

MASTER THESIS

# Conceptualization of an automotive interface for self-controlled privacy in a connected car

**Nupur Aggarwal**  
Interaction Design M.Des. (2015 -17)

**Supervisor**  
Prof. Dr. -Ing Ralph Bruder

**Project Guide**  
M.Sc. Jonas Walter

**Supervisor**  
Prof. Dr. Gaur G. Ray

**Project Guide**  
Prof. Dr. Sugandh Malhotra



# Acknowledgement

I would like to thank Prof. Gaur G. Ray for his supervision and initiation into the project and the efforts he has put for successful integration of this semester exchange into the M.Des. curriculum and for providing me with the opportunity to carry out my thesis at TU Darmstadt. It is only possible because of the efforts to develop an exchange of knowledge and culture between IAD at TU Darmstadt and IDC at IIT Bombay. I would also like to thank Prof. Sugandh Malhotra for being my project supervisor and giving his valuable inputs in this project and in the organisation of the overall programme. I would sincerely thank IDC and IIT Bombay for providing with an opportunity to carry out this semester exchange which would not be possible otherwise.

I thank Prof. Dr. -Ing Ralph Bruder for extending his generous invitation and supervising the project at IAD. My deepest gratitude goes to M.Sc. Jonas Walter who agreed to guide me through the entire project and his relentless and cautious guidance towards the thesis. Without his guidance the project could not have materialised. My genuine thanks to M.Sc. Christopher Stockinger who ensured a great organisation of the programme and helped me manage the overall stay. I also extend my thanks to all the colleagues at IAD, especially Katharina, who have been supportive throughout my work. Thanks to the Tutor International group for ensuring a smooth inculcation into the university and a very friendly start. Also the international office at TU Darmstadt, especially Ms. Pia Schmitt and the overall organisation at TU Darmstadt for encouraging a student exchange such as this.

I would like to thank DAAD for this IIT Master Sandwich program Scholarship, and Ms. Anuroopa Dixit for giving me this opportunity to study at TU Darmstadt and provide with all possible means. I would extend my regards to my friend and colleague, Dhruv Soni, for helping me proof read and improve my report, and also provide with the motivation, without whom this would not have been possible. Lastly, I would like to thank everyone involved in this exchange program, my friends and family for the kind of support one would require to complete a semester abroad.

June 2017

**Nupur Aggarwal**

Interaction Design M.Des. (2015 -17)

**IDC IIT Bombay**

iaD

Technische Universität Darmstadt  
Institut für Arbeitswissenschaft

## Masterthesis

---

**Conceptualization of an automotive interface for self-controlled  
privacy in a connected car**

Nupur Aggarwal

---

## Summary

---

Modern day connected cars equipped with infotainment and telematics systems that can collect substantial amounts of sensitive data and various smartphone applications as well as manufacturers and service providers have access to a huge pool of data that can be transmitted from a car that contains private information. There is a need for an application that can help users control their privacy by making informed decisions about the data that they are going to share.

The user studies conducted by FIA and IAD are referred to formulate a catalogue of Requirements for the design of such an app, and the technical requirements of making a vehicular HMI are derived from existing literature. Then a UX-design approach is followed to create a concept that allows users to quickly select pre-defined settings based on recommendations from an internal privacy scale that rates applications based on their frequency and volume of data sharing and it also lets users make customized settings for providing data access to applications.

Finally the prototypes of the concept are developed and tested for their ease of use and usability parameters. Some parameters are suggested for future testing in a simulated driving environment, as the application will be used in both driving and non driving situations. A smartphone application is also developed to help make the privacy settings on the go.

A comparative study between Indian and German privacy views reveals that the concept is easily implementable in India as the privacy concerns are largely similar and both the places are ready to have more control over their privacy settings.

## Practitioner Summary

Following a human-centered design approach to formulate a concept for an interface for self-controlled privacy in a connected car, based on the user's view on privacy and data sharing. It allows the user to select between pre-defined privacy settings or customize settings based on privacy recommendations.

---

## Table of contents

---

<b>LIST OF FIGURES</b> .....	<b>IX</b>
<b>LIST OF TABLES</b> .....	<b>XI</b>
<b>LIST OF ABBREVIATIONS</b> .....	<b>XII</b>
<b>1 INTRODUCTION</b> .....	<b>1</b>
<b>2 LITERATURE REVIEW</b> .....	<b>2</b>
2.1 WHAT IS A CONNECTED CAR.....	2
2.2 PRIVACY IN A CAR.....	2
2.3 SELF CONTROLLED PRIVACY IN A VEHICLE.....	4
2.3.1 <i>Overview of norms on vehicular interface design</i> .....	5
2.3.2 <i>Overview of user opinion on connected cars</i> .....	6
2.3.3 <i>Overview of user opinion on privacy in connected cars</i> .....	8
<b>3 REQUIREMENTS CATALOGUE</b> .....	<b>10</b>
<b>4 METHODOLOGY</b> .....	<b>18</b>
4.1 REQUIREMENTS REVIEW AND USER PERSONA.....	18
4.2 BRAINSTORMING AND MIND MAPPING.....	18
4.3 INFORMATION ARCHITECTURE.....	19
4.4 PAPER PROTOTYPING.....	20
4.5 DIGITAL HI-FIDELITY PROTOTYPES.....	20
4.6 USER TESTING OF DIGITAL HI-FIDELITY PROTOTYPE.....	21
4.7 ITERATIONS TO DIGITAL PROTOTYPE.....	23
4.8 USER INTERFACE DESIGN AND INTERACTIVITY.....	23
4.9 USER TESTING FOR APPLICATIONS DESIGN.....	23
<b>5 RESULTS</b> .....	<b>25</b>
5.1 REQUIREMENTS REVIEW AND PERSONA.....	25
5.2 BRAINSTORMING AND MIND MAP.....	27
5.3 INFORMATION ARCHITECTURE.....	28

5.4	PAPER PROTOTYPES .....	31
5.5	DIGITAL HI-FIDELITY PROTOTYPES .....	33
5.6	USER TESTING OF DIGITAL HI-FIDELITY PROTOTYPE.....	37
5.7	ITERATIONS TO DIGITAL PROTOTYPE .....	42
5.7.1	<i>Locating the duration option.....</i>	42
5.7.2	<i>Making the pre-defined settings discoverable .....</i>	43
5.7.3	<i>Starting the custom settings with pre-sets.....</i>	43
5.8	USER INTERFACE DESIGN.....	44
5.9	USER TESTING FOR APPLICATIONS.....	47
<b>6</b>	<b>CONCLUSION AND DISCUSSION .....</b>	<b>48</b>
6.1	REQUIREMENTS CATALOGUE ANALYSIS .....	48
6.2	NEXT STEPS FOR TESTING AND FUTURE SCOPE.....	61
6.3	PRIVACY CONCERNS IN INDIA VS GERMANY VS REST OF THE WORLD .....	62
6.3.1	<i>India .....</i>	62
6.3.2	<i>Germany.....</i>	64
6.3.3	<i>Anonymous Users – All over the world.....</i>	67
6.4	CONCLUSION.....	70
	<b>BIBLIOGRAPHY .....</b>	<b>LXXII</b>
	<b>APPENDIX .....</b>	<b>LXXIV</b>
A	COLOUR SPECIFICATIONS CHART FOR FOREGROUND AND BACKGROUND COLOUR IN THE VEHICLE HMI .....	LXXIV
B	QUESTIONS FOR SEMISTRUCTURED INTERVIEW.....	LXXV

---

## List of figures

---

Figure 1: Where the types fall on a scale of interest in connected cars versus concern about data security .....	7
Figure 2: A typical user persona relating to his views on privacy in connected cars .....	21
Figure 3: Brainstorming using keywords based on privacy and connected cars.....	22
Figure 4: Mind map for possible ideas for the privacy application .....	22
Figure 5: Information architecture for the application .....	23
Figure 6: Initial prototype for determining the information architecture .....	24
Figure 7: Paper prototype 1 .....	25
Figure 8: Paper prototype 2.....	26
Figure 9: Interactive screens using pull out men .....	26
Figure 10: The two available displays .....	17
Figure 11: Home creen for digital prototype .....	27
Figure 12: Sign up screen for digital prototype .....	27
Figure 13: Different profiles of users can be created, or used as guest for digital prototype .....	28
Figure 14: The main homepage for digital prototype with option to switch off data sharing, select pre-defined settings or go to custom settings. .	28
Figure 15: Information on the modes by clicking on them, for digital prototype.....	29
Figure 16: "Next step" Duration, for digital prototype .....	29
Figure 17: Home page for custom settings for digital prototype.....	30
Figure 18: H Selecting or deselecting an app changes the "privacy level" for digital prototype .....	30
Figure 19: Available filters for finding the apps based on their category or the data type being used by them, for digital prototype.....	31
Figure 20: Feedback that you are now using custom settings. ....	31
Figure 21: Before and After for the side menu option to include "Duration" service.....	37
Figure 22: Before and After for homepage where the users can know that the options contain more information .....	37
Figure 23: Before and After for homepage where the users now know that it is possible to customize the pre-set .....	38
Figure 24: Before and After for the customize page, where selecting the slider on the preset levels of High, medium and low will make the required changes to the applications, which the user can edit. ....	38
Figure 25: Homepage now consists of 4 steps instead of two, including an optional step of customizing the pre-sets. The user is guided through each step by giving feedback and directions towards next steps. ....	39

Figure 26: These icons present the current privacy state. Green means high privacy, yellow is medium privacy and red is low privacy settings while driving conditions. .... 40

Figure 27: Overview screen which shows the applications/ services running and their privacy status ..... 40



---

**List of tables**

---

Table 1: Requirements catalogue for the privacy-app concept .....	9
Table 2: Additional comments for the requirements mentioned above .....	12
Table 3 : Important User Centered Requirements to be considered for building the concep .....	20
Table 4 : Observations based on the four tasks performed by users. Users are PT01 to PT05 .....	32
Table 5 : SUS scores for the five participants .....	34
Table 6: Responses of participants after the test, during semi-structured interview .....	34
Table 7: The demographics of the users and also the responses when asked about the differences they would want in the current options of app overview information and app full view options .....	41
Table 8 : Comparison for requirements catalogue .....	42

---

**List of abbreviations**

---

IAD	Institut für Arbeitswissenschaft der Technischen Universität Darmstadt
FIA	Federation Internationale De' L Automobile
SUS	System usability scale

---

## 1 Introduction

---

Automotive Technology is increasingly advanced and along with these advancements come major privacy concerns for drivers. This is especially true for modern day connected cars equipped with infotainment and telematics systems that can collect substantial amounts of sensitive information. As cars begin to communicate wirelessly, the market for vehicle data is a lucrative new horizon. There is a rush to control this data and many vehicle manufacturers, who control this data at present, aim to become the service provider for all your car-related needs.

Connected cars in the market which are equipped with internet access are able to send and receive data, enable tracking and are able to communicate private information about consumers. Various smartphone applications as well as manufacturers and service providers have access to a huge pool of data that can be transmitted from a car and there is a clear disconnect in what is being tracked and what citizens are willing to accept when it comes to car data.

This not only needs strong data protection, but consumers have a right to know what data they are sharing in order to make informed decisions. Several user studies reveal that the consumers feel the need to control their data and the service provider they choose to share it with. They also must have the possibility to shut off communication when possible. Along with the user needs and technical requirements, this project aims at formulating a concept for an interface for self-controlled privacy in the connected cars.

A catalogue of requirements for the concept is presented after studying the available literature and the user studies which examine the user intentions and expectations from privacy in a car. Based on the requirements listed in the catalogue, a concept for step-wise privacy settings is suggested, which walks the user through the possible changes they can make to ensure privacy. A user-centered approach is followed while creating an interface for the vehicle and an accompanying mobile phone application. The final results are presented along with an analysis of the requirements which are being fulfilled or not by the concept suggested.

