5-Anon: Privacy for Connected Vehicles

May 18, 2022

Brijesh Mishra,Naveen Janarthanan  
Umesh Tanniru, Jose Valadez, Harrison Pierce

Intro and/or Abstract

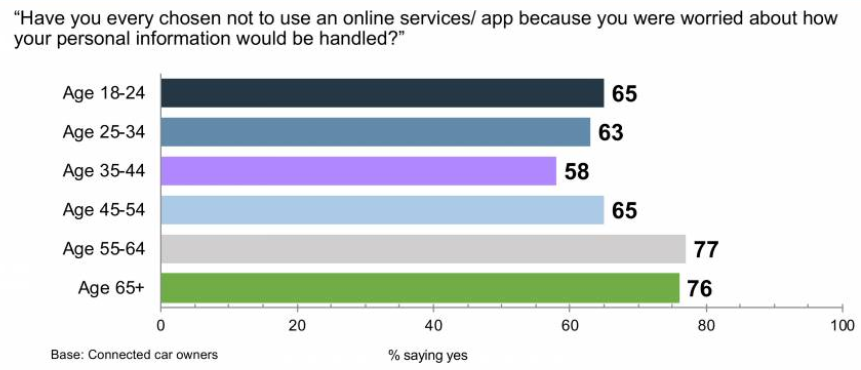
As the world becomes increasingly connected, so do our cars – but greater connectivity equates to more data, privacy, and security concerns. Modern vehicles often contain hundreds of Electronic Control Units (ECUs) communicating over internet-connected networks, and sharing information about drivers, their behavior and surroundings.

Problem Statement

Automobile manufacturers are re-inventing themselves and becoming more like software driven companies. Connected vehicles, as these new generations of vehicles are called, collect data by design about the car, driver, ride, and its surroundings. [1]According to AAA, an average connected vehicle could generate 380 TB to 5100 TB of data in just one year while driving 17,600 minutes on average.

Owner information is required and is received by vehicle manufacturers with the owner’s permission upon signing purchase contracts. Vehicle diagnostic data like powertrain and emission related information may not create data privacy issues directly; however if this data is published publicly or shared with 3rd parties, it can pose identity disclosure issues indirectly. Other sensors found on the vehicle assist with driver behavioral data like speed of the vehicle, when sudden brakes are applied, etc.

Many drivers are unaware of the data that is collected by vehicle manufacturers. According to a survey [2] done among drivers within ages of 18-65+, people of all ages raised suspicion about their personal information being handled appropriately by online services.



*This survey points out that drivers are concerned about data privacy.*

In a different survey, drivers were surveyed about their interest in new services using the collected data. Results were mixed, with only 33% of respondents trusting 3rd party partners. According to an article [3] in “The New York Times” dated May 20, 2019, cars know everything about you, including your weight, driving speeds, where you live and even your financial information.

To sum up, connected vehicles collect data by design about the vehicle, driver, driving dynamics, and its surroundings. Data collection is not clearly mentioned to the users upon vehicle purchase. To make matters worse, vehicle manufacturers do not easily allow customers the flexibility and control over data collection measures. So, what options do drivers have to protect their privacy? What can vehicle manufacturers do to raise confidence in vehicle owners about the data custody that they have?

