of these components and buses are segregated from one another for compartmentalization; however, they are all able to communicate with one another to fulfill the vehicle user's demands using the Control Area Network (CAN) bus. There are multiple modules/units and respective buses and they are each responsible for specific traffic flow inside the vehicle, as depicted in Figure 1.[15]

The following list shows the core networking buses within a vehicle for data exchange:

- CAN (Controller Area Network) – Core bus that links all buses together for data exchange and provides an interface for on-board diagnostics.
- LIN (Local Interconnect Network) – Sub-network used for low-speed and bandwidth applications. e.g., doors and sliding windows up and down.
- FlexRay – Sub-network used for safety critical and high-speed messages. e.g., vehicle stability control and embedded sensors.

---

[13] Cheng, H. T., H. Shan and W. Zhuang (2011). "Infotainment and road safety service support in vehicular networking: From a communication perspective." Mechanical Systems and Signal Processing 25(6): 2020-2038.
[14] Toor, Y., P. Muhlethaler and A. Laouiti (2008). "Vehicle ad hoc networks: applications and related technical issues." Communications Surveys & Tutorials, IEEE 10(3): 74-88. See also Willke, T. L., P. Tientrakool and N. F. Maxemchuk (2009). "A survey of inter-vehicle communication protocols and their applications." Ibid. 11(2): 3-20.
[15] Everett, C. E. and D. McCoy (2013). OCTANE (Open Car Testbed and Network Experiments): Bringing Cyber-Physical Security Research to Researchers and Students. CSET, Citeseer.

- MOST (Media Oriented System Transport) – Sub-network used for high-speed and bandwidth multimedia related applications. e.g., music/video streaming and vehicle cameras.

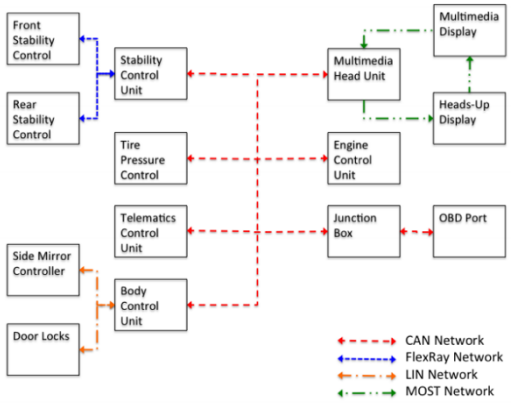

Figure 1. Vehicle network components and buses

The following list describes the core modules attached to the aforementioned buses. In general, they are found in modern vehicles and associated internal networks:

- Junction Box – provides typical functions for the vehicle's circuits but in this case, connects the OBD II (On-Board Diagnostics) port to the CAN bus.
- Engine Control Unit – Controls actuators for the engine to ensure optimal performance and does so by reading acquired data from multiple sensors through the CAN bus.
- Multimedia Head Unit – infotainment system in this case, communicates to the dashboard and multimedia displays through the MOST bus and can receive data from CAN bus as well.
- Stability Control Unit – uses the FlexRay sub-network to engage stability control ECUs and actuators and relays/receives information to the CAN bus.
- Tire Pressure Control Unit – directly affiliated with Tire Pressure Monitoring System (TPMS) for relaying information about each tire through the CAN bus.
- Telematics Control Unit – controls embedded systems (e.g. GPS unit, 3G/LTE, WiFi communication interfaces) within the vehicle through the CAN bus.
- Body Control Unit – uses the LIN bus for engaging door locks, window/side mirror positioning, seat positioning, etc. and relays/receives information through the CAN bus.

The CAN network is responsible for forwarding all traffic that needs to be relayed between each sub-network. It is essential to the vehicle's operation since it forwards all queries and responses. Error messages also circulate on this network for diagnostic purposes. End users are then notified through the vehicle's dash display about a present issue. Access to a CAN bus could lead to disclosure of live vehicular forensics if enough data is collected and analyzed correctly. Once connected to the CAN, it could grant potential access to separate modules within the vehicles and their respective ECUs. This could then lead to further vehicular forensic opportunities through

non-volatile memory. The network/bus used for infotainment/multi-media traffic is the MOST bus. The MOST bus makes use of optical fibre cables and can now reach speeds of up to 150 Mbps.