---

## 2 Literature review

---

### 2.1 What is a connected car

*A car equipped with Internet access that can send and receive data on the vehicle's status, condition and user preferences. Smartphone applications, car diagnostics and parking recommendations can use the vehicle data and be displayed on the vehicle's dashboard screen.* (FIA Region 1, 2016)

According to the American Department of Transportation, “Connected vehicle applications provide connectivity among vehicles to enable crash prevention, between vehicles and the infrastructure to enable safety, mobility and environmental benefits; among vehicles, infrastructure, and wireless devices to provide continuous real-time connectivity to all system users” [US Department of Transportation 2015]. It is worth noting that, in this case, general networking capabilities are considered, not indispensably a connection to the Internet. (Coppola & Morisio, 2016)

Connected-vehicle technologies are visualised to ultimately include safety, mobility, and environmental applications. Connected-vehicle safety applications would enable vehicles to have 360-degree awareness to inform a vehicle operator of possible hazards. These safety applications have the potential to reduce crashes through advisories and warnings. Connected-vehicle mobility applications are intended to provide a connected, data-rich travel environment based on information transmitted anonymously from thousands of vehicles that are using the transportation system at a particular time. Providing travelers with real-time information about traffic congestion and other travel conditions is expected to help them make more informed decisions that can reduce the environmental impact of their trip. Informed travelers may decide to avoid congestion by taking alternate routes or public transit, or by rescheduling their trip, all of which can make their trip more fuel-efficient and ecofriendly. (Schoettle and Sivak, n.d.-b)

### 2.2 Privacy in a car

*In a general sense, privacy may be defined as the ability of individuals to decide when, what, and how information about them is disclosed to others. Privacy principles demand that systems minimize personal data collection, for example through anonymization. Before personal data can be collected, consent from the data subject needs to be obtained by notifying about the nature and purpose of their data-collection and offering policy choices. Furthermore, it also requires the application of privacy preferences, either through technology, business practices, laws, or some combination thereof, in the use and further dissemination of the disclosed information.* (Duri et al., 2002)

The data in a car can be classified as two broad categories : Telematic and infotainment data. (Jaisingh, El-Khatib, & Akalu, 2016) Telematics systems contain vehicular information about internal systems such as fuel efficiency, engine failures, brake pad wear, transmission issues, oil life, climate control, biometric sensors, vehicle speed, acceleration, direction, braking, cornering, ignition, steering, seat belts, door locking, tire pressure, and recently visited destinations including routes travelled. This data is primarily used for vehicle diagnostics and emergency situations to automatically provide roadside assistance service providers pertinent information. Infotainment systems contain non-vehicular information such as voice calls, text messages, emails, social networking, personal contacts, calendar/planner schedules, search history, recently viewed content (photos, audio, video, websites), and any other data which may be synced from mobile devices. Moreover, infotainment systems provide drivers the convenience they desire and the ease of use they need while performing various onboard tasks when driving. Such onboard tasks may include hands free calling, text messaging, emailing, etc. Other types of data may be driver's profile and preferences, GPS & location data and the driver/ rider profile. Recently, modern infotainment and telematics services are merging together to provide drivers both infotainment and telematics data for various applications requiring both sources of information. Such applications may include automatic text messaging of estimated time until arrival based on the vehicle's current location and average speed, or automate certain infotainment services based on ignition, door locking/unlocking, etc.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA), is a legislation which was established to provide a set of rules governing how private sector businesses may collect, use, and disclose personal information through the course of their commercial activities while recognizing individuals' right to privacy with respect to their personal information. By definition, according to PIPEDA, personal information is "information about an identifiable individual". Moreover, within the context of vehicular data, this includes various pieces of information which can be obtained from both infotainment and telematics systems. Information may include identification data, personal communications data (voice, text, email, social networking data), location data, biometric and health data. In addition, both driver behavior data and miscellaneous infotainment data may not constitute personal information in accordance to PIPEDA, however, they certainly have implications on one's privacy.

Customer data produced by both infotainment and telematics systems have become a very hot product for infotainment and telematics service providers seeking substitute revenue streams as many third parties such as marketers, merchants, application developers, insurance companies, governments, data brokers, and law enforcement agencies are interested in buying this data for the valuable insights it can deliver using data analytics. (Jaisingh, El-Khatib, & Akalu, 2016) That being said, with respect to knowledge regarding service and aftermarket repairs, much of this data may be retrieved and instigate from vehicle infotainment/telematics systems. Data brokers then investigate the data using data analytics to

make potentially sensitive inferences about different drivers and later share this information with third parties for purposes such as behavioral profiling or advertising.

It is important that automakers and infotainment/telematics service providers do not collect more data than compulsory for providing the service, because the risks of over-collection increase privacy consequences as more unexpected third parties gain access to potentially sensitive information for secondary purposes. Regarding secondary purposes, collected data should only be used for the original purpose which it was intended as stated in company's terms and policies. In fact, using collected data for secondary purposes may infringe on the privacy of customers. Another example of a possible privacy alarm is the data that persists on infotainment systems even after the driver has disconnected their mobile device. This concern mainly applies to shared vehicles as the previous driver's synced data such as email, contacts, and calendar may still be available to a stranger. (Jaisingh, El-Khatib, & Akalu, 2016)

### **2.3 Self controlled privacy in a vehicle**

Upon reviewing the current state of data privacy in the car, it is suggested that we create a privacy interface for automobiles. A user-centered application which can let the user control their privacy and also review what is being shared. But this interface would be required to have compliance to the norms of vehicular interface design. Keeping the definition of user privacy and the possible implications of data-collection and usage in a vehicle in mind, it may be required to discuss some existing norms for vehicular interface design that need to be consulted while designing a system that lets the user control the privacy of their data in all possible scenarios, like driving or in a parked position and also be able to control the privacy of their data remotely through other connected devices.

The following sections provide an overview of the norms for designing such vehicular interface and reports the studies about user's opinions on the connected car technology as well as opinions about privacy in a vehicle. The user studies will help to understand the concerns and get clues to designing such an interface which is usable.

Upon studying the given norms for interface design and the user's expectations with privacy related to connected vehicles, a catalogue is presented in Section 3 with all the requirements to be kept in mind while designing the concept for such an interface which allows the user to control the sharing of data in their vehicle.

### 2.3.1 Overview of norms on vehicular interface design

The National Highway Traffic Safety Administration (NHTSA) has issued a nonbinding, voluntary NHTSA Driver Distraction Guidelines to promote safety by discouraging the introduction of excessively distracting devices in vehicles. The NHTSA Guidelines list certain secondary, non-driving-related tasks that, based on NHTSA's research, are believed by the agency to interfere inherently with a driver's ability to safely control the vehicle. The Guidelines recommend that those in-vehicle devices be designed so that they cannot be used by the driver to perform such tasks while the driver is driving. The list of tasks considered to inherently interfere with a driver's ability to safely operate the vehicle include: displaying images or video not related to driving; displaying automatically scrolling text; requiring manual text entry of more than six button or key presses during a single task; or requiring reading more than 30 characters of text (not counting punctuation marks). All the relevant guidelines are listed in the catalogue in Table 1. (NHTSA-2010-0053)

Driving is a complex task requiring continuous allocation of attentional resources to both driving and non-driving tasks. Because of this, driving is an interactive balance between cognitive, physical, somatosensory, visual and psychomotor skills. Driver and vehicle form an integrated system that includes the environment, vehicle controls, and displays collectively defined as the transport information and control systems (TICS). Since driving is an interactive systems activity, vehicle characteristics in combination with human capabilities constitute important factors in the performance of this TIC system. In order to achieve optimal driver performance, the purpose of TICS is to support drivers in their primary task such that performance, comfort and safety are increased and overall driver workload is not negatively influenced by the use of TICS. One set of factors influencing this process involves the characteristics of visual displays. Some design standards define certain properties of an HMI and follow continuously technological and methodological progress. In many cases they represent an important basis for regional recommendations and memoranda of understanding, covering the dialog management principles, visual presentation and auditory presentation of information in the vehicle HMI. Such requirements are listed in the catalogue. (E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008) (E DIN EN ISO 15005:2016-02 ; ISO 15005:2002(E))

Another solution for in-vehicle interfaces is by using speech recognition. Speech recognition converts spoken words to machine-readable input, this input allows the machine to identify words the person is speaking and subsequently process the command. (Hua & Ng, 2010) It lets users manipulate the machine verbally without having to manually control it. This has the benefit of helping users to complete their work more

efficiently while doing multiple tasks simultaneously. Using a case study and review of the literature, the paper illustrates a set of guidelines which are mentioned in the requirements catalogue.

While navigation decision making can be largely memory-driven, requiring little if any new information, guidance decision making and control decision making are based on the immediate driving environment and can be considered as mainly data-driven. A framework for providing ecological function allocations in intelligent driver interface consists of four general principles, as described in (Wang, Hou, Tan, & Bubb, 2010), each corresponding to a specific design requirement. The design principles are as mentioned below.

- Principal 1: to support interaction via time-space signals, the driver should be able to act directly on the display, and the structure of the displayed information should be isomorphic to the part-whole structure of movements.
- Principal 2: to provide a consistent one-one mapping between the driving domain constraints and the cues or signs provided by the interface.
- Principle 3: to represent the driving domain in the form of an abstraction hierarchy to serve as an externalized mental model that will support knowledge-based problem solving.
- Principal 4: navigation/strategic decision making can generally be done while driving as time permits from minutes to hours. Guidance/tactical decisions are considered to take place in seconds while control operational decision require only milliseconds to execute.

### 2.3.2 Overview of user opinion on connected cars

A survey (Schoettle & Sivak, n.d.-b) examined public opinion regarding connected-vehicle technology across three major English-speaking countries—the U.S., the U.K., and Australia. The survey yielded useable responses from 1,596 persons over the age of 18. The majority of respondents had not previously heard of connected-vehicle technology; however, most had a positive initial opinion of the technology. In an evaluation for user interest in the new services of a car in a separate study (Zimmermann M, 2016) respondents exhibited greater interest in faster navigation and improved safety, followed by better entertainment and more information about the car, whereas connectivity features were given the least importance. The majority felt that the expected benefits like fewer crashes, reduced severity of crashes, improved emergency response to crashes and better fuel economy are likely to occur. Respondents generally expressed a high level of concern regarding the data privacy, system security (from hackers), safety consequences of equipment failure or system failure and increased distractions for drivers. The majority of those surveyed stated that safety was the most important aspect of connected vehicles, while mobility and environmental applications were given very less weightage.



Most individuals said that it is important for personal communication devices to integrate with connected vehicles, as well as for such vehicles to have Internet connectivity. The majority of respondents expressed a desire to have this technology in their vehicle. When it comes to connected cars, consumer interest remains consistent and new functionalities do not overtake traditional interests. (FIA Region 1, 2016). Willingness to pay for connected-vehicle technology was moderate amongst all countries. The results from all three countries surveyed were remarkably similar in most regards. However, U.K. and Australian respondents were less concerned with security related to hacking and data privacy than U.S. respondents. The study also shows younger respondents were more interested in the entertainment services like music streaming and preferred it over e-mail services in the connected cars. There was no such clear differentiation amongst older respondents.

Users can be divided into six kinds based on their views about connected cars, i.e. Enthusiasts (12%), Connected & relaxed (20%), interested but hesitant (25%), distant (19%), anxious & not interested (14%) and opposed (10%). The visualisation is shown below.

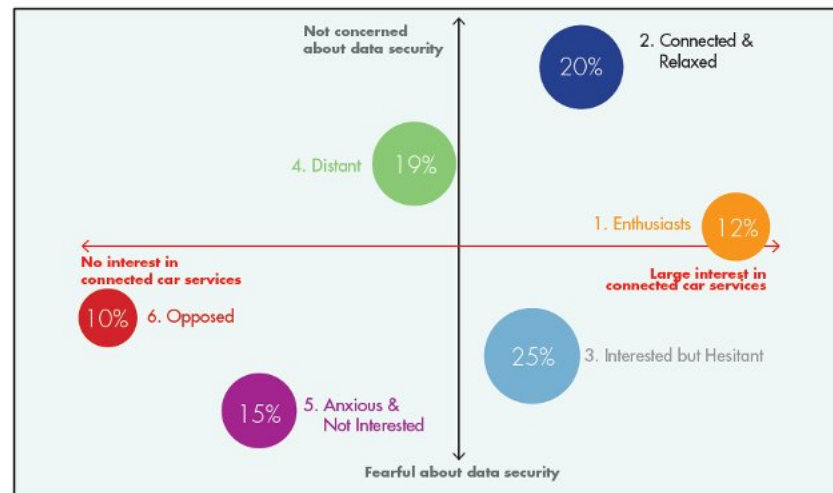


Figure 1: Where the types fall on a scale of interest in connected cars versus concern about data security.

