2019-01-0479 Published 02 Apr 2019

Survey of Automotive Privacy Regulations and Privacy-Related Attacks

Mert D. Pesé and Kang G. Shin University of Michigan

Citation: Pesé, M.D. and Shin, K.G., "Survey of Automotive Privacy Regulations and Privacy-Related Attacks," SAE Technical Paper 2019-01-0479, 2019, doi:10.4271/2019-01-0479.

Abstract

Privacy has been a rising concern. The European Union has established a privacy standard called *General Data Protection Regulation* (GDPR) in May 2018. Furthermore, the Facebook-Cambridge Analytica data incident made headlines in March 2018. Data collection from vehicles by OEM platforms is increasingly popular and may offer OEMs new business models but it comes with the risk of privacy leakages. Vehicular sensor data shared with third-parties can lead to misuse of the requested data for other purposes than stated/intended. There exists a relevant regulation document introduced by the Alliance of Automobile Manufacturers ("Auto Alliance"), which classifies the vehicular sensors used for data collection as covered and non-sensitive parameters.

This paper reviews existing privacy standards as well as ongoing efforts in the automotive domain, and surveys the landscape of automotive privacy-related attacks which can be classified into three categories: *driver fingerprinting*, *location inferencing* and *driving-behavior analysis*. These three categories are derived from the aforementioned guidelines of covered information. Based on this survey, we define a *Privacy Score* (PS), quantifying the risk associated with each vehicular sensor. Sensors contributing to multiple privacy attacks will be assigned a higher PS. Furthermore, combinations of sensors used in privacy attacks must be considered and assessed in the PS metric as some attacks cannot be mounted using a single independent sensor alone.

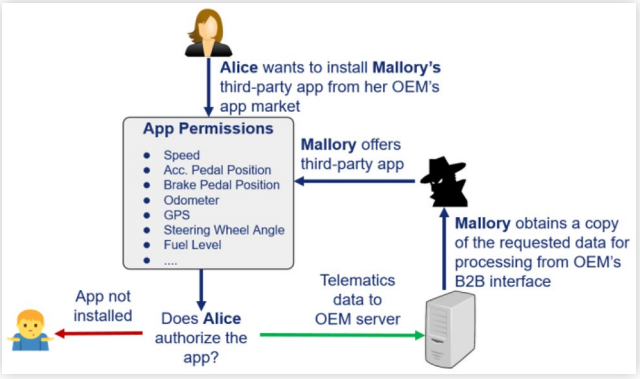
Introduction

Several OEMs have proposed data-collection platforms, such as the BMW *CarData* platform [1], in order to collect and store data on OEM servers and upon explicit users' consent to share data with third-party service providers through an "app store". The third-party must explicitly request certain parts of telematics data, such as the odometer reading, which is then securely collected from the in-vehicle network and transferred to the service provider's server which can then process the data in any way it wants. Fig. 1 depicts the proposed threat model related to the vehicular data-collection platforms.

Vehicular data collection and applications are of growing interest/importance to the public as well as businesses. As a result, both OEMs and third-party companies are in a race to develop data-collection platforms and build new business models to monetize the collected data. Besides offering the OEMs' own native services (e.g., remote unlocking, service notifications), these platforms also provide third-party apps to be installed and operate on vehicular data; for instance, insurance companies to analyze the driving behavior or fleet management for company vehicles. The growth of these apps accompanies increasing privacy concerns on sharing the driver's data with app developers and cloud services since the users must be sure to share their data with non-malicious or benign entities and know what data they are giving away and how it is used and stored. Therefore, privacy-preserving vehicular data collection is of growing concern to the public and has spawned many large-scale research efforts.

The rise of data collection and processing platforms based on vehicular telematics data leads to many research questions. Privacy of the vehicle owner's data is an important subject about which the US Government Accountability Office (GAO) released a document in July 2017. Furthermore, the Alliance of Automobile Manufacturers (AAM) have recently developed a set of privacy principles-the Privacy Principles for Vehicle

FIGURE 1 Threat model of Vehicular Data-Collection Platform



Technologies and Services ("Consumer Privacy Protection Principles") [2] which went into effect January 2, 2016. Among other principles, these guidelines encourage affirmative consent for collection of sensitive data, such as geolocation or driver behavior data. As a result, the platforms for vehicular data collection have to ask the users for their consent before collecting certain sensitive data on them.