1.2 Vehicular infotainment systems and forensic potential

VANETs differ from traditional mobile ad hoc networks (MANETs) in terms of network architecture, user mobility patterns, energy constraints and application scenarios. Unlike typical nodes in a MANET, the nodes (i.e. vehicles) are fast moving. This presents a number of challenges with respect to evidence collection in these types of networks. These challenges include:

- Mobility – node localization is difficult due to network changes
- Existing security mechanisms – forensics in malicious networks are more difficult to detect
- Topology changes – network state determination is difficult because of constant network condition changes
- Unreliable channels – packet loss due to nature of wireless networks
- Multi-hop communication – source of suspected traffic is difficult to trace
- Low power devices – power constraints for data collection and data selection (except for VANET)
- Interoperability – crime point of origin is difficult to determine

Acessing infotainment system data might help determine points of origin through local GPS data acquisition, breadcrumb trails and end point destinations. Analysing data remnants of applications used by the infotainment systems could also help determine the malicious user (e.g., unknown applications being used and/or illegitimate uses of legitimate applications).

Infotainment systems, such as Ford's SYNC modules, have GPS embedded into them when manufactured. Since the infotainment platform produces this type of data by design, it is clearly highly sensitive. It must be determined how this data is stored inside the vehicles, and for how long. There is also the multitude of metadata produced by current/future in-car applications as well as social media applications. Boundaries must be determined, but methods to access and determine how the information is stored must also be established.

1.3 Preliminary analysis of a F-150 Truck infotainment unit

As part of our research, we were able to acquire a logical and file system dump of a Ford F-150 truck SYNC infotainment's file system and associated content files. The infotainment system is of a Windows based type architecture since SYNC currently runs on Microsoft's automotive OS, Windows CE. As for hardware, the interface that connects to the vehicle's dashboard appears to be proprietary as no schemes for its wiring could be found. The SYNC modules mainly interact with each other, the dashboard and Bluetooth devices (assuming the SYNC has the feature offered).

The nature of infotainment systems also suggests that the data collected could potentially go beyond the direct interactions of the driver and the system. Since navigation data has multiple uses, this relationship could be combined with other available information such that even more about the user could become known.

1.3.1 Data Dump format and details

The logical dump itself resembles a direct data dump (dd) from a POSIX system with encoded metadata, which is not that surprising since information such as original file name, checksum and disk location can be found. These dumps were accessed and read through the use of the Forensic Toolkit (FTK) version 5 data analyser.

The file system dump contains many ".swf" (Flash) files since SYNC is highly interactive with its UI (User Interface). The fact that Flash is employed does hint at potential security holes, which could be exploited by circumventing security mechanisms in order to gain access to stored data for analysis. Direct access to the data inside the file system without the FTK and/or special forensics software will be nearly impossible since encryption and/or compression is being employed on the data itself. The entire payload is then certified with a self-signed Microsoft publisher certificate. From this, it is uncertain whether it is simply a test certificate or if it is actually being authenticated to a CA (Certification Authority). The dumps themselves seem to be generated by a built-in dump utility employed by Windows CE. The VIN (Vehicle Identification Number) has been potentially located but not fully verified and more testing will be needed to check if it is encrypted. Once the VIN is confirmed, it will then be possible to check whether the infotainment system uses some form of authentication process using a VIN for booting up.

1.3.2 File system file contents

The acquired logical and file system dumps provided access to some content from the SYNC's infotainment systems. Compared to the file system dump, the logical one gave us the least amount of information to analyse although it is the easiest one to acquire. Special forensics software Encase (trial edition) and Autopsy (The Sleuth Kit's graphical user interface version), was used for data analysis. It is important to note that a portion of the files and content was in an unreadable format.

The use of compression and encryption is also adding difficulty of appropriate analysis of acquired data. The following list is a preliminary compilation of observations and is being presented as a statement that establishes that infotainment systems do have the potential to withhold user data. It is not limited to personal information as the objective is to show what can be obtained from an infotainment system by acquiring memory contents, whether it be the entire file system dump or just parts of it.