An overwhelming majority of consumers called for legislation to protect user data with connected cars. There was some indecision as to whether this should be European or national legislation, but a small preference for European legislation was seen. (FIA Region 1, 2016)

Another survey (Schoettle & Sivak, n.d.-a) which examined the public opinion regarding autonomous and self driving vehicle technology yielded similar results, with some anomalies. While a majority of individuals had previously heard of self-driving vehicles, a majority had not previously heard of connected vehicles. Most respondents felt that less traffic congestion and shorter travel time were each unlikely to occur with self-driving vehicles, however they were rated higher on the expectations scale for connected vehicles. A higher level of concern was expressed regarding the use of self-driving vehicles. However, concern was high in both studies regarding data privacy for U.S. respondents. Interest in having connected-vehicle technology was much higher than the interest in having self-driving technology on respondents' vehicles. A higher percentage of respondents were willing to pay extra for connected-vehicle technology. However, those who were willing to pay for self driving technology were willing to pay more than those who would pay for connected vehicle technology.

### 2.3.3 Overview of user opinion on privacy in connected cars

The study to determine the status quo of data security in cars from the user's point of view (Zimmermann M, 2016) reveals that the readiness amongst the users to release their data is overall low and depends on the location of storing and processing the data. Overwhelmingly respondents felt that the data generated by the car should be owned by the driver or owner of the vehicle. Almost all drivers wanted the possibility to switch off all communication from their vehicle, which is also covered in the requirements catalogue. (FIA Region 1, 2016)

As illustrated in the catalogue of requirements, they are somewhat comfortable to release data if it is stored and processed within the vehicle like saving contacts internally. Sending music preferences to the music provider, sending data to or contacting the manufacturer and sharing GPS data with the provider are least preferred. The identity of the data receiver and the location of the data being stored and processed is relevant to the user. The users exhibit greater trust in the police and rescue workers and the mechanical workshops with their data, and lesser with the car manufacturers, music streaming providers and providers of rebates. The relevance of the situation or the service is also important, as more users are comfortable sharing their GPS data with the rescue workers in case of an emergency as compared to the manufacturers of the car. Users perceive calendar entries, GPS data and the travel profile as more personal data than the music selection and vehicle data (like motor power, breakage and acceleration, steering or fuel behaviour). However, the latter may be a

potential source of information. The users are most motivated to release their data when there is complete transparency about who receives the data and how it is being processed, which is a big requirement factor for the self controlled privacy. Moreover, users are willing to release their data if there is a perceived added value of the

service, like saving travel time. However, financial incentives like good value for money are not important motivations to release data. There is a behavior gap as the studies reveal that the users are not very critical and controlling of the data on their smartphone and computers. Not all users ensure the activation of their smartphone location services or verify data protection regulations while installing an application. Users who reported a careful handling of data while using the navigation services on their smartphones and computers also exhibited a lower willingness to release their data than those who reported a lower control of their data in everyday life.

Upon review of all the norms for vehicular design and upon reading and evaluating the user expectations from privacy in connected cars, the requirements catalogue is formulated in a tabular format and it is presented in Table 1 in the next section. The requirements catalogue is followed by the method that will be used to realise the requirements into a concept for self-controlled privacy.

### 3 Requirements catalogue

Based on the review of technical requirements of the vehicle interface from the above mentioned literature, and from the study of user opinion of privacy in connected cars, a list of requirements is derived. The user statements listed in user studies conducted by FIA and IAD are interpreted to reveal the motivations and expectations of the users to share information with service providers and third party applications. The requirements are derived either from direct user statements or by interpreting what the studies show by analysis. The process of reviewing the requirements and interpreting them to give design directions is explained in the next section. These requirements will guide the conceptualisation process for the interface to control privacy of data. Table 1 lists all the requirements along with the source. Table 2 lists additional comments for the requirements list. Refer to Appendix A for the color specifications.

Table 1: Requirements catalogue for the privacy-app concept

Nr.	Description of the requirement	Category of requirement	Source
1	The displayed text should not be continuously moving text.	Per se lock out	NHTSA-2010-0053
2	A driver should not enter more than six button or key presses during a single task.	Per se lock out	NHTSA-2010-0053
3	There should not be more than 30 characters of visually presented text.	Per se lock out	NHTSA-2010-0053
4	When manual device controls are placed in locations other than on the steering control, no more than one hand should be required for manual input to the device at any given time during driving.	Single handed operation	NHTSA-2010-0053
5	The maximum device response time to a device input should not exceed 0.25 second.	Response time	NHTSA-2010-0053
6	A TICS dialog shall regulate the flow of information so that it can be easily perceived	Dialog management principles	Heinrich C, Automotive HMI International Standards
7	The driver must be able to override any intervention of the system towards driving functions	Dialog management	Heinrich C, Automotive HMI

		principles	International Standards
8	Systems that are not intended to be used while driving must be deactivated or the manual must contain an appropriate warning	Dialog management principles	Heinrich C, Automotive HMI International Standards
9	Glances of 1.5 seconds shall be sufficient to gather relevant information	Dialog management principles	Heinrich C, Automotive HMI International Standards
10	System reaction time should not exceed 250 ms.	Dialog management principles	Heinrich C, Automotive HMI International Standards
11	Displays supporting dialogue should only present symbols, signals, tell-tales, graphical elements and terminology (terms, abbreviations, etc.) likely to be understood by the driver	Dialog management principles	E DIN EN ISO 15005:2016-02; ISO 15005:2002(E)
12	The particular input required to reach the intended goal should be made obvious to the driver.	Dialog management principles	E DIN EN ISO 15005:2016-02; ISO 15005:2002(E)
13	If the same information is presented in more than one display, at least one of the information displays shall meet the requirements of the International Standard.	Redundant information display	E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008
14	Dynamic text, especially text related to messages that are urgent in nature, should be set in mixed or lower case, unless otherwise required by the national body.	Text case	E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008
15	The x-height of the font must be at least 70% of the Cap height of the font	Font specification	E DIN EN ISO

			15008:2016-02 ; ISO/DIS 15008
16	Typefaces selected should not be too light or too bold. The proportion of the stem width to the ascender height should range between 10 – 20 %.	Font specification	E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008
17	Typefaces selected should not be too narrow or too wide. The proportion should be between 65 – 80 %	Font specification	E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008
18	Typefaces selected shall be evenly and proportionately spaced and the space between vertical strokes (such as between l and m) should range between 150 – 240 % of the stem width. The space between diagonal characters and a vertical (such as between v and l) should be a minimum of 85 % of the stem width. Two diagonal characters shall not touch. The words space is related to the intercharacter spacing of the typeface. The proportion of word space to intercharacter space can range between 250 and 300 %.	Font spacing	E DIN EN ISO 15008:2016-02 ; ISO/DIS 15008
19	The sound level must be loud enough to be well perceived but shall not startle the driver	Auditory presentation of information	Heinrich C, Automotive HMI International Standards
20	The timing shall be appropriate for the type of information	Auditory presentation of information	Heinrich C, Automotive HMI International Standards
21	To ensure good audibility also in case of age related hearing loss a frequency range from 400 Hz to 2000 Hz is recommended	Auditory presentation of information	Heinrich C, Automotive HMI International

			Standards
22	For important warnings redundant visual information is required.	Auditory presentation of information	Heinrich C, Automotive HMI International Standards
23	The speech recognition interface should use a broad and shallow hierarchy structure.	Speech recognition interface	Hua Zhang et al. 2010
24	The interface should provide visual feedback and memory aids	Speech recognition interface	Hua Zhang et al. 2010
25	The interface should provide quick access to a final speech recognition command, by providing vocal shortcuts.	Speech recognition interface	Hua Zhang et al. 2010
26	The functions that the user needs immediate and quick access to should be activated by hard keys or steering wheel controls.	Speech recognition interface	Hua Zhang et al. 2010
27	The user should decide if they want to share their data.	User Centered	FIA Region 1, 2016
28	The user should be provided with all relevant information to make a decision about sharing their data.	User Centered	Zimmermann M, 2016
29	The kind of party receiving the data externally should be revealed to the user	User Centered	Zimmermann M, 2016
30	The identity of the data receiver should be revealed to the user.	User Centered	Zimmermann M, 2016
31	The location of the data receiver should be revealed to the user.	User Centered	Zimmermann M, 2016
32	The user should be able to decide the level of how “personal” the data is to them	User Centered	Zimmermann M, 2016
33	The data sharing should be based on the type of function of the application.	User Centered	Zimmermann M, 2016

34	The user should be able to switch off/ on all data sharing.	User Centered	FIA Region 1, 2016
35	The user should be able to share data anonymously.	User Centered	FIA Region 1, 2016
36	The user should be able to choose the duration for which the data being shared with any party.	User Centered	FIA Region 1, 2016
37	Privacy protection has to be compatible with the core functions of the concerned apps as well as with the driving task.	User Centered	Sedafa Projekt report
38	Privacy should not reduce the usability of the general usage of the vehicular HMI.	User Centered	Sedafa Projekt report
39	The hmi has to be in line with current situational, cognitive and security-relevant circumstances in the car	User Centered	Sedafa Projekt report
40	Data deletion should be possible and it should be ensured that data cannot be recovered after deletion.	User Centered	Sedafa Projekt report
41	The HMI of the privacy app (here: wrapper app) should be intuitive and usable. Distraction should be minimized.	User Centered	Sedafa Projekt report
42	For each data usage, the data receiver has to convey the reason for data collection.	User Centered	Sedafa Projekt report
43	All affected persons must be able to control data transmission.	User Centered	Sedafa Projekt report
44	Opportunities for privacy control should be layed out such that prior knowledge and situational factors like cognitive workload or motivational influences do not hinder control.	User Centered	Sedafa Projekt report
45	The user has to be aware of all control possibilities.	User Centered	Sedafa Projekt report
46	The user should be informed right in the situation in which he/she has to make his/her privacy decision	User Centered	Sedafa Projekt report
47	The car must be able to categorize the recorded, used or processed data according to its person-relatedness (relatable to a person, not relatable)	User Centered	Sedafa Projekt report
48	The car must be able to identify if for each single datum an user agreement is available	User Centered	Sedafa Projekt report



49	Per default, each datum has to be labeled as "not agreed on".	User Centered	Sedafa Projekt report
50	It has to be verified technically that the agreement was indeed done by the effected person and that the agreement is only applied to him/her.	User Centered	Sedafa Projekt report
51	The car has to inform the user on which datum is recorded/processed/used, for what, from whom? how long/often? what are the consequences of denial?	User Centered	Sedafa Projekt report
52	The car has to inform the cooperating system in case of data transmission about the presence or absence of an user agreement.	User Centered	Sedafa Projekt report
53	All agreements have to be saved in the car. the user has to be able to recall the agreements at any time point and make a denial. He or She has to be informed about the consequences of denial. The denial must not influence the application at a whole.	User Centered	Sedafa Projekt report
54	For each data transmission the presence of an user agreement has to be verified.	User Centered	Sedafa Projekt report