These guidelines are a good starting point to address the issue of data privacy of car owners. To further evaluate this space, we investigate the implications of vehicle data privacy through possible attacks targeting *personally identifiable information* (PII) and ways to address possible weaknesses or vulnerabilities by using privacy-preserving mechanisms.

This paper makes the following contributions:

- Introduction of existing privacy regulations in the automotive domain and definition of covered information (vehicular data containing PII).
- Survey of the landscape of automotive privacy-related attacks targeting PII.
- Definition of Privacy Score (PS) to quantify risk of each independent vehicular sensor alone, and combinations thereof.

The paper is organized as follows. First, we will provide background on the relevance of automotive privacy. Then, we will introduce existing privacy regulations and derive privacy attack categories. For the aforementioned attack categories, we will list existing academic efforts. For evaluation purposes, we will assess the risk of 20 frequently collected sensors and other data (highlighted in Fig. 2) before concluding the paper.

Background

Before detailing privacy regulations, we present a brief overview of automotive data collection. Vehicular sensor data is collected from a set of Electronic Control Units (ECUs) in the vehicle. ECUs are interconnected by an In-Vehicle Network (IVN), usually Controller Area Network (CAN) bus which is pinned out to the OBD-II port of the vehicle. Some of the CAN data can thus be accessed by anyone through aftermarket dongles [14]. One example is usage-based insurance (UBI) dongles [15,16]. CarLab, an open-source software framework from the University of Michigan, collects OBD-II data to provide an interface for third-party app developers and researchers to conveniently build applications [13].

OEMs can also collect data from ECUs without the use of aftermarket dongles. Data is collected through the built-in telematics platform and shared with the OEM by an LTE connection. A recent Frost&Sullivan study [18] gives an overview of frequently used sensors and data for vehicular data-collection systems as depicted in Fig. 2.

We would also like to stress the significance of this research by showing the public acceptance. Figs. 3 and 4 from a recent McKinsey study [12] show that sharing vehicle data with third-parties - which our threat model is based on - is well accepted by consumers and they are also well aware of possible threats about sharing their private data with third parties.

It is also noteworthy that the acceptance of data sharing with third-party service providers rose in each surveyed market from 2015 to 2016. Although there are no figures for the following years as of the time of this writing, we expect