The following system contents were obtained:

- "phone book" folder was discovered – XML file found containing "Device ID", "Call name", "Call Type" and "Call Time" (time it was made). Potential information retained from Bluetooth phone devices connecting to the infotainment system include the device name, phone logs, missed calls and text messages
- Bluetooth connection attempts and potential security PIN revealed in hexadecimal format when authenticated
- Infotainment system's Bluetooth address acquired
- WiFi SSID (Service Set Identification) revealed, associated security type and if SSID is broadcasting – helps determine if easily accessible

- logs of USB device connections and respective file structure – it was discovered that the system also checks for valid installation files when a USB device is connected. If a valid .lst file is found, check .cab file and Ford Root CA. Also useful for determining who interacted with the infotainment system based off name of USB device
- .ctx files which store images and source code
- last known AM/FM frequencies and Sirius radio related information – useful for general localization information
- "mailbox" folder was discovered – no emails were found as of now, unsure if this feature was used. Pertinent to how long sent and received items are stored, or cached and for how long
- SYNC version and build number – the version, helps determine if it can be exploited more easily as well as the hardware arrangement
- copyright information and involved partners – hints at embedded technology
- profile Internet information – sub-folders include cookies, history and temporary Internet files but nothing was discovered inside these folders (possibility that the feature was not recently used/or at all)
- graphical BMP files – geographical weather locations, perhaps relates to GPS data
- OpenSSL is used – potential "Heartbleed" vulnerability depending on its version
- SQLite is being used for database formation and management
- many databases were found relating to fuel price listings, WiFi network listings, movie listings, etc.
- database entries and associated attribute values
- header files and related information
- "dummy" file used for creation of CAB file
- large amount of various log files – GPS.log, version.log, Database.log, logs directly pertinent to user activity, etc.
- "www" folder found – Windows CE Web Server is enabled by default
- ECU response was located – interaction with other device apart from infotainment modules.
- climate state/configuration – potentially can determine if a vehicle was left inside/outside as well as general temperature of environment
- odometer readings are displayed in some files – allowing for determination total distance travelled from last known point
- GPS related information – source/destination
- GPS favourite and "my home" information – longitude, latitude, altitude, city, state/province, etc.). "User data" folder found that holds this type of information. e.g., movie listings and searches, fuel prices and gas stations nearby, etc.
- broadband information – username, password, phone number, carrier and country data set found
- configuration logs and device profiles – e.g., NVRAM configuration, USB modem configurations, specific libraries to use with specific devices, etc.
- Bluetooth firmware version – potential vulnerabilities depending on its version
- active audio sources, USB port and Bluetooth device statuses
- Windows CE version – potential vulnerabilities depending on its version.
- basic attributes of entire file system and associated content

- encoding used is ISO-8859-1 and Windows-1252
- private key file referenced – privkey.pm but location does not exist therefore must be hidden with associated directories
- certificates in binary blobs – located in log files and "validcert.com" is referenced as a CA, needs to be confirmed if only CA or if there are others
- VIN number located potentially useful for booting infotainment and testing

As shown above, a considerable amount of information can be found due to the nature of a file system dump. Some of it can be less relevant to forensics and analysis but can be useful in attempting to exploit the device for easier and quicker data access and extraction. At present, it is unclear how long these log files store the information for and if it is a continuous log. Using Google maps searches, the retrieved latitude and longitude coordinates, demonstrates that the vehicle's actual location at the time of display can be determined. An interesting amount of configuration logs have also been retrieved. This allows the exact configurations used by the system to become known. Other relevant information we found in the log files show when the vehicle doors open, when it is put in reverse (camera activates so potentially parking-aid engages), when an external device plugs in, etc.

Overall, based on this preliminary analysis, it is safe to say that the Ford SYNC infotainment system holds a considerable amount of data. What would be more interesting would be to look into the Bluetooth component of infotainment systems since more personal data is contained in modern phones. It would be important to have such a device connected to the SYNC module for further analysis. This would help determine to what extent data is being migrated/copied to the infotainment platforms.

Part 2 – Analyzing User Perceptions of Privacy and Security in the Connected Car

Consumers have different requirements and constraints when it comes to the purchase and use of their vehicle. The relative novelty of infotainment systems suggests that users may not be aware of the potential for privacy harms associated with the operation of their connected car.

User perception of privacy related concerns in vehicle telematics and infotainment systems has not been studied extensively. There have been a few attempts to poll the attitudes of Canadians regarding the use of telematics by the insurance industry however.[16] In March 2015, the Canadian Automotive Association conducted a survey indicating that consumers believe that drivers should control access to and have exclusive rights associated with the data generated by their vehicles.[17]

While this survey pointed out consumer concerns regarding privacy in the context of connected cars, it was not designed to capture the factors that influence data sharing and trust among drivers and between drivers and automakers with respect to data generated by infotainment and telematics systems.

We conducted our own survey in order to gather and analyze user perception of privacy and security in the use of vehicle infotainment and telematics systems. The survey assisted in identifying the factors that motivate information sharing and privacy concerns in this context.