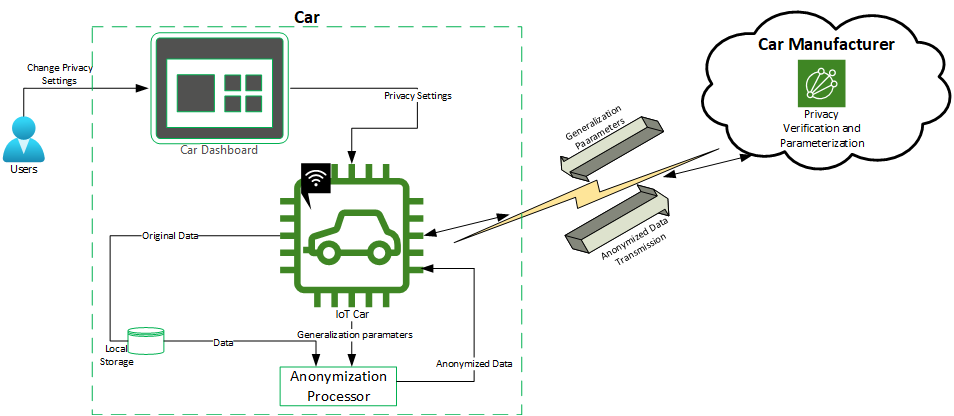
Approach

Our approach to solving this problem is to implement a user-friendly privacy settings dashboard within the vehicle’s on-board computer that would allow the owners of the vehicle to control what sensitive groups of data should be anonymized prior to the data getting sent to the car manufacturer in an effort to maintain privacy. With this approach, only anonymized data would be sent to the car manufacturer. The image below is a sample of what the privacy settings dashboard could look like, with the main sensitive groups of data identified.



*Representation of a “Privacy Settings” on the Car Dashboard*

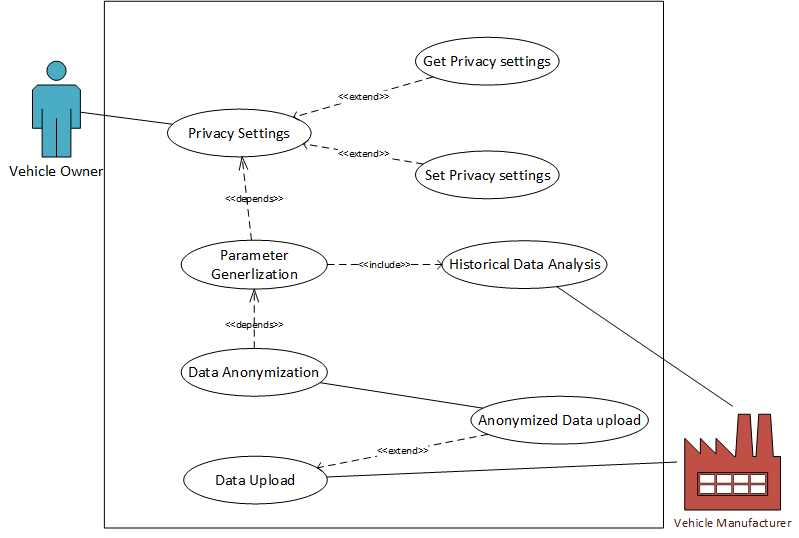
At a high level, the anonymization takes place locally within the vehicle based on the user defined privacy settings. Whenever the vehicle manufacturer requests data from the vehicle, it will send a predetermined set of parameters/recommendations for anonymization based on the user’s privacy settings. The vehicle will process the locally stored raw data from within the Anonymization Processor found within the vehicle with the given generalization parameters from the manufacturer. The anonymized dataset is then sent back to the vehicle manufacturer, where it will be aggregated with other vehicles’ data into one large dataset.



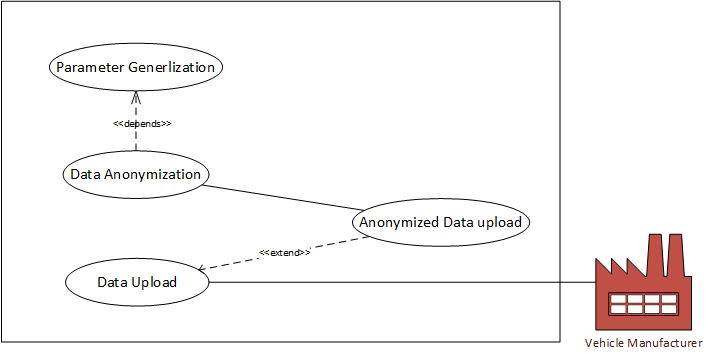
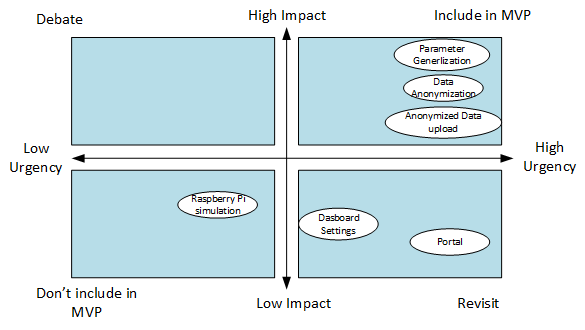
*Representation of our proposed data anonymization implementation process*

This process is cyclical and happens on a regular schedule determined by the car manufacturer. As needed, the vehicle manufacturer will be able to send updated generalization parameters to the vehicle via software updates to improve the anonymization process and maintain privacy threshold compliance. Additionally, R&D in the future would likely introduce improved algorithms/processes that could improve the overall data anonymization, which can also be completed via over-the-air updates to the vehicles.