FIGURE 2 Most frequently collected sensors and privacy-related data

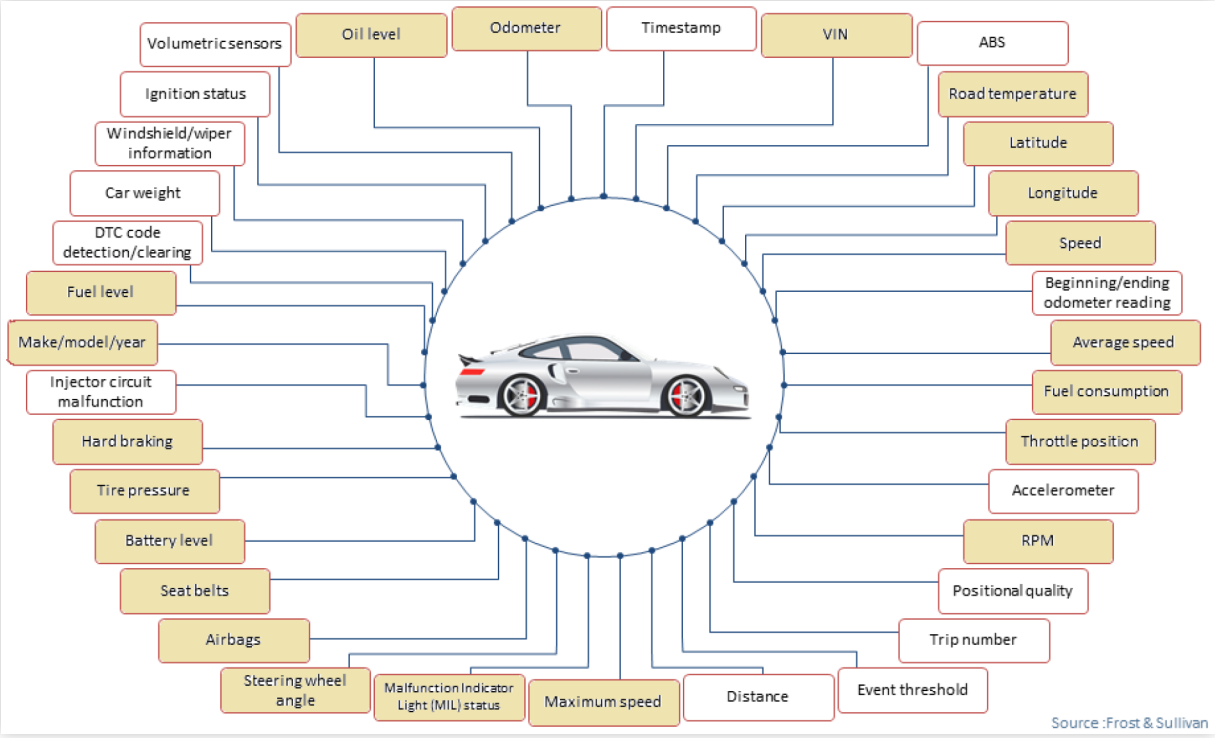


FIGURE 3 Willingness to share vehicular data [12]

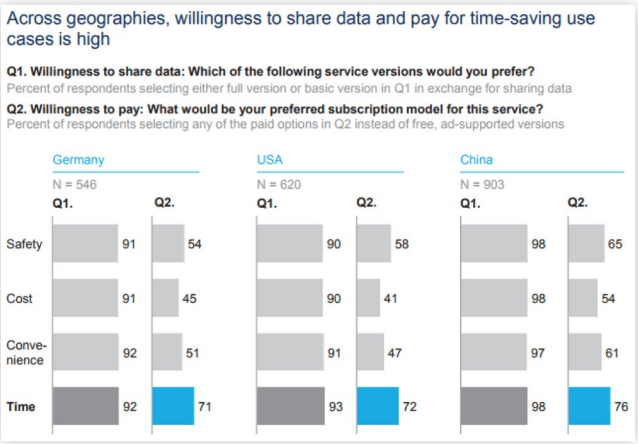
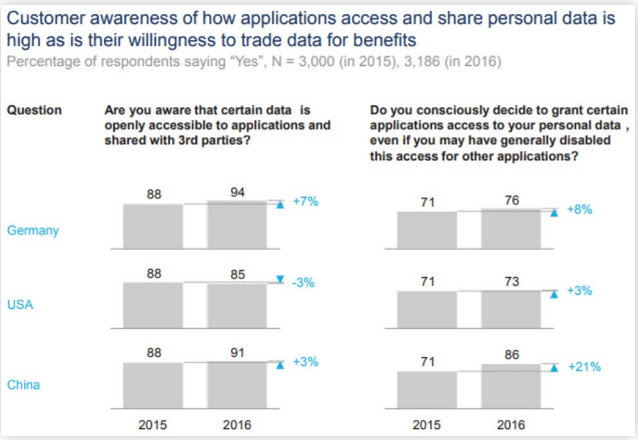


FIGURE 4 Awareness of third-party vehicular data sharing [12]



that with further awareness and market penetration of vehicular data-collection platforms, the acceptance levels will continue increasing. This makes vehicle privacy a very important R&D topic since attacks on drivers' privacy will become feasible, especially with lax privacy regulations as we will show next.

Privacy Regulations

Unfortunately, privacy regulation in the automotive domain is sparse since it is an emerging area. In this paper, we would like to point out the few existing privacy guidelines about vehicular data that can be taken as a starting point.

According to voluntary guidelines passed by the AAM [2], which are the main regulation document, there are three categories called "covered information" which the OEM must ask drivers for explicit permission:

- *Driving behavior*: Information about how a person drives a vehicle. Concrete examples stated in that document are vehicle speed, seat belt use, and information about braking habits. Information used only for safety, diagnostics, warranty, maintenance, or compliance purposes are explicitly ruled out.
- *Geolocation*: Information about the precise geographic location of a vehicle.
- *Biometrics*: Information about a vehicle owner's or registered user's physical or biological characteristics that can be used to identify the person.