2.1 Methodology

2.1.1 Participants

The sample consisted of 239 Canadian residents. A 15-minute anonymous survey was administered online between February 5th and February 25th, 2016. Based on a sample of this size, the overall result can be considered accurate within a margin of error of ±7%, that is 19 out of 20 times. The margin of error is greater for results relating to subgroups of the total sample.

Data were weighted to reflect the population of Canada based on the 2011 census data. Lack of enthusiasm and reliability in online surveys were two possible fears, but research has shown that online respondents are usually motivated because of self-selection.[18] Anonymity does not have an adverse effect on data integrity.[19]

16 Perspectives, P. S. (2014). Phoenix Strategic Perspectives Survey of Canadians on Privacy, Office of the Privacy Commissioner of Canada.
17 CAA (2015). CAA In-Car Data Survey, CAA.
18 Kraut, R., J. Olson, M. Banaji, A. Bruckman, J. Cohen and M. Couper (2004). "Psychological research online: report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet." American psychologist 59(2): 105.
19 Sax, L. J., S. K. Gilmartin and A. N. Bryant (2003). "Assessing response rates and nonresponse bias in web and paper surveys." Research in higher education 44(4): 409-432.

2.1.2 Design and materials

An online questionnaire was designed using Limeservice online data collection program. The survey was divided into two sections with Section A asking for generic information such as primary occupation, educational background and driving experience. The second section, Section B, covers questions on privacy and security in vehicle infotainment telematics systems, with questions on frequency of use, familiarity, and types of services accessed. Section B also focuses on data use, collection and sharing, with its final segment looking at willingness and refusal to share using a ten-point Likert scale from least important (1) to most important (10).

2.1.3 Procedure

Following Research Ethics Board (REB) approval, a link to the survey questionnaire was posted on the research website, the UOIT Faculty of Business and IT message board and different social media accounts of the research team such as LinkedIn, BBM, WhatsApp, Facebook and Twitter. Advertisements were posted at different locations across UOIT campus sites to promote the survey. A five-minute Faculty of Business and IT student session was held in a number of classes to inform participants about the survey. The contact details of the first author and that of UOIT REB was given for any queries about the study. Participants were informed that participation was entirely voluntary and that the research was conducted according to the University of Ontario Institute of Technology Research Ethics Board code of conduct for research involving humans. They were also informed they could exit the survey at any time by not clicking on the submit button on the survey page, or simply exiting their internet browser, if they no longer wish to continue. All duplicate data and responses with more than 50% missing were omitted from the data before the analysis.

2.1.4 Limitations

The respondents were at least moderately homogeneous (well-educated, students and professionals). The number of car drivers was lower than expected, although, users of infotainment platforms may not necessarily be car drivers.

2.2 Results

Different concerns were raised when it came to data collection in the use of vehicle infotainment systems. 20% of respondents were worried about not knowing who had access to their data, 18% were concerned because they did not know who was collecting their data, 16% were more concerned about not knowing what data is being collected. Not knowing the reason for data collection was at 14%, 12% of respondents were concerned about not knowing who was collecting data and 4% were concerned because the data retention policies of the companies involved with vehicle infotainment systems were ambiguous.

As with previous survey research, control over personal information strongly influenced participant responses. People are less willing to share personal information than we give them credit for. With respect to push notifications, there seems to be a low willingness to share personal information.

Part 3 – Expert Insights on Privacy in the Connected Car

In this part, we report on discussions with privacy officers at leading automakers regarding how personal information passes through a typical infotainment system and the safeguards that are in place to protect this data. We also took this as an opportunity to obtain industry insights into automotive trends with respect to the protection of personal information. The main question we wanted to address to privacy officers at car manufacturers is: How are car manufacturers currently addressing the privacy concerns of their customers regarding the use of infotainment systems?

This question was broken down into the following 5 sub-questions:

1. How aware are consumers of the potential privacy harms associated with the use of vehicle infotainment systems?
2. What safeguards have car manufacturers put in place to mitigate these risks?
3. What can consumers do to prevent potential privacy harms associated with their use of an infotainment system?
4. Are the current laws/regulations, in particular the Personal Information Protection and Electronic Documents Act adequate, or is sector specific legislation needed?
5. What combination of technical/regulatory/consumer awareness solutions (if any) are appropriate in this context?