Use cases



MVP/Prioritized Use Cases

Benefits of Solution

Existing automotive privacy solutions do not properly consider car owners’ privacy needs. The privacy dashboard solution allows vehicle manufacturers to create effective data privacy processes, which will improve compliance with future car privacy standards. Consumers can use this privacy dashboard to take control of their privacy by privatizing specific data groups before the data even leaves the car. Car manufacturers can continue to collect data for R&D purposes, while gaining customers’ trust and respect.

SWOT Analysis

| STRENGTH   * Anonymization at the data origin * Vehicle owner controls their Identity and other associated information privacy * Protects against privacy threats (membership disclosure, identity disclosure, attribute disclosure) via privacy engineering techniques * Approach is scalable for every car model/manufacturer | WEAKNESS   * Car manufacturer adaptation * Determining privacy thresholds for anonymization - to ensure privacy is maintained for customer satisfaction |
| --- | --- |
| OPPORTUNITY   * Increased awareness for privacy of data from consumers * Connected vehicles being treated as technology, which will require privacy methods/techniques to be implemented to comply with evolving vehicle regulations in the near future | THREATS   * Car manufacturers not collecting driving behavior data from user vehicles - highly unlikely this will materialize, as data is essential for R&D for future developments * Regulations permitting data collecting without any anonymization techniques - due to rapid tech developments in the automotive space, government agencies have not been able to identify data privacy rules in the automotive space |

Competitive Analysis

There are 3 competitive products available in the market that provide privacy for automotive data but none of them provide consumers the control over their personal data as well as all of those operate after the fact.

**Celanture**[4] offers a fully-automated anonymization solution for images and videos to comply with privacy law. They anonymize the RGB-imagery (both still images and videos). The anonymization quality rate is up to 99%. One drawback we found with this solution was that this has to be implemented at the manufacturer's cloud thereby taking the raw data out of vehicle owner’s control.

**sioSHIELD**[5] offers switchable privacy for connected vehicles. The idea behind this solution is to avoid distraction by infotainment contents on the dashboard for the driver while driving. This solution lets owners switch between public and private modes. Navigation and other car relevant information can be displayed in public mode (visible to driver and passenger). The entertainment is displayed in public mode that allows only the passenger/s to view the content.

**Privacy4cars**[6] provides solutions to delete your personal data, safeguard your identity and assert your data rights. It lets you delete your personal data before selling your vehicle, returning a lease or dropping off a rental.

End of Semester Deliverables

The deliverable for our project would include a proof of concept that includes

1. An application simulating car dashboard allowing user to change their privacy settings
2. Anonymization processor that would take anonymization parameters from simulated car manufacturer
3. A database or a portal where anonymized data would be uploaded
4. Threat Model
5. Additional documentation/training material as deemed necessary

References

[1] “Data Privacy in Autonomous Vehicles - Can Anonymization Solve The Problem? - Blickfeld,” Jan. 28, 2022.<https://www.blickfeld.com/blog/data-privacy-in-autonomous-vehicles/> (accessed Apr. 15, 2022).

[2] “OtonomoPrivacyPaper.pdf.” Accessed: Apr. 15, 2022. [Online]. Available:<https://fpf.org/wp-content/uploads/2020/01/OtonomoPrivacyPaper.pdf>

[3]“Opinion | Your Car Knows When You Gain Weight - The New York Times.”<https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html> (accessed Apr. 15, 2022).

[4] Who will take care of Data Privacy on Autonomous Vehicles?

[Celantur - Automated Data Anonymization for Photos and Videos](https://www.celantur.com/)

[5] Switchable privacy for automotive - display information in public and private mode <https://www.sioptica.com/solutions/>

[6]Privacy4Cars

https://privacy4cars.com/personal-use/