As a result, the platforms for vehicular data collection must ask the drivers for their explicit consent before collecting this type of data from them. All other data can be theoretically collected and shared with third-parties without the driver's prior consent. These guidelines are a good starting point to address the issues with the permission models of the data-collection platforms, but they are not legally binding as of the time of this writing.

The US lawmakers were aware of vehicular privacy issues and introduced the Driver Privacy Act of 2015 as part of the comprehensive FAST Act [19]. This bill covers how to deal with sensitive driving data retrieved from event data recorders (EDR) for crash analysis and traffic safety research and does not cover data-collection platforms that have different purposes and capabilities. While EDRs are only required to record and share crash-related data in a limited time frame before and after the crash, the data-collection platforms from OEMs and third-party companies provide time-series data [11] giving a potential attacker more possibilities to compromise drivers' privacy, such as their entire location or speed trace.

There is a need to identify sensors which contribute to these categories by analyzing existing/proposed attacks. The attacks contributing to these three categories would be driver fingerprinting, location inferencing, and driving-behavior analysis, respectively.

Privacy Attacks

Driver Fingerprinting

Driver fingerprinting is one of the most common vehicular privacy-related research subjects. The goal behind this attack is to distinguish different drivers using the same car by analyzing vehicular sensor data during trips. It has been shown in [5] that using 15 sensors, it was possible to identify 15 different drivers with 100% accuracy. Other similar work has been done in [8,21,22]. The authors of [7] showed how drivers can be distinguished before even starting their trip. The main privacy issue behind fingerprinting drivers is to conclude that different drivers than the main (authorized) driver have used that vehicle. Especially automotive insurance companies are interested in this information since this might violate their terms and/or lead to a change in the insurance premium. Usage-based Insurance (UBI) companies are already offering OBD-II dongles for their customers who can optionally enroll in a program to save on their premium by driving safely [15,16,17,20]. The dongles collect vehicular OBD-II data which is transferred to the insurance companies'

data centers and then analyzed for driving behavior, such as speeding or hard braking. Insurance companies could also use this data to distinguish between drivers as shown in the aforementioned papers. If the third-party is authorized for analyzing driving behavior only, the use of the collected data for another purpose, such as fingerprinting, will only be allowed upon explicit permission of the driver. Although insurance companies can be regarded as a trusted third-party, under an honest-but-curious threat model, we cannot exclude any misuse of the data by UBI companies. UBI companies are also planning to be part of OEM data-collection platforms in the future [23], which will extend further the pervasiveness of this attack category.

Location Inferencing

Another attack category is location inferencing. To this date, little has been done to infer user location based on vehicular data. This might be due to the lack of relevance since vehicular data collection has not become a major focus of attention until summer 2017, although it has always been possible to collect vehicular data for research through the OBD-II port. It has been shown that traveled routes of the user can be inferred by merely using the speed trace of a trip [9,10,11]. We believe that this also is possible by using other vehicular sensors such as steering wheel angle. Since speed is part of the "covered information" from aforementioned privacy guidelines, a location- inferencing attack under the proposed threat model in Fig. 1 might not work as easily as an attack using steering wheel angle readings since explicit consent for the speed parameter might deter drivers from installing a dubious third-party app. Furthermore, the Vehicle Identification Number (VIN) parameter can be leveraged as side-channel information to obtain knowledge about the rough location through dealership or service shop records which can be found by querying the VIN on online websites such as vehiclehistory.com [6].

Driving-Behavior Analysis

Finally, vehicular data is so rich that individual driving behavior can be analyzed. As already mentioned, this is done by various insurance companies to adjust the premium rate. In order to preserve drivers' location privacy, these companies prefer collection of a range of other sensors. Table 1 gives an overview of major UBI companies and the data they collect for driving-behavior analysis.

Another application is to detect distracted or drunk driving [3,4].