We contacted a number of auto manufacturers directly and were also assisted in contacting privacy officers by the Canadian Vehicle Manufacturers Association (CVMA). The CVMA is the industry association representing Canada's largest manufacturers of light and heavy-duty motor vehicles. We received several written responses that were marked confidential and so we are unable to disclose names of the respondents. We are, however, able to provide a summary of responses to our interview questions.

3.1 Summary of responses

A consensus held among automakers was that while they are committed to privacy protection, there is always some level of risk associated with connectivity. These risks, in their view, were outweighed by benefits such as increased safety and helping customers maintain optimal vehicle performance, as well as improved efficiency and convenience.

For certain services, such as dispatching emergency or roadside assistance providers, for example, vehicle location information is disclosed to third party providers. Automakers regarded their publicly available privacy policies as sufficient to permit consumers to make informed choices about their products and services. It was observed by respondents that subscribers cannot be supplied with the services they want without accessing vehicle information, including certain location information. One automaker recommended that users perform a Master Reset to erase all stored information in the vehicle if a person no longer plans to use the infotainment system or plans to sell the vehicle. Consumers should lock their vehicle when left unattended to prevent theft of the vehicle and any of its contents.

Another common response was the fact that automakers were part of a highly integrated global market. They pointed to collaborations with the U.S. Department of Transportation (DOT), the U.S.

National Highway Traffic Safety Administration (NHTSA) and other research and industry consortia to address security and privacy implications with respect to emerging infotainment, telematics and safety related technologies. As such it was felt that it would be necessary to harmonize a regulatory framework with respect to privacy as a result.

One leading automaker remarked that the benefit and advantage of PIPEDA and its uniform application is that it ensures a common standard for all involved in any way in the provision of vehicle infotainment systems. PIPEDA's technology neutral approach also enables PIPEDA to apply effectively to emerging technologies. This being the case, current laws and regulations in Canada, including PIPEDA, were regarded as strong regulatory frameworks for protecting consumers, while enabling the development and implementation of new technology. Replacing or amending PIPEDA would therefore be unnecessary. Moreover, sector-specific regulations would likely result in unduly prescriptive, unique-to-Canada requirements, and consumers would have reduced access to new technological enhancements and face increased costs as a consequence.

Part 4 – Recommendations for Reform

We have grouped our recommendations for reform into two sections: theoretical and practical. As we noted in part one, infotainment and telematics systems, like all information systems, typically perform one or more of the following tasks: data transfer, data storage and data processing. The impact on privacy will necessarily depend on how these system operations are performed.

The focus of this project considered how this data is stored inside the vehicle and what data can be obtained from an infotainment/telematics unit. Modern vehicles and their connectedness are technological developments that have profound implications for privacy. The fact that cars are becoming increasingly part of a social network of vehicles will necessarily require novel technical and regulatory solutions, which we outline in this part.

We begin with a presentation of theoretical commentary of the concept of privacy and highlight the need for a freestanding reasonableness requirement for third party co-operation with law enforcement. We then discuss practical recommendations as they relate to connected cars. Specifically, we recommend automakers to adopt codes of practice with respect to network sharing. In addition, we outline the privacy requirements for ITS. This particular recommendation relies on establishing an independent credentialing authority that would need to be created by statute and trusted by customers, manufacturers, system operators, and service providers to manage pseudonymous data. We begin with a discussion of privacy theory in relation to the connected car.

4.1. The concept of privacy

Laws and policies relating to privacy have closely followed the development of new technologies. The ITS and VANETS do not easily fall into the domain of traditional privacy theory so we are required to clarify the concept of privacy in order to assess what constitutes a reasonable expectation of privacy under the circumstances.

Warren and Brandeis writing about the privacy expectations of early photograph technology formulated privacy as the 'right to be let alone.'[20] This formulation emphasized the notion that privacy is about seclusion and separation and that the loss of privacy was a harm that laws and policies ought to protect. The harm associated with the loss of privacy was (and remains) difficult to characterize. It is highly subjective and context-specific. The regulatory challenge presented by this conceptualization of privacy was to develop privacy principles that could be applied across a range of contexts and thereby provide an effective measure of governance.

The individual or institution (and their consent to information sharing) was placed at the centre of the regulatory model of privacy. 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."[21] The definition provides a distinction between, 'us' and 'them', or, put another way, a dichotomy between 'public' and 'private' information.[22] These individual-centric conceptions of privacy imply

[20] Warren, S. D. and L. D. Brandeis (1890). "The right to privacy." Harvard law review: 193-220.
[21] Westin, A. F. (1967). "Privacy and Freedom, Atheneum." New York: 7.
[22] Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life, Stanford University Press.

that individuals controlled information about themselves and could 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. This approach to individual control over personal data or informational self-determination became a basis of the OECD Fair Information Principles (FIPs)[23].