Table 2: Additional comments for the requirements mentioned above

Nr.	Additional comments
1	The visual presentation of limited amounts of static or quasi-static text is acceptable. (The following in-vehicle device tasks should always be locked out unless either (1) the vehicle's engine is not running, or (2) the vehicle's transmission is in "Park" (automatic transmission vehicles) or the vehicle's transmission is in "Neutral" and the parking brake is on (manual transmission vehicles)
2	This would include drafting text messages and keyboard-based text entry.
3	Not counting punctuation marks, counting each number, no matter how many digits it contains, as one character, and counting units such as mph as just one character
5	If device response time exceeds 0.25 second, a clearly perceptible indication should be given indicating that the device is responding.
12	EXAMPLE 1 When a menu is used, only the available options is presented for selection. ; EXAMPLE 2 Guidance is given to the driver on the

	current phase within the system dialogue structure.; EXAMPLE 3 Prompts are displayed indicating that the system is available for input. These prompts provide information on the type of driver input that is valid, given the current system status.
14	Uppercase could be used for texts that are a permanent part of the UI such as buttons and labels as the frequency and predictability of appearance of such text will improve the reading time required
15	(as can be seen by dividing the width of the lower case letter L by its height)
16	(as can be seen by dividing the width of the lower case letter L by its height)
17	The proportion of the letter H (width of H divided by height of H)
23	A broad menu tree allows users to access available menu options at top hierarchy level without unnecessarily going too deep into any particular category. Shorter menu paths will also reduce task completion times efficiently. The ideal number of levels in a menu should not be more than three for a user to complete a final command
24	Visual feedback corresponding to the voice menu will facilitate users in command recall. It will also enable them to know what commands had been given, and if the system is expecting a response from them.
25	It is especially useful for frequently used commands or when users forget where they are in the system. The two approaches, "Flexible Shortcuts" and "Our-of-turn" solve this problem
26	Functions that the user performs in the car should be analyzed before porting all their trigger mechanisms to voice.
29	Could be the police, ambulance, car manufacturers, GPS providers or car insurance/ rebate providers.
30	The more relevant the receiver and the location, the less reluctant the user is to share the data.
31	The more relevant the receiver and the location, the less reluctant the user is to share the data.
32	The perceived levels of personal information like Contact details, Music preferences, GPS data, travel profile or the technical car data.
33	Different functions like E-call, navigation, entertainment, insurance etc.
34	90% of the users want to be able to switch off all data sharing. (A warning is necessary here as it may hamper the working of some apps)
35	2/3rds of the users feel comfortable sharing their data anonymously to improve driving or get other benefits.
36	Permanent / For a given time / Per ride

Based on the requirements listed above, a methodology is discussed in the next section, which follows user-centered design approach to realise a concept and build a prototype ready for testing. Such methodology is mentioned in detail in the subsequent section, and supporting it, there are outcomes of the methodology which are mentioned in section 5, Results.

---

## 4 Methodology

---

This section explains the step wise process used while formulating the concept and giving it shape into a product, using user-centered design approach. The steps used below are as follows: requirements review and creating user persona, brainstorming and mind mapping, creating information architecture, paper prototyping, digital prototyping and testing, iterations to digital prototyping(simultaneously along with digital prototyping and testing), user inteface design and user testing. Since the process was iterative in nature, many times steps were repeated to include new ideas or findings. The steps and the reasoning for the steps are explained below, and their outcomes are explained in section 5 : Results.

### 4.1 Requirements review and user persona

A Review of the requirement list was done to understand user perspectives and interpret them to include in the design of the application. It is important to look carefully at the users that were participants in the research(es) for determining user’s view on privacy in connected cars. The possible design implications of some requirements are listed in Table 3.

A sample persona is created, for a typical type of user who will be using the product, based on the given demographics in the studies. (Allabarton, 2016) The persona is fictional but represents a selection of the real audience and their behaviors. It also helps set the user expectations from the product and help understand the scenarios in which the product may be used. The persona is presented in Figure 2.

### 4.2 Brainstorming and mind mapping

A quick brainstorm of all the spontaneous keywords was listed down. It was mixed with various ideas that may be of help during the mind mapping. A brainstorm helped to start thinking of possible ideas for the concept and also lay down some important keywords like “step wise settings” & “Red-light settings”. Refer to Figure 3 for the detailed brainstorming.

Based on the brainstorming, a mind map was developed, where data and information collected during formulation of requirements was put into more structured thought. The ideas also generated during during brainstorming were considered to come up with a mind map for what the product would be. By analyzing, correlating and synthesizing ideas, eventually a pattern was derived which would be the rough draft to build the information architecture on. (Allabarton, 2016) As depicted in Figure 4, the mind mapping of ideas also helped come to the basis of the concept-the privacy levels.

### 4.3 Information architecture

After creating a map of the higher level set of actions that would need to be supported, thus began the mapping of an ideal user flow, which was mostly “directional” and the supporting content was thought of, that could provide clarity and context for a given situation. Most of the flow is linear so there would not be many divergent routes that the user may take. A formal structure was decided, including the important information that needs to be conveyed to the user. (Allabarton, 2016) Some navigation and data was inserted and the linear flow is fixed. While deciding the Information architecture, the following concepts are kept in mind :

- Cognitive load is the amount of information that a person can process at any given time. Keeping in mind the user’s cognitive load helps prevent information architects from inadvertently overloading a user with too much information all at once. (UX Booth, 2015)
- Mental models are the assumptions people carry in their minds before interacting with a website or application. Information is easier to discover when it is in a place that matches the user’s mental model of where it should be. (UX Booth, 2015)

The purpose of Information Architecture was to structure, label, and organize the content on the application so that users can find exactly what they need to perform the task they want and to reach their goal. Through this structure it is possible to visualize how all the elements relate to one another. The architecture can be referred to in Figure 5.

An initial wireframe was also developed to display how the structure may look like. Based on the information gathered during research and the decisions made during hierarchy creation, a sketch was made to display key screens in order to demonstrate how a user will interact with the information available. Since it was easier to think visually about the flow, these initial wireframes helped to make way for paper-prototypes. (UX Booth, 2015) A sample of the first paper wireframes can be referred to in Figure 6.

The alternative to creating wireframes could be to create more detailed flowchart to depict user flow, but it was easier to visualize the steps in the form of a wireframe, so further research about the ideal flow was conducted using multiple wireframes and iterations.

#### **4.4 Paper prototyping**

Created simple paper prototypes based on the concept, which determined the allocation of space on every page, the distribution of content, how content is prioritized, what functions are available and what behavior of the user is intended. The simple sketch on paper method ensures that we can focus on the navigation and functionality of the product rather than the visual layer of the prototype. (Allabarton, 2016)

There were two versions of the prototypes created. Figure 7 represents version 1 which was a modification of the mobile wireframes created on the previous section while Figure 8 represents a more detailed and refined version, with more changes incorporated and Figure 9 represents an interactive paper prototype which was created to replicate a sliding menu.

#### **4.5 Digital Hi-Fidelity prototypes**

Once the paper prototypes were fixed, it was decided to create digital prototypes of the same concept in order to be able to test the prototype with users. The advantage of creating digital clickable prototype is also that it replicates the exact functionality that the real application would do, using the prototyping software “Axure RP 8”. After a discussion on the model for implementation of the design, a volkswagen Passant with an 8-inch central display with 800x480 px display was decided. It would be a touch display, but the current design is restricted to touch only and cannot be implemented with sound. Also it was decided against the head-up display. So the two main features for displaying the information would be the central display and the dashboard display (1440x540 px). A sample of the displays is shown below in Figure 10.



*Figure 10: The two available displays:*

- 1. Central touch display*
- 2. Dashboard display without touch*

The aim of this step is to get the basic design and getting the functionality in place. It was tried that all the functions in the final application should be replicated in the prototype, after which the first round of testing was done.

#### **4.6 User testing of Digital Hi-fidelity prototype**

Based on the digital prototype created so far, a testing was conducted with participants likely to use such a product in the future. The results from the test helped in iterating the digital prototype, which is described in detail in the next sub-section. The testing protocol used was as follows :

Testing Protocol: The digital wireframes were installed on a touch screen laptop to imitate the experience of using a car interface, with touch capacity. The purpose of in-person usability testing is to identify problems or issues the user has with the interface and why these issues arise. 5 users were selected at random, within the age groups of 25 to 40, only Germans, for a one-on-one testing.

The test was conducted in a neutral room and it lasted for 45 min - 1 hour for every participant. The method used was "Think-aloud" test. It means that the users are asked to talk through their actions out loud as they are making them. This gives a greater insight into what is going on in the user's mind while they are using the product. The tester was present in the room to observe, take voice recording and prompting the user to think aloud whenever required. Except that the tester did not help the users complete the tasks. The users were not explained to about the product at first, they were directly given 4 tasks to complete. The tasks given were as follows.

Tasks to do (think aloud test)

- Task 1 : Choose not to share any data of your car with any applications or service providers, and ask the app to remind you after a week if you changed your mind.
- Task 2 : Select a pre-dened setting which shares some, but not all sensitive data with third party apps. It includes sharing data with emergency apps, GPS & navigation apps and some utility apps (eg. Mileage report). Let the setting be always on until you turn it off. Then exit the app.
- Task 3 : Use a high privacy mode, but make exception to sharing all information with whatsapp.
- Task 4 : Provide access to only the apps which are meant for emergency situations (like car crashes).

The observations of the tasks are Listed in table 4.

Once the tasks were completed, a formal explanation of the product is given to the user, then they fill the SUS form, whose results are listed in Table 5 and the questionnaire is listed in Appendix B. The System Usability Scale (SUS) is a simple, ten-item scale giving a global view of subjective assessments of usability. The SU scale is generally used after the respondent has had an opportunity to use the system being evaluated, but before any debriefing or discussion takes place. Respondents should be asked to record their immediate response to each item, rather than thinking about items for a long time. (Brooke John ,1995) The SUS scores are from 0 to 100, where 100 means most usability and 0 means the least.

After that a semi structured interview was conducted, which is listed in Appendix C. The results of the semi structured interview and the actionable items are presented in Table 6.



#### **4.7 Iterations to digital prototype**

Based on the reviews of the users, the tabular list of changes is consulted and required changes are made based on the feedback. Certain changes made are listed in the table, refer to Figures. 22, 23 and 24 for a comparison of changes made to accommodate the responses from users.

#### **4.8 User Interface design and interactivity**

An interface is designed, keeping in mind the requirements of the interface in the vehicle, including color specifications, font sizes and spacing. Refer to Appendix A for detailed color requirements and Appendix D, E and F for the final and complete design of the three mentioned scenarios : The non-driving scenario in the car, the driving situation and the smartphone application which lets you make changes on the go.

The tour in the beginning of the product is also populated with animated graphics to help the users understand what the product is about and what is the benefit of using the product. Then the interface is populated with first the static elements, then imported to Axure for a clickable working digital prototype with the design. Continuous iterations are made in order to include small changes upon discussion with users and the project guide.

#### **4.9 User testing for applications design**

An intermediate test is conducted before the final testing to determine what information should be presented while making custom settings for applications or services being used in the settings. The test is defined in Appendix G. The users' details and their views are captured, along with the changes suggested by them in the Table 7. The following data is also collected from the users :

- Age
- Gender
- If they have driving license or not and Driving experience
- Method of using internet in their car (wifi on board/ smartphone mirroring or none)
- Level of automation on the car
  - 0 - No Automation - full time performance of human driver of all aspects of the dynamic driving task

- 1 - Driver assistance - ***the driving mode*** - specific execution of the driver assistance system of either steering or acceleration/ deacceleration using information about the driving environment and with the expectation that the driver will perform rest of the dynamic driving task
- 2 - Partial automation - ***the driving mode*** - specific execution by one or more of the driver assistance system of both steering and acceleration/ deacceleration using information about the driving environment and with the expectation that the driver will perform rest of the dynamic driving task (Repairerdrive, 2016)

The following section shows the outcomes of all the steps involved in the design proces. The suggestions for user testing are also mentioned in the next section.

---

## 5 Results

---

### 5.1 Requirements review and persona

The requirements formulated by the user studies need to be inculcated in the design, so the list of requirements is interpreted and the following key requirements are addressed while thinking of the concept. It also helps us understand what the user might expect from the application and how the major expectations can be fulfilled using the application. A brief review also reveals that a smartphone application accompanying the main application may be necessary to make settings for privacy on the go. The other important takeaways from the requirements catalogue and their possible design implications are mentioned in the table below.