Risk Assessment

Based on the survey of privacy attacks presented above, we need to quantify the privacy risk of each sensor. For this evaluation, we use the highlighted sensors from Fig. 2. Table 2 shows a matrix of the contribution of each sensor to the aforementioned attacks. Since some attacks are also possible through a combination of multiple sensors, we need to consider the pairwise correlation of sensors contributing to an attack category. Each entry in the matrix consists of a 3-tuple of following syntax:

$$\begin{pmatrix} Driver\ Fingerprinting, Location\ Inferencing, \\ Driving\text{-}Behavior\ Analysis \end{pmatrix} \quad (1)$$

If a sensor combination contributes to an attack category, it is denoted with logic value 1 in the respective position; 0 otherwise. The diagonal entries of the symmetric matrix denote the case when only a single independent sensor is sufficient to be used in an attack category.

Privacy Score

The Privacy Score (PS) is a metric defining the privacy risk associated with data from a specific vehicular sensor. This parameter is defined through extensive literature survey of the three attack categories on user privacy using vehicular data which is summarized in Table 2. Based on this matrix, we can define PS_k for sensor k as a value ranging from 0 to 1, with 0 denoting no privacy risk associated to that sensor and 1 maximum privacy risk. The latter would mean that a sensor contributes to all three attack categories not only by itself, but also in pairwise combinations with all other sensors.

Let N be the number of sensors which our vehicular data-collection system can report. In our example, $N = 20$. For each sensor $k = \{1,\ldots,N\}$ an entry in the row (or column since the matrix is symmetric) of this sensor is a 3-tuple $c^i_{k,j}$, with i denoting the attack category ($i = 1,2,3$) and j denoting the other sensor ($j = 1,\ldots,N$), respectively. For the sake of generalization, we want to assign weights w_i for each attack category. The architect of a privacy-protection scheme might use different weights to prioritize the relevance of an attack category. The Privacy Score PS_k for a sensor k can thus be defined as:

$$PS_k = \frac{\sum_i \sum_j w_i\, c^i_{k,j}}{N \sum_i w_i} \quad (2)$$

TABLE 1 Data collection of UBI companies

Company	Mileage	Speed	Acceleration	Hard Braking	Turns
Progressive [15]	✓	✓		✓	
State Farm [17]	✓	✓	✓	✓	✓
Allstate [16]	✓	✓		✓	
Esurance [20]		✓	✓	✓	

© 2019 SAE International. All Rights Reserved.

TABLE 2 Risk assessment for 20 most frequently collected sensors and privacy-related data

	Odometer	VIN	Outside Temperature	GPS	Current Speed	Average Speed	Maximum Speed	Fuel Consumption	Throttle Position	RPM	Steering wheel angle	Airbag status	Seat belt status	Battery level	Tire pressure	Hard braking	Make/model/year	Fuel level	Check engine light on	Oil level
Odometer	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/1	0/0/0	0/0/1	0/0/1	0/0/0	0/0/1	0/0/0	0/0/0
VIN	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Outside Temperature	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Location (GPS)	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1
Current Speed	0/1/0	0/1/1	0/1/0	1/1/1	0/1/0	0/1/0	0/1/0	1/1/0	0/1/1	0/1/1	0/1/1	0/1/0	0/1/1	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0
Average Speed	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Maximum Speed	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Fuel Consumption	0/0/1	0/0/1	0/0/0	1/1/1	1/1/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0
Throttle Position	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/1	0/0/0	0/0/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
RPM	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Steering wheel angle (SWA)	0/1/0	0/1/0	0/1/0	1/1/1	0/1/1	0/1/0	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0
Airbag status	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
Seat belt status	0/0/1	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/1	0/0/0	0/1/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
Battery level	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Tire pressure	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Hard braking	0/0/1	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/1/1	0/0/1	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Make/model/year	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Fuel level	0/0/1	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0
Check engine light on	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Oil level	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0

© 2019 SAE International. All Rights Reserved.