The limitations of the informational self-determination model of privacy regulation have been highlighted with respect to the fundamental disconnect between privacy rights and obligations and the design of technical systems. Nissenbaum refers to privacy in terms of norms governing distinct social contexts, a framework she refers to as contextual integrity.[24] The term 'lateral privacy' was coined by Mulligan and King to describe the privacy-related harms that have arisen among users of social networking sites.[25] The authors argue that the harms experienced by users of a common platform (e.g. Facebook) are not covered by the dominant theory of privacy put forth by regulators - privacy as individual control. They argue that individual control offers little insight into the experiences of privacy violations claimed by users.

An alternative approach to conceptualizing privacy asserts that privacy regulation should be extended to address "social dynamics" viz. violations that users experience vis-à-vis each other while using a social networking platform such as Facebook. What it actually means to design privacy involves back-end software implementations (i.e. hidden from user) and front-end user interfaces (i.e. privacy user settings, notification, user consent etc.). However, while contextual-based data disclosure allows us to articulate information-sharing norms in a particular context, it offers no independent justification for privacy. As such, if we come to expect surveillance as the norm, then we no longer can argue that this is a privacy violation.[26]

It is important to appreciate that the above-noted conceptions of privacy rely on ex post analyses of purported privacy violations. We are considering actual harms in specific contexts when we make our assessment that a given event constitutes a violation of privacy. However, we argue that this approach leads to a culture of privacy compliance rather than responsibility for privacy protection. Basing our privacy regulations around the individual is important, but this leads to individuals making decisions that they cannot be meaningfully informed about. Individuals are in no position to assess the risk associated with disclosing personal information. This is particularly the case in the context of connected cars, where the market is complex and highly integrated.

Such an approach leaves unanswered the question of who should bear the risk associated with the privacy harms that were unforeseen by the service provider or the user when a new technological feature is implemented.

As Spiekermann observes, there are considerable challenges, including management commitment to integrating privacy into systems. This is due to the 'fuzzy' nature of the privacy concept – making it difficult to determine what is being protected. There is also no agreed upon methodology for

---

[23] Organisation for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sep. 23, 1980)
[24] Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life, Stanford University Press.
[25] Mulligan, D. K. and J. King (2011). "Bridging the gap between privacy and design." U. Pa. J. Const. L. 14: 989.
[26] Austin, L. (2003). "Privacy and the Question of Technology." Law and Philosophy 22(2): 119-166.

systematically integrating privacy into systems. Lastly, there is little knowledge of the tangible and intangible benefits of privacy protection and risks associated with a given company's privacy practices.[27] A common argument among car manufacturers is that the benefits of the connected cars in terms of safety outweigh the potential privacy harms. However, safety should not come at the expense of privacy since privacy may also be viewed as a safety issue. A concept of privacy that engenders risk would arguably provide a more meaningful discussion in the context of connected car technologies since we would be able to frame harm in terms of acceptable risks of re-identification.

4.2. Third party co-operation with law enforcement

In Part 1 we showed that a considerable amount of data in a given car's infotainment system may be accessed using vehicle forensics. Some of this data is innocuous, but there is a considerable amount of personal data that can be obtained. As connected car service providers may be asked to release information to police it is important that informed decisions on whether to voluntarily cooperate with police investigations. This can occur where the business is approached by police requesting voluntary disclosure of information on company's computers or networks. Such requests made by police are a combination of statutory provisions within the criminal code and PIPEDA.

Section 487.014 of the Criminal Code states: "For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing." Section 7(3)(c.1) of PIPEDA allows organizations disclose customer data without consent where "a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law." Clarity regarding what is meant by 'lawful authority' has been provided by the Supreme Court of Canada pursuant to R v. Spencer where the Court reasoned:

> The reference to "lawful authority" in s. 7(3)(c.1)(ii) must mean something other than a "subpoena or [search] warrant". "Lawful authority" may include several things. It may refer to the common law authority of the police to ask questions relating to matters that are not subject to a reasonable expectation of privacy. It may refer to the authority of police to conduct warrantless searches under exigent circumstances or where authorized by a reasonable law... As the intervener the Privacy Commissioner of Canada submitted, interpreting "lawful authority" as requiring more than a bare request by law enforcement gives this term a meaningful role to play in the context of s. 7(3) and should be preferred over alternative meanings that do not do so.[28]

While it is always within the rights of a third party (that is, not the target of the investigation) to require a warrant or production order, there are some circumstances which Canadian privacy law

[27] Spiekermann, S. (2012). "The challenges of privacy by design." Communications of the ACM 55(7): 38-40.
[28] R v. Spencer 2014 SCC 43, at para 71.

recognizes as appropriate, allowing for voluntary cooperation with police investigations without customer consent.