Table 3 : Important User Centered Requirements to be considered for building the concept

Nr.	Descriptipn of the requirement	Possible Design Implication
27	The user should decide if they want to share their data.	Have yes/ no option first
28	The user should be provided with all relevant information to make a decision about sharing their data.	Provide pop ups/ info blocks
29	The kind of party receiving the data externally should be revealed to the user	Provide actual app manufacturer information
33	The data sharing should be based on the type of function of the application.	Indicate the type of app/ divide them by types
34	The user should be able to switch off/ on all data sharing.	Have options for switching data on/off from home screen
36	The user should be able to choose the duration for which the data being shared with any party.	Provide options for choosing duration
40	Data deletion should be possible and it should be ensured that data cannot be recoverd after deletion.	Provide a delete option at all times
42	For each data usage, the data receiver has to convey the reason for data collection.	Provide information wherever there is decision making

46	The user should be informed right in the situation in which he/she has to make his/her privacy decision	Provide information wherever there is decision making
51	The car has to inform the user on which datum is recorded/processed/used, for what, from whom? how long/often? what are the consequences of denial?	Provide a section of information about the app/ make app profile

A typical user persona is described below, based on the user studies mentioned in the literature review. The user description would be kept in mind while designing the concept and testing the application. Since the study conducted is limited to European citizens and lists similarities between all the countries participating in the study, the persona is assumed to be German and is usually a tech-savvy enthusiast, who can adopt new technologies. Find a brief persona of the user below.



## SAM SMITH PERSONA

Age: 28    Nationality: German  
Occupation: Marketing manager

Traits:

- Owns a new car(less than 5 yrs old)
- Knows about connected cars
- Spends >2 hrs online everyday
- spends >30 min on social media
- Uses several apps in his car and phone
- Willing to share data but is concerned about his privacy

Figure 2: A typical user persona relating to his views on privacy in connected cars

## 5.2 Brainstorming and mind map

Initial brainstorming using spontaneous keywords and suggested ideas is shown below. Various unrelated terms are listed down.

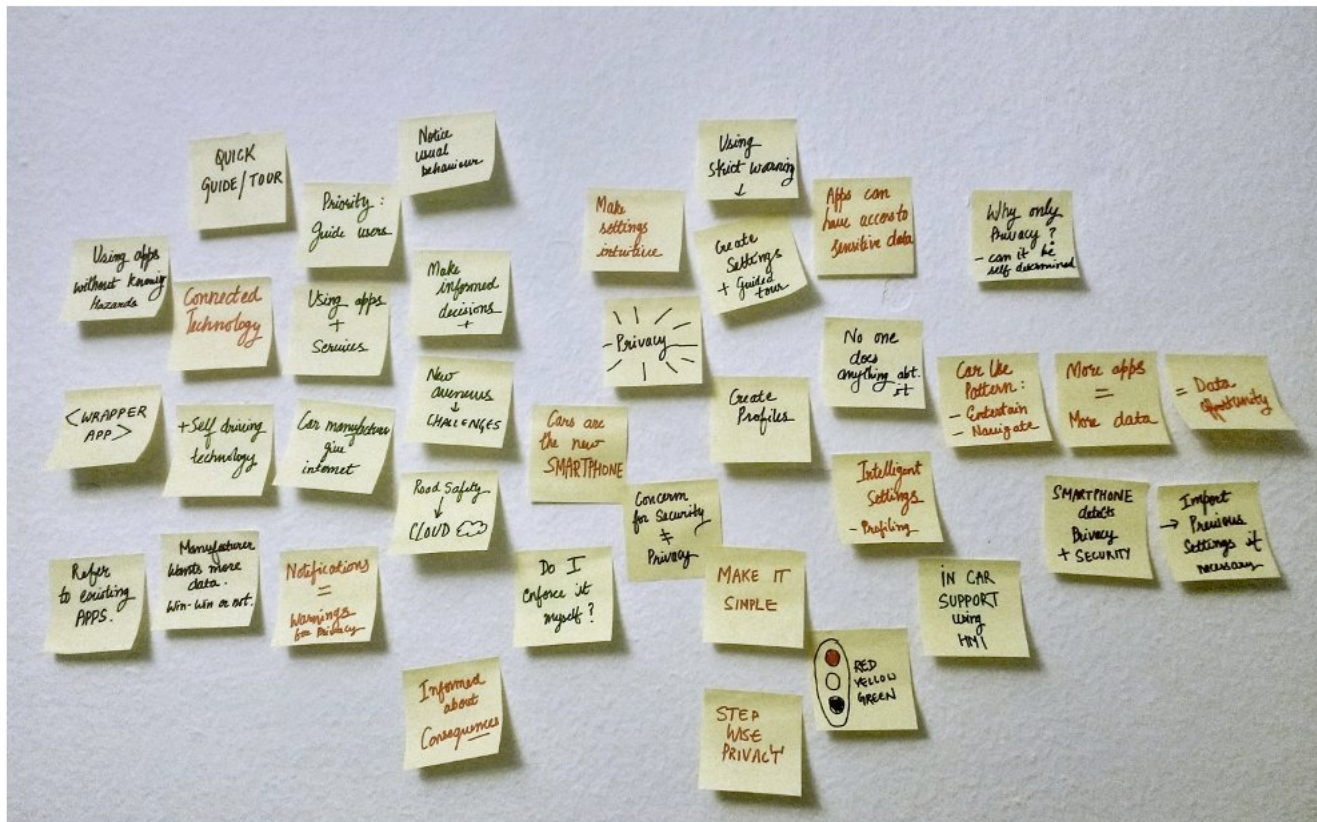


Figure 3: Brainstorming using keywords based on privacy and connected cars

Using the keywords generated during the brainstorming, a more structured mind map is created and the related terms are linked together to make meaning out of the exercise.

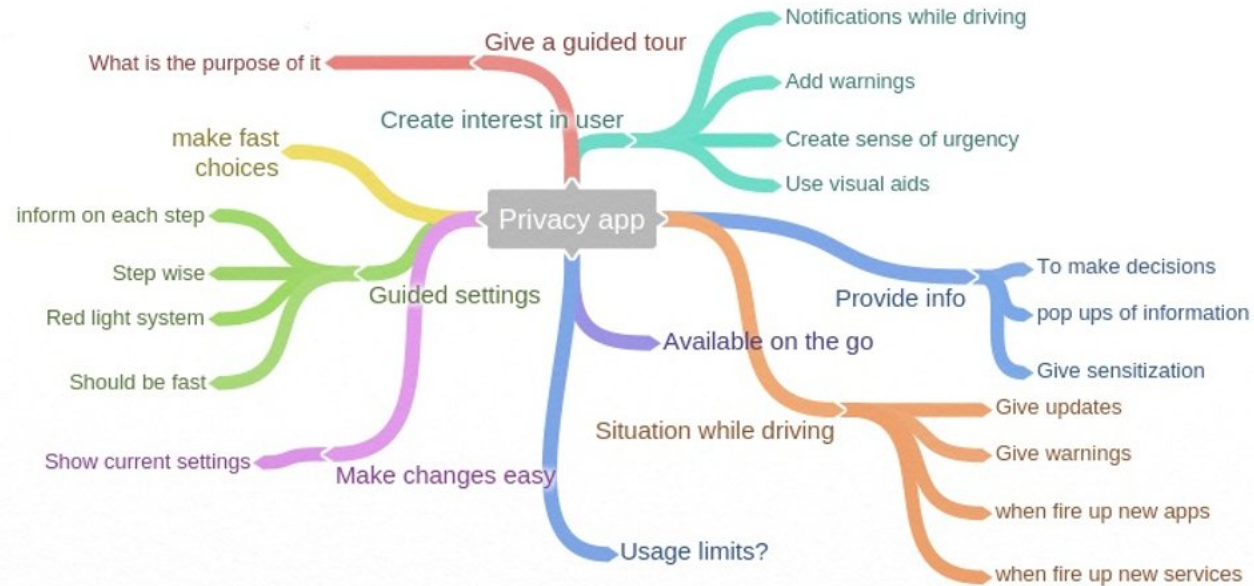


Figure 4: Mind map for possible ideas for the privacy application

### 5.3 Information architecture

The concept of the app is as follows. It contains three pre-defined privacy levels which contain some pre-defined settings for the user to quickly select and then exit the application. These three pre-defined levels are determined using a PRIVACY SCALE which determines how safe or unsafe an application is, based on certain parameters. The suggested privacy scale levels would be 1 to 10, where 1 means lowest privacy offered and 10 would be the highest. This scale would be defined by the following parameters:

- Type of application (emergency apps, driving assistants, music etc.) – An app which is of utmost importance during emergency/ accidents would be rated higher on the scale as compared to apps which are for entertainment purposes

- Credibility and trust-worthiness of the application manufacturer/ data collector, based on information provided on the app-store
- Amount of data collected by the app and for which functions
- Frequency of data collected
- Type of data collected (e.g. Location services, media library, call logs etc.) – The more sensitive data being used, the lower would be the privacy rating of the application.

This scale would use an algorithm that is suggested to be created and then it would sort each application installed on the system within the privacy levels and help define the three pre-defined levels, which would take the following things into consideration:

- Category of applications (emergency, navigation, music, car analytics, services etc.)
- Type of data being shared by the above mentioned applications

Formal structure of the information is created, using a flowchart. The organised content is shown in Figure 5.

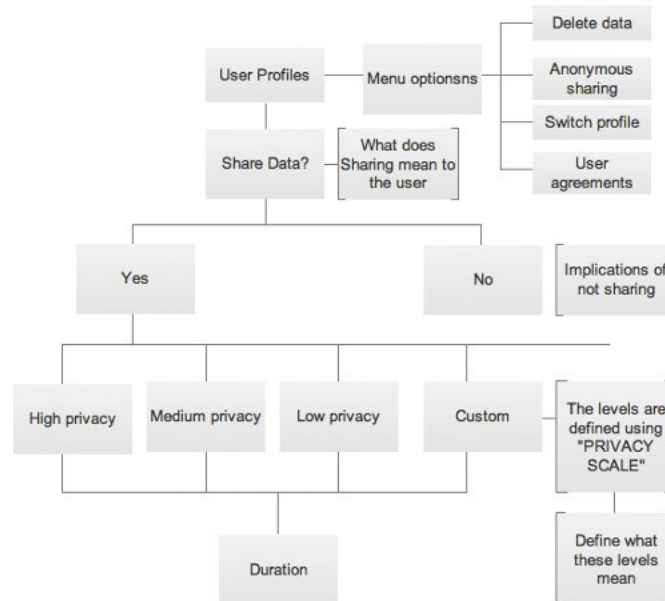


Figure 5: Information architecture for the application

To visualize the information in a better manner, an initial mobile prototype was made, as shown below in Figure 6. This version contains the same step wise process that is almost present in the final design of the application, but with many modifications. Also, this version does not contain many navigation features which were added in the paper prototype upon discussion. This prototype also relies heavily on pop-up screens of information in each step, which was decided against as it increases the number of steps performed to make a decision. The structure was then discussed in detail which led to the development of the paper prototypes as shown in the next section. It was also determined that since mobile is not the most prioritized device to be used for settings, the wireframes should be made on a screen which resembles the screen in a car. So the prototypes are made according to an 8 inch screen as in a Volkswagen Passat (new model).



Figure 6: Initial prototype for determining the information architecture



## 5.4 Paper prototypes

Paper prototype 1 : As shown in Figure 7, the paper prototype consists of 3 basic functions that the user needs to perform, i.e. Select whether to share data or not (Screen 1), Select the privacy level (or create your own privacy settings using custom)(Screen 2 and 4) and select duration of data sharing (Screen 3). This process should take the minimum time, and the surrounding functions should be minimized. The custom settings page consists of two important components : the privacy level scale, which you can drag and change to 5 different levels, i.e. Highest Privacy(no data sharing), High (pre-set), medium (pre-set), Low (pre-set) and Lowest Privacy (all data sharing). The benefit of this scale is that it gives live feedback to the user whenever they make a change in the settings of an app or service, which brings us to the second component of the custom settings page, the app settings area. In this prototype, the left side displays the categories of apps or services available on the system, and displays them category wise when you select. There is a direct checkbox for selecting the app along with all it's settings to share all data. Further changes are realised in paper prototype 2.