TABLE 3 Privacy Scores (PS) and Normalized Privacy Scores (NPS) for 20 most frequently collected sensors

Vehicular Sensor	Privacy Score (PS)	Normalized Privacy Score (NPS)
Odometer	0.17	0.10
VIN	0.12	0.04
Outside Temperature	0.08	0.00
Location	1.00	1.00
Current Speed	0.48	0.43
Average Speed	0.08	0.00
Maximum Speed	0.08	0.00
Fuel Consumption	0.18	0.11
Throttle Position	0.15	0.08
RPM	0.15	0.08
Steering wheel angle	0.42	0.37
Airbag status	0.12	0.04
Seat belt status	0.17	0.10
Battery level	0.08	0.00
Tire pressure	0.10	0.02
Hard braking	0.18	0.11
Make/model/year	0.10	0.02
Fuel level	0.12	0.04
Check engine light on	0.08	0.00
Oil level	0.08	0.00

In what follows, we apply Eq. (2) to the values in Table 2. In our example, we do not prioritize any attack category and thus assign $w_1 = w_2 = w_3 = 1$. All PS values are rounded to two digits:

Discussion

According to the calculated Privacy Score (PS) in Table 3, the top 3 of the riskiest sensors regarding privacy consist of location, current speed, and steering wheel angle. One thing all these three sensors have in common is that they are contributing to at least one attack category by themselves without the need of any other sensor. The riskiest sensors which need at least another sensor in combination to contribute to an attack category are fuel consumption and hard braking. The former can be leveraged as side-channel information for location-inference attacks whereas the latter is used in driving-behavior analysis. The sensors with the least privacy risk are outside temperature, average speed, maximum speed, battery level, check engine light on, and oil level. These sensors have the minimum possible score possible since only in combination with the top 3 riskiest sensors, they contribute to the PS according to the definition in Eq. (2). In order to eliminate this effect, we calculate a Normalized Privacy Score (NPS):

$$NPS_k = \frac{PS_k - \min(PS)}{\max(PS) - \min(PS)} \tag{3}$$

In this equation, PS is denoting the vector of all N Privacy Scores, PS = (PS_1, … ,PS_N). All NPS values are included in Table 3 as well.

Summary/Conclusions

This paper surveyed vehicle privacy regulations and the landscape of privacy attacks. Due to increasing pervasiveness of vehicular data- collection platforms, the likelihood of attacks on drivers' private information is rising as well. We introduced a possible threat model and showed the need of continuously improving currently existing privacy regulations in the automotive domain to prevent attacks on drivers' privacy. We identified three main attack categories and described existing work for each category. Finally, we assessed the risk connected with 20 vehicular sensors and other privacy-related data by systematically compiling the affected sensors for each attack into a matrix. The definition of a metric called *Privacy Score* (PS) allowed us to draw conclusions about the riskiest vehicular sensors. Besides other possible metrics such as third-party trustworthiness score, the latter shall be taken into consideration while designing a privacy-protection scheme for vehicular data since they can leak the most relevant information about a driver. Third-party apps requesting sensitive sensors such as GPS or speed must be treated differently than apps that are monitoring the fuel consumption. As a result, PS can be leveraged as an input parameter for several privacy frameworks, such as Differential Privacy. The larger the PS, the larger is the amount of noise that is added to the original signal to distort it. It might also be possible to reduce the sampling rate of sensors with a higher PS while sharing them with a third-party service provider. All in all, we expect the introduced *Privacy Score* metric to become an important parameter in future automotive privacy-protection frameworks which will again be an inevitable component of future vehicles that will be increasingly connected.

References

1. BMW Group launches BMW CarData: new and innova-tive services for customers, safely and transparently, May 2017, https://www.press.bmwgroup.com/global/article/detail/T0271366EN/bmw-group-launches-bmw-cardata:-new-and-innovative-services-for-customers-safely-and-transparently?language=en.
2. VEHICLE DATA PRIVACY Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role, July 2017. http://www.gao.gov/assets/690/686284.pdf.
3. Chen, S.H., Pan, J.S., and Kaixuan, L., "Driving behavior Analysis Based on Vehicle OBD Information and Adaboost Algorithms," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, 18-20, 2015.
4. Li, Z., Bao, S., Kolmanovsky, I.V., and Yin, X., "Visual-Manual Distraction Detection Using Driving Performance

Indicators with Naturalistic Driving Data," *IEEE Transactions on Intelligent Transportation Systems*, 2017.