Section 7(3)(c.1)(ii) of PIPEDA grants businesses governed by that legislation the discretion (that is, the choice) to voluntarily cooperate with police investigations. However, this section of the Act is governed by the overall requirements set out in sections 3 and 5, which stipulate that the organization will only collect, use and disclose personal information for purposes that a "reasonable person would consider appropriate in the circumstances." What constitutes "reasonable" may change over time, a normative concept that varies with respect to what we find acceptable in keeping with the rule of law in a free and democratic society.

It is clear from R v. Spencer that police information requests must also comply with s. 8 of the *Charter of Rights and Freedoms*, which protects us against "unreasonable" search and seizure by state actors or other agents of the government. Individuals and organizations not acting on state business are not directly governed by the *Charter,* but the Supreme Court of Canada has noted consistently that all Canadian law should be interpreted in compliance with *Charter* values.

Nonetheless, this does not mean that what a reasonable person would consider appropriate limits to police powers is the same as what a reasonable person would consider an appropriate decision by a business faced with a police request for information. Reasonableness is always measured by its context. Canadian courts have held that where a business acted reasonably when disclosing information to police, this reduces the reasonableness of the target customer or employee's expectation that the business would not share that information to police without a warrant.

In other words, if a business is considered to have acted unreasonably if they voluntarily disclosed the information to police, then the customer's reasonable expectation that the business would ask for a warrant is stronger. Police would further likely need a warrant or production order in order to use this information in the investigation or prosecution of the crime, or else risk a *Charter* challenge.

Factors that Canadian appellate courts have found relevant to determining whether a business's decision to disclose customer information to police is reasonable in the circumstances include:

- The nature of the information requested (is it sensitive information?);
- The nature of the investigation (the seriousness of the crime under investigation, whether it directly implicates the facilities or service of the business);
- Contractual terms of service that give customers notice of the willingness of the business to cooperate with police investigations, especially where there has been an express violation of the terms of service. Employee policies on appropriate use of the organization's facilities or services can also serve this function.

Businesses need to analyze the sensitivity of the information being requested and assess whether the customer has a "reasonable expectation of privacy" in that information. Customer name and address are not generally considered sensitive information as it is regularly shared with third parties. However, where police are tracing the identity of a subscriber back from anonymous use, the subscriber's identity *is* sensitive information. It is unclear what information would require a warrant in the connected car context. It should be noted that while terms of service agreements that indicate a business will cooperate with the police may reduce the reasonable expectation of privacy of a

customer, it does not negate it since this depends on the nature and quality of the information shared with police.

The preceding discussion demonstrates a need for clear guidance regarding the scope of private sector voluntary co-operation with police requests generally and with connected car service providers in particular. In determining whether a business has acted reasonably in co-operating with police is a balance that businesses must strike between their legitimate business interests and the privacy interests of their customers. Guidance to the private sector in the form of a freestanding reasonableness requirement to balance these interests would assist in determining whether a business should voluntarily co-operate with a given police request.[29]

4.3. Privacy management codes of practice

At the present time, the focus of automakers' attention with respect to privacy protection is their customers. This is of course appropriate as they have a direct relationship. However automakers may also need to inform users of the data handling policies of partners with whom they share data. The sharing of data raises significant privacy concerns that the user is unlikely to be aware of. Framing the discussion as one of consumer choice and control over personal information that users are assumed to be informed about via a privacy statement is not a meaningful approach to privacy protection. As we have seen, 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 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.[30] 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.