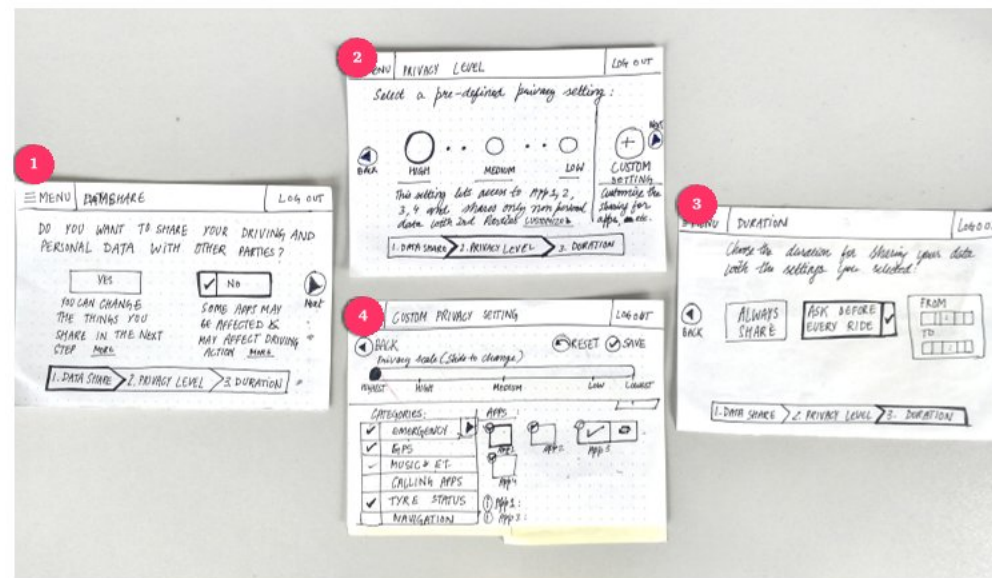


Figure 7: Paper prototype 1

Paper prototype 2 : As shown in Figure 8, the prototype includes most of the functionalities, including the user profiles (Screen 3)(the user profiles are created because of the need to have many drivers drive the same car but they may need to have their own settings), the two steps in the previous prototype, i.e. Step 1 and step 2 of selecting to share data and selecting the pre-sets is combined to reduce a step (Screen 4), however this needed to be changed back after the user testing, and the custom settings are made more comprehensive by providing filters like app categories and data type used, to the apps and services. Screen 9 is the overview screen in case of the car is running and the user would like to know which apps are using data and upto what extent by providing percentage.

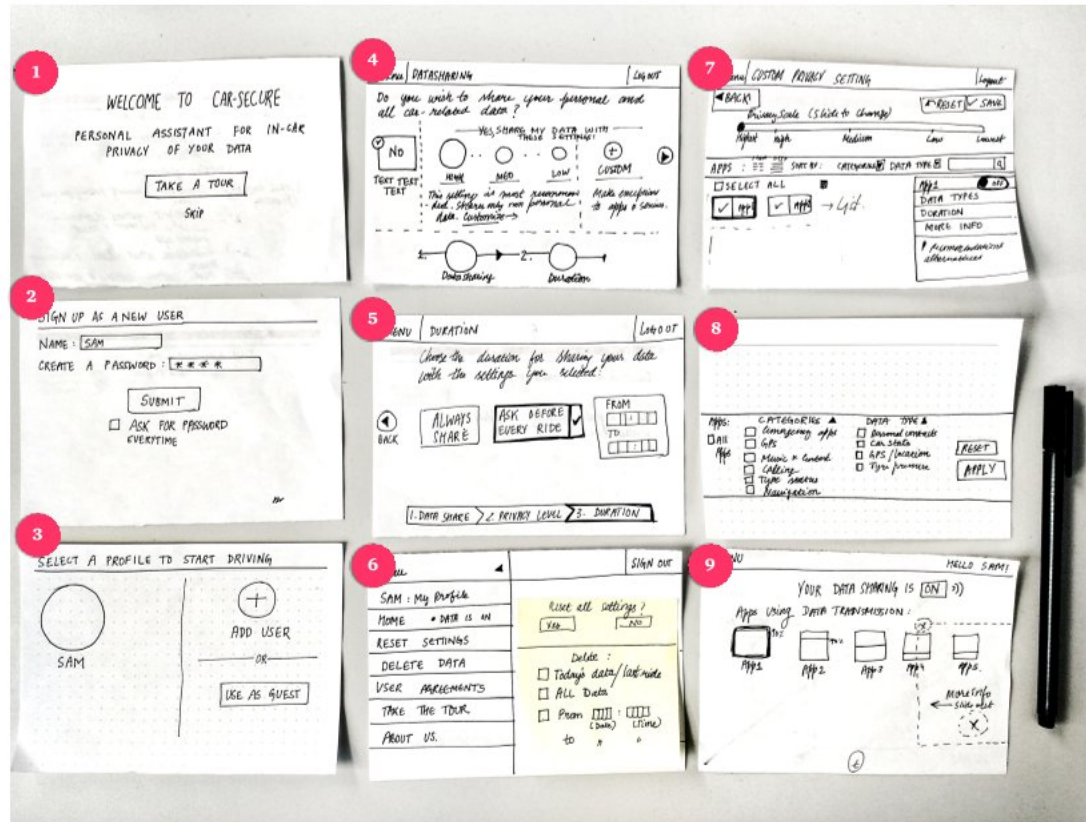


Figure 8: Paper prototype 2

## 5.5 Digital hi-fidelity prototypes

The following prototype screens are created using a graphic design software and then are linked using a prototyping tool "Axure RP 8". The main screens of the prototype are described below. The feasibility and usability of these prototypes is tested in the next section.

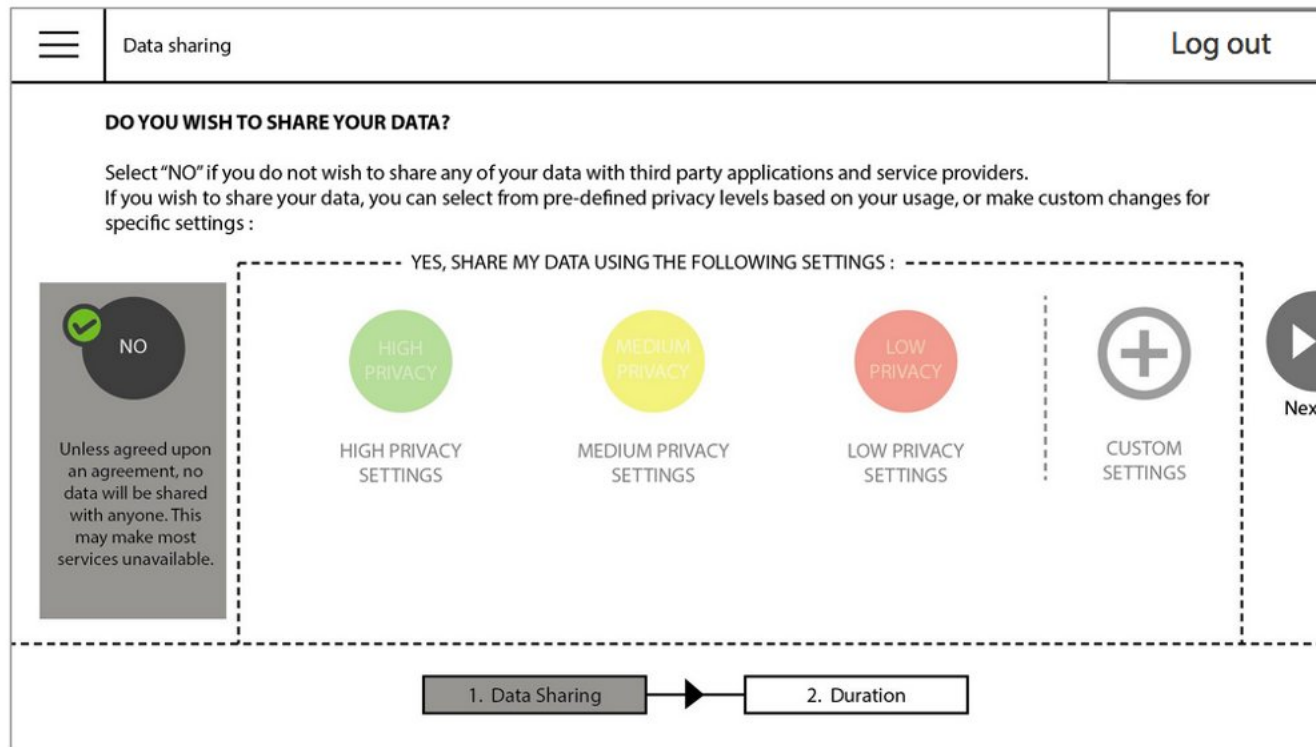


Figure 14: The main homepage for digital prototype with option to switch off data sharing, select pre-defined settings or go to custom settings.

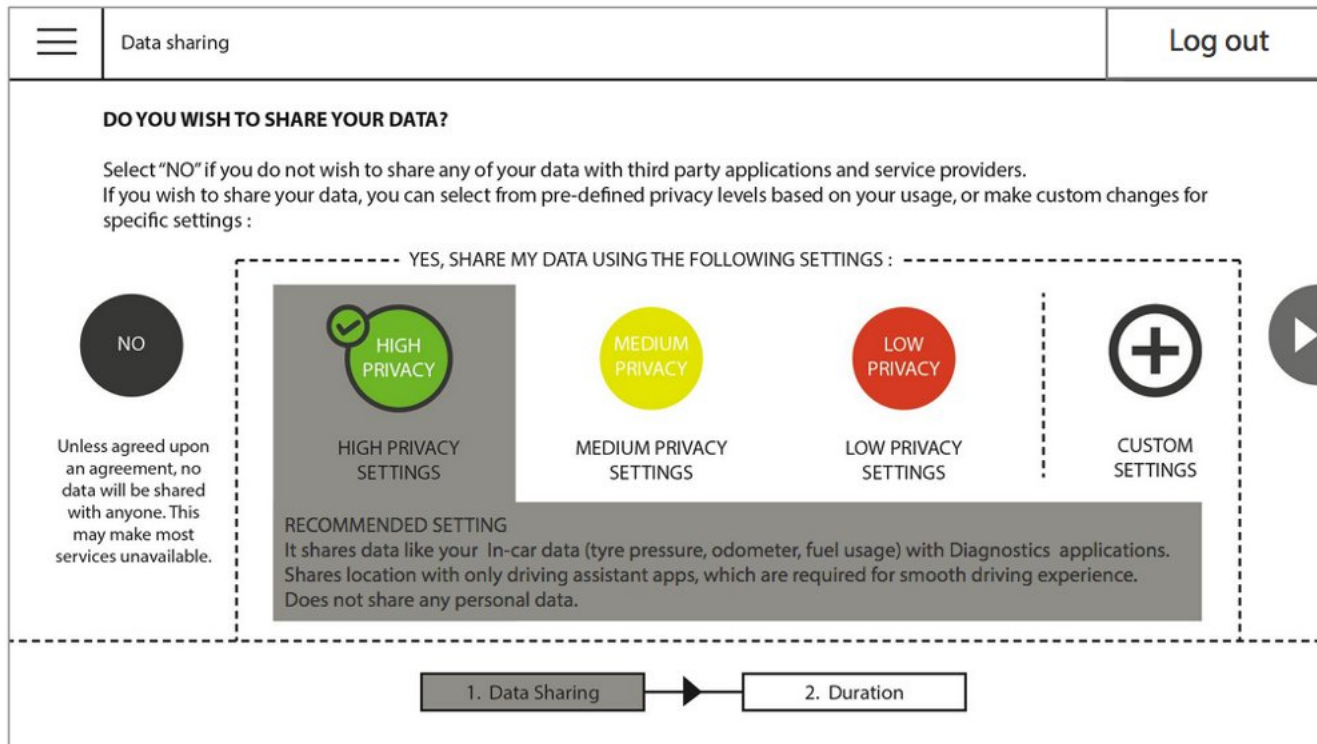


Figure 15: Information on the modes by clicking on them, for digital prototype

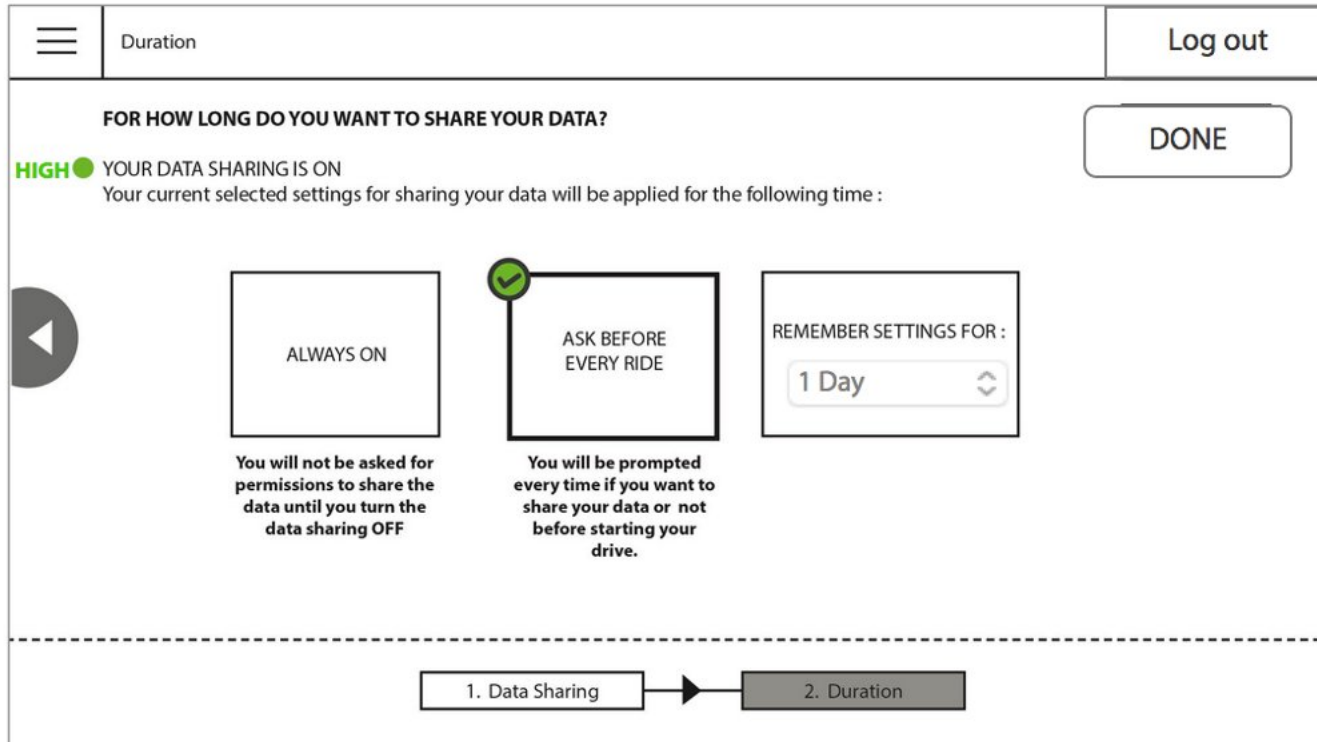


Figure 16: "Next step" Duration, for digital prototype

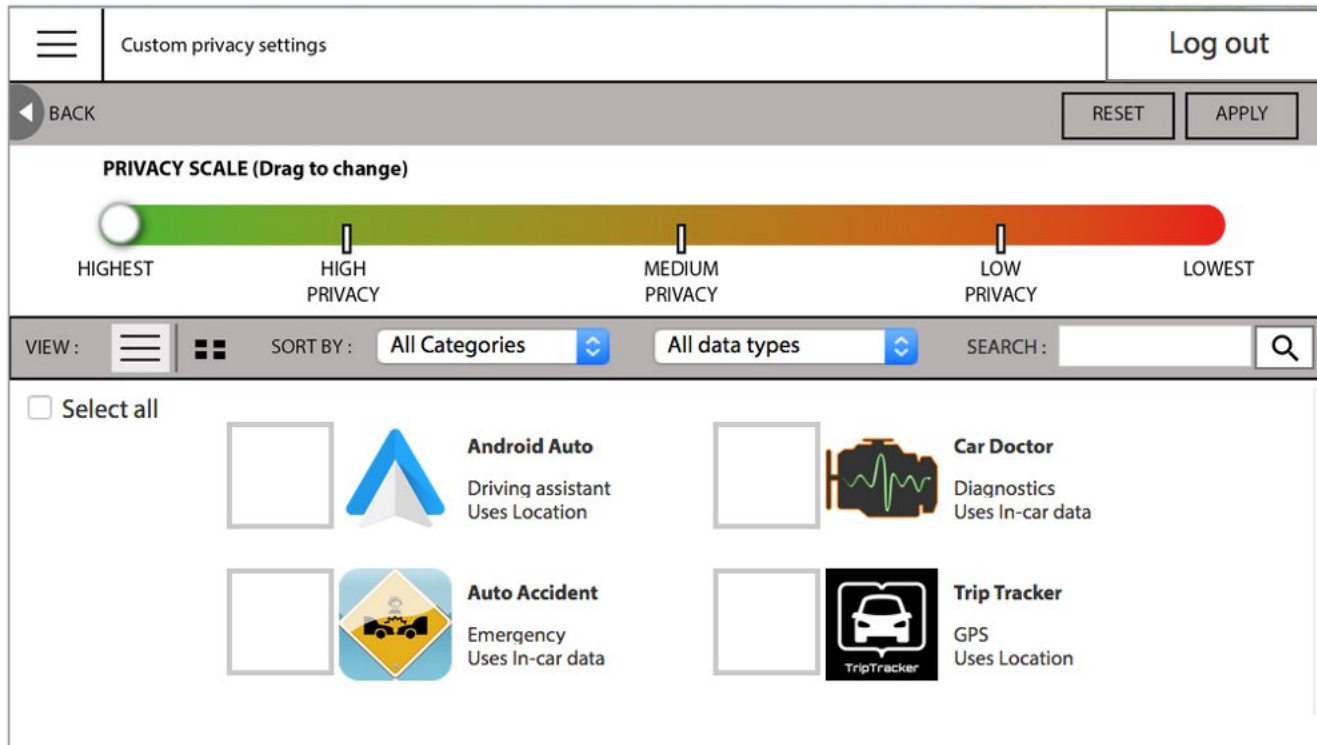


Figure 17: Home page for custom settings for digital prototype

## 5.6 User testing of Digital Hi-fidelity prototype

Based on the digital prototypes created in the previous step, a test was carried out. The following are the observations while the users performed the tasks as mentioned in section 4.6.

Table 4 : Observations based on the four tasks performed by users. Users are PT01 to PT05

Task	PT01	PT02	PT03	PT04	PT05
Pre-tasks	Tell the user when they are using for the first time, they dont know why to sign up	Tell the user when they are using for the first time, they dont know why to sign up	Tell the user when they are using for the first time, they dont know why to sign up	Taking too much time to read the tour	Selects "ask for password". Make the ask for password clear..what wil it do?
	Tour taking too much time,	Make it more intuitive to select the user profile. Like write "who's driving?"			
Task 1	Make "no" more visible on the homepage, difficult to spot	Separate the homepage from the next-next-next system	Need to make duration more clear	Easily done	Thought custom was also for duration but was too lazy to check it
	Put an option of duration in the menu, natural instinct to go there	The user thought they can go to the next into only after they select one of the levels..they read about them already before starting the task. Make it clear that those are settings			
	Go to duration if the user selects an option and clicks on it again	Put an option of duration in the menu, natural instinct to go there			
		Make it easier to go to the duration			

		option			
Task 2	On the homepage when no is selected, tell the users that clicking on the levels will give you more info	Easy to do for the user since thry already read about all the privacy settings	Reading takes too much time	Selects medium, its right. Selects them without reading	Goes to custom directly
	Thinks it should be always on - since i already selected it				Doesnt use the presets
Task 3	Confusion between highest and high. Can we make it clearer?	Need to have customise/ select the privacy level and then if you go to custom, you have already the settings shown there	Re-reading the presets- thinking something is special	Select preset and then go to custom	Goes to custom directly
	Can put a small demo about the move in privacy scale when you select/ deselct an app	can we show already how these pre-sets look like to the user before going to custom? the two pages, ie. homepage and custom settings	The hih-med-low on the privacy scale are not clear	Alternatives to scrolling - find out	
Task 4	Can have an option for alphabetic apps	Making exception - tell that to the user before going to custom settings	Thinks that emergency apps shoiuld be in medium setting	Thinks it is 'high' - then doesnt find it in high	Goes to custom directly
	Expects emergency apps to be on the top - importance wise sorting			Selects apps only from scrolling	

After the test, the users were asked to fill a System usability scale (SUS). The original format for SUS is presented in appendix B. The scores of the SUS are mentioned below. As mentioned earlier, the score ranges from 0-100, with 100 being the most usable and 0 being the least. The average score was 73.



Table 5 : SUS scores for the five participants

Participant	Score
PT01	75
PT02	75
PT03	55
PT04	75
PT05	85

The table below reflects the responses of participants against the questions asked after the test, in a semi-structured interview. The interview questions are listed in Appendix C.

Table 6: Responses of participants after the test, during semi-structured interview

Question	PT01	PT02	PT03	PT04	PT05
1. Do you think the slider is helpful if it can show you the current state of privacy/ level of privacy?	Highest and lowest - didnt understand. Could we change it to no data and all data sent	Pre-select a setting when you select it and then go to custom	Foucssed on the centre, so slider is not visible	High - custom should be high	Looks clear after explanation
	For apps - show more data on the same page				
	If we want to use only a certain data for any apps or deselect it for all apps				
	In case a new app is added, then also that type of data is not shared				

Option 1/2/3 slider	1, since it is clear	1, since you can have separate info for every app	Option 2	Option 3	Option 2
2. Are the 3 defined modes self explanatory?	Make it visual, using checkboxes etc	Yes, very clear since they read all of it	Confusion what low means	Visual is more important than text	Thought that you cant customize presets
					Choosing also means selecting, not just for info
3. Are you able to find information easily and fast?	Next button for duration not clear, it should be automatic, or ask with a popup	Give moe info about every app, very important	yes, quite easy	yes, easy	Self explanatory ; but scroll not visible on custom page
4. Do you find the product internally consistent?	Not consistent. Next would mean other privacy settings - not duration	Since tour had next-next, confused it here with the home page. Put arrows at a different place	Colors are supportive so yes	No, some pages could be more consistent	yes
	Put arrows lover or upppe for navigation, not in centre				
5. Did you think that it was too much or too less of a cognitive load for you?	Too much text. I want to do this but too much info	No, it was easy to identify the predefined levels	First time load is high	For people who only use cars but not smartphones, it could be difficult as they are not used to using tech	No, it is quite linear
6. Did you understand the conceptual model of the	Yes	yes, easy	Custom settings is not clear	Yes	Couldnt think that you can customise

app ?					settings
7. Do you think it is easy to make changes to your decisions on this app?	Yes, but selecting no should mean it never asks me again automatically and Keep no inside the box	yes, but may have to make changes again by reading everything once more	yes, easy	Yes	Yes
8. Is it easy to navigate around the application?	Yes	Yes	Yes, next is always in the middle so its easy	yes, duration and menu are nice	yes, but scroll not visible
9. Do you think it should have multiple customised settings? You can create many types of settings and save?	Yes, u dont want to change profile once uou are logged in	yes, depends on whos driiving, its better than having to switch profiles	No, since if i make a decision i would not change it often	every app can have custom settings	multiple should be there
10. Do you think the duration of the reminders is convenient? Default settings should be?	Always on	Ask before every ride, also since it would tell you which apps will be running before driving - but rather give an overview in my opinion	Always on	make duration for every app	Always on
11. Any suggestions? general feedback?	-	-	What happens when you download a new app?	How about car rentals? do they have different settings?	-

The above responses from users give insightful details about the changes that can be made to the current prototype, and those iterations are reflected both in the iteration of digital prototype and the final user interface design. The next sub-sections talk about the changes in more detail.

## 5.7 Iterations to digital prototype

Based on the observations listed in tables 4 and 6, some changes were incorporated in the wireframes. A few examples of the changes based on users feedback are listed below :

### 5.7.1 Locating the duration option

It was difficult for almost all users to locate duration tab, due to navigation issues and also it was not provided in the side menu. Almost everyone looked for it during task 1 which asked to set the duration to "remind me in a week". So the duration option is introduced in the side menu and more changes are incorporated which will be reflected in the UI design.

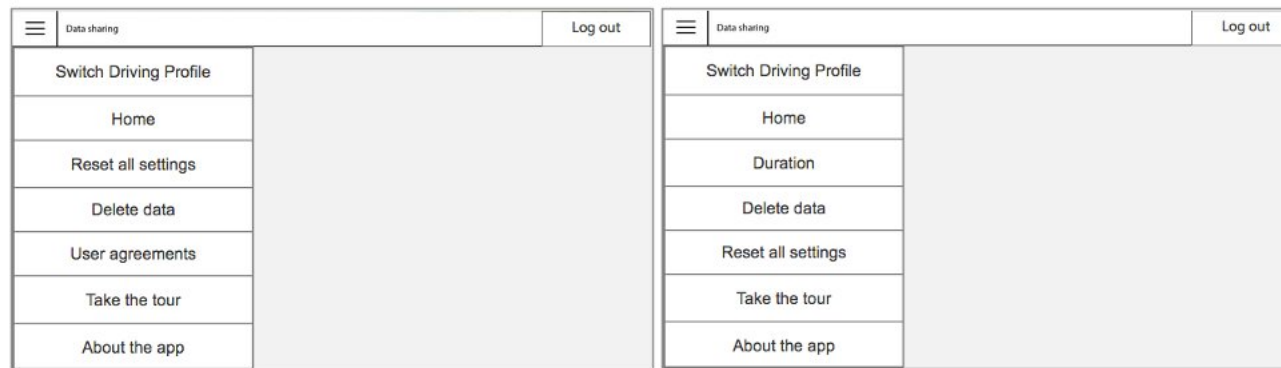


Figure 21 : Before and After for the side menu option to include "Duration" service

### 5.7.2 Making the pre-defined settings discoverable

Some users did not identify that the pre-sets can be clicked on for more information. So this variation will make it clearer.

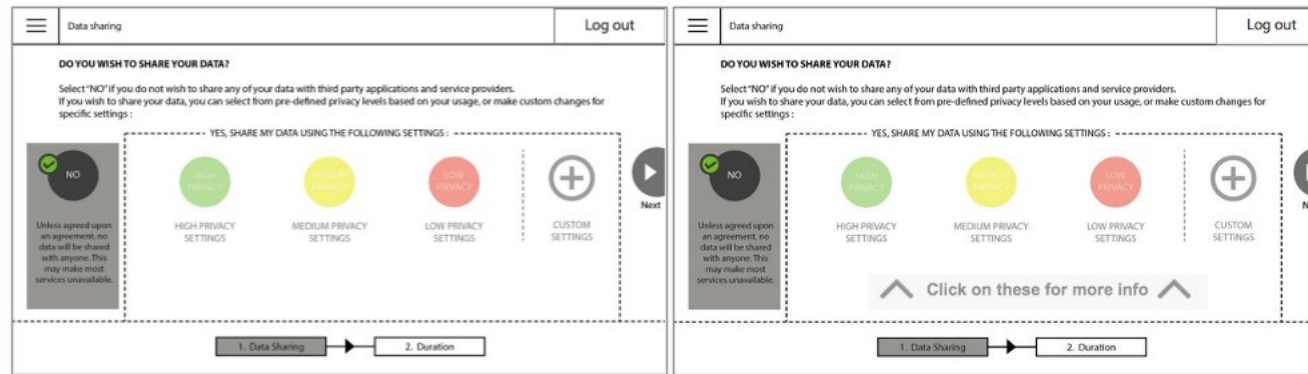


Figure 22 : Before and After for homepage where the users can know that the options contain more information

### 5.7.3 Starting the custom settings with pre-sets

A user assumed that clicking on the pre-set and then going to custom means that you can customise the pre-set. This is solved by two changes :

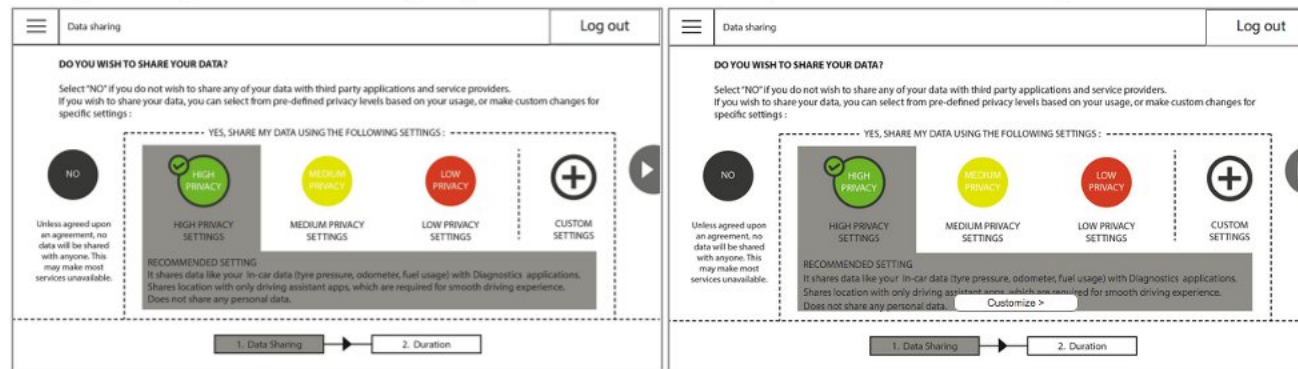


Figure 23 : Before and After for homepage where the users now know that it is possible to customize the pre-set

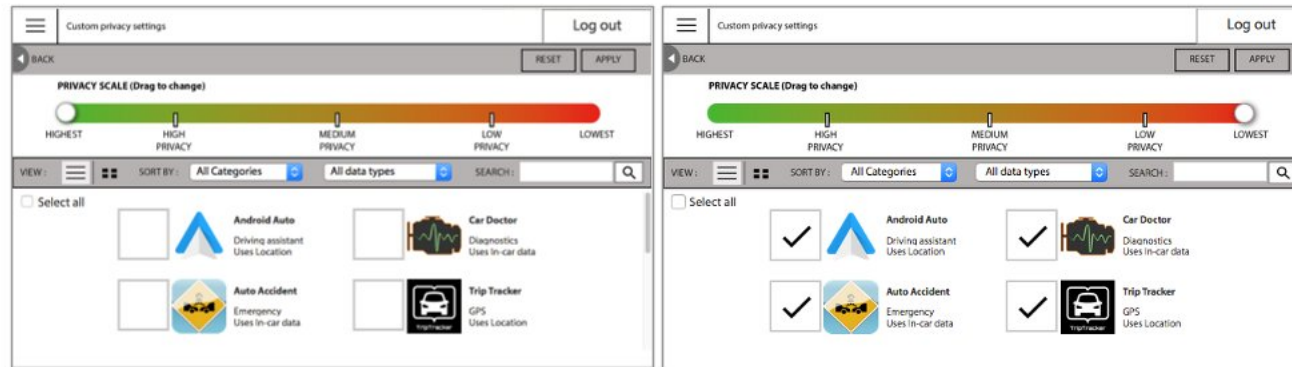


Figure 24 : Before and After for the customize page, where selecting the slider on the pre-set levels of High, medium and low will make the required changes to the applications, which the user can edit.

## 5.8 User interface design

Finally, the interface is designed for the three scenarios as mentioned : The non-driving situation, the driving situation and the smartphone application. Some important corrections are made in the non-driving situation design, after consultation with the project guide and the implementations of the user testing are reflected in the design too.

The complete design of the non-driving situation is reprinted in Appendix D.

Figure 25 is a sample of the screen designed as the homepage for the new user interface for non-driving situation.

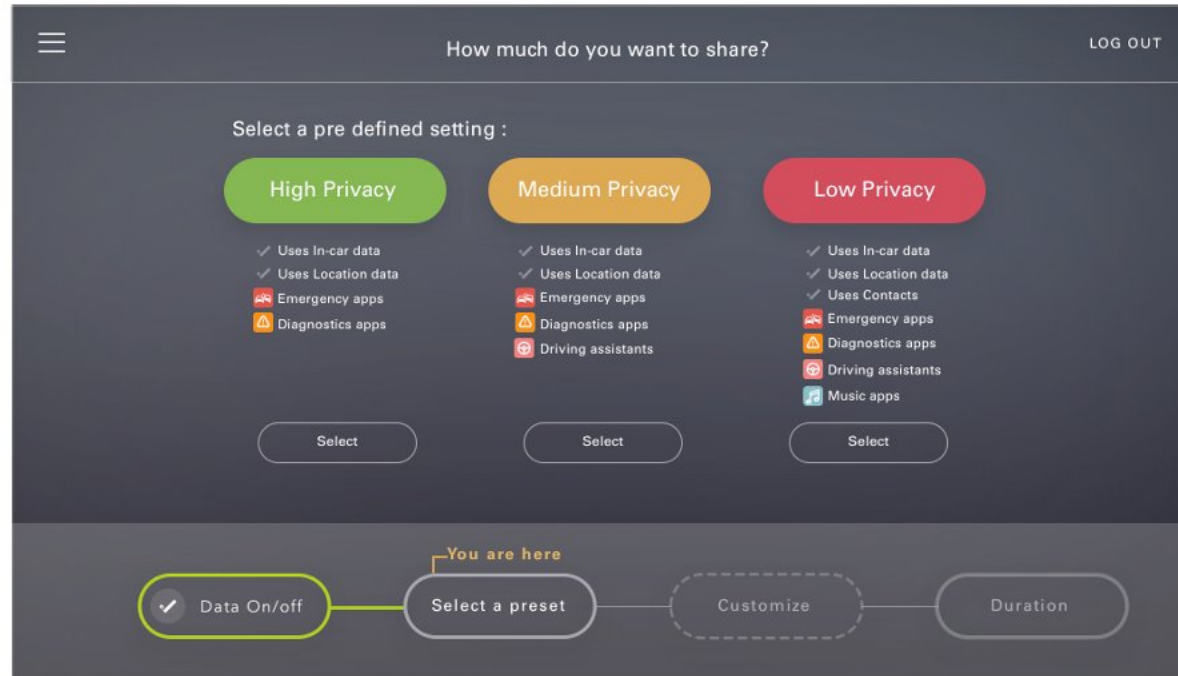


Figure 25: Homepage now consists of 4 steps instead of two, including an optional step of customizing the pre-sets. The user is guided through each step by giving feedback and directions towards next steps.

Next is the design for the smartphone application, which is based on the same design as that of the car application, but with few minor changes. The complete design of the mobile application is listed in Appendix E.

For the driving situation, a set of icons is suggested, to be always present on the top status bar of the display in the car. The icons, presented in different colors, denote the current level of privacy, and they blink and change color whenever the user triggers a new application of service which will be consuming more/ less data than current status. These icons will help the user to be warned in case his usage goes below the state he has selected, which may be getting violated in case of using extra data using applications. The icons are represented in figure 26.



Figure 26: These icons present the current privacy state. Green means high