5. Enev, M. et al., "Automobile Driver Fingerprinting," *Proceedings on Privacy Enhancing Technologies* 1:34-50, 2016.
6. Research Any Vehicle In Seconds, VehicleHistory.com - Vin Check Vehicle History with Our Free Vin Lookup and Make Model Year Search Tools, accessed October 02, 2018, https://www.vehiclehistory.com/
7. Kar, Gorkem, Jain Shubham, Gruteser Marco, Chen Jinzhu, Bai Fan, and Govindan Ramesh, "PredriveID: Pre-Trip Driver Identification from In-Vehicle Data," in *Proceedings of the Second ACM/IEEE Symposium on Edge Computing*, 2, ACM, 2017.
8. Bo, W., Panigrahi, S., Narsude, M., and Mohanty, A., "Driver Identification Using Vehicle Telematics Data," SAE Technical Paper 2017-01-1372, 2017, doi:10.4271/2017-01-1372.
9. Dewri, R., Annadata, P., Eltarjaman, W., and Thurimella, R., "Inferring Trip Destinations from Driving Habits Data," in *Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society*, 267-272, ACM, November 2013). .
10. Gao, X., Firner, B., Sugrim, S., Kaiser-Pendergrast, V., Yang, Y., and Lindqvist, J., "Elastic Pathing: Your Speed is Enough to Track You," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 975-986, ACM, September 2014.
11. Zhou, L., Chen, Q., Luo, Z., Zhu, H., and Chen, C. (June 2017). Speed-Based Location Tracking in Usage-Based Automotive Insurance, in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, 2252-2257, IEEE.
12. McKinsey & Company, Monetizing car data: New service business opportunities to create new customer benefits September, September 2016.
13. Pesé M. D., Ganesan A., and Shin K. G., "CarLab: Framework for Vehicular Data Collection and Processing," October 2017, 43-48.
14. OBD - Elm Electronics, "Small Solutions from Elm Electronics," www.elmelectronics.com/products/ics/obd/.
15. Progressive, "What Is Snapshot and How You Can Save," www.progressive.com/auto/discounts/snapshot/.
16. Drivewise - Allstate, "Allstate," https://www.allstate.com/drive-wise/drivewise-device.aspx.
17. Drive Safe & Save™ - State Farm®, "State Farm," https://www.statefarm.com/insurance/auto/discounts/drive-safe-save.
18. Frost & Sullivan, "Automotive Data Monetisation Pricing and Business Models," http://www.frost.com/c/10046/sublib/frost-content.do?sheetName=report-overview&sheetGroup=MD48-01-00-00-00&viewName=virtual-brochure&repid=MD48-01-00-00-00.
19. D & R. (2015, December 04). Text - H.R.22 - 114th Congress (2015-2016): FAST Act. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-H7E76328B2CD946219201C9FF6470C491.
20. Esurance Insurance Company, Esurance, 2018, Accessed October 02, 2018, https://www.esurance.com/drivesense.
21. Ezzini, S., Berrada, I., and Ghogho, M., "Who is Behind the Wheel? Driver Identification and Fingerprinting," *Journal of Big Data* 5(1):9, 2018.
22. Corbett, Cherita, Alexis Jimmy, and Watkins Lanier, "Who's Driving You?," *Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual*, 1-4, *IEEE*, 2018.
23. BMW CarData, A sign of things to come for all OEMs, n.d., Retrieved from https://www.ptolemus.com/blog/bmw-cardata-a-sign-of-things-to-come-for-all-oems/.

Contact Information

Mert D. Pesé, M.Sc.
University of Michigan
4956 Beyster Building, 2260 Hayward St.
Ann Arbor, MI 48109-2121, U.S.A.
mpese@umich.edu

Kang G. Shin, Ph.D.
University of Michigan
4605 Beyster Building, 2260 Hayward St.
Ann Arbor, MI 48109-2121, U.S.A.
kgshin@umich.edu

Definitions/Abbreviations

OEM - Original Equipment Manufacturer
OBD-II - On-board Diagnostics Protocol v2
PS - Privacy Score
NPS - Normalized Privacy Score
PII - Personally Identifiable Information
IVN - In-Vehicle network
CAN - Controller Area Network
LTE - Long-Term Evolution
EDR - Event Data Recorder
VIN - Vehicle Identification Number
RPM - Revolutions per minute, engine speed
UBI - Usage-based Insurance
SWA - Steering wheel angle
GPS - Global Positioning System

ISSN 0148-7191