4.4. Intelligent Transport System - Privacy Requirements

ITS will enable social interactions among vehicles, among drivers and between infrastructures and drivers/vehicles/pedestrians. The fact that vehicles will increasingly connect with each other and with public networks (e.g. V2V, V2I) makes it inevitable that nodes will exchange neighbourhood information on a regular basis. Thus, in the context of the social internet of vehicles, we will increasingly become concerned with privacy harms among users of the network. It will be necessary to determine in advance the degree of privacy that is appropriate in the circumstances and design the ITS system accordingly. An important task is to devise appropriate privacy preserving protocols, which are typically based on anonymity schemes, relying on temporary pseudonyms. Most of the privacy threat scenarios in relation to VANETs are related to position identifiers.[31] Dötzer has identified a number of privacy requirements to achieve adequate privacy in VANETs.

---

[29] Slane, A. (2013). "Privacy and Civic Duty in R v. Ward: The Right to Online Anonymity and the Charter-Compliant Scope of Voluntary Cooperation with Police Requests." Queen's LJ 39: 301.
[30] Spiekermann, S. and L. F. Cranor (2009). "Engineering privacy." Software Engineering, IEEE Transactions on 35(1): 67-82.
[31] Dötzer, F. (2005). Privacy issues in vehicular ad hoc networks. Privacy enhancing technologies, Springer.

1. It is possible to use pseudonyms as identifiers instead of real-world identities.
2. It is possible to change these pseudonyms.
3. The number of pseudonym changes depends on the application and its privacy threat model.
4. Pseudonyms used during communication can be mapped to real-world identities in special situations.
5. A set of properties and/or privileges can be cryptographically bound to one or more pseudonyms.[32]

In addition to these requirements user interfaces and usability would also need to be considered.

4.5. Independent Credentialing Authority

As VANETs further develop, there will likely be a need for a degree of technical standardization and regulatory harmonization in order to facilitate inter-operability between devices. If pseudonyms are used as part of VANETs there will be a need to create an independent credentialing authority that is trusted by customers, manufacturers, system operators and service providers. Such an authority would need to be created by statute and establish rules for 1) Initialization – when vehicles are initially set-up 2) Operation – during the major mode of operation and for credential revocation – pre-defining situations that can lead to revealing the real identity of the user.

Automakers that we interviewed cautioned against overly prescriptive 'unique to Canada' solutions since they operate in a North American market. This, they argue, will result in increased cost for consumers. However, it should be noted that privacy protection laws amongst countries may be based on similar principles; their enforcement and application vary considerably.[33] As Levin and Nicholson note, the EU and Canada centrally supervise the private sector's use of personal data, whereas the US regulation of the private sector is minimal.[34] This being the case, it may be possible to set up an independent credentialing authority that allows for decentralized domestic enforcement.

To guard against unauthorized use of data, the system's security architecture must be very carefully designed, especially if it is deployed between countries. Hubaux et al. have argued that because of the information it will protect, registration authorities must devise an appropriate public key infrastructure. They write that "this challenge is equivalent to securing credit cards or mobile phones, but it also includes newer, more difficult problems: it must embed security features in stringent real-time protocols such as those used to prevent accidents, secure physical location and distance, and support communication within highly sporadic groups of participants." [35]

---

[32] Ibid.
[33] Bennett, C. J. (1992). Regulating privacy: Data protection and public policy in Europe and the United States, Cornell University Press.
[34] Levin, A. and M. J. Nicholson (2005). "Privacy law in the United States, the EU and Canada: the allure of the middle ground." U. Ottawa Tech. Law J. 2: 357.
[35] Hubaux, J.-P., S. Capkun and J. Luo (2004). "The security and privacy of smart vehicles." IEEE Security & Privacy Magazine 2: 49-55.

Conclusion

The aim of this project has been to determine the privacy implications of vehicular digital forensics as applied to car infotainment systems. To this end, we assessed the information stored in an infotainment unit. The data obtained from an infotainment unit in an F-150 truck revealed a considerable amount of personal information.

That change is occurring in the automotive industry in the advent of infotainment, telematics and connectivity is beyond question. The issue is not whether the transition to connected cars and ITS will happen, but rather how we make this change happen in the most socially acceptable way.

Our survey research indicates that privacy will be an enabler of the connected car. The notice and consent model can be used in the context of ITS, but it is of limited application since additional warnings, choices and interruptions are likely to be more confusing than productive as people systematically under-estimate long-term privacy risks associated with the sharing of personal information. Such an approach is likely to result in ITS designers regarding privacy protection as an abstract problem that can be solved by a well-drafted privacy policy.

In this project, we argue that a risk approach to system design provides users with better privacy protection without the need to analyze and negotiate privacy policies. Such an approach would emphasize the use of pseudonyms and client-side storage and data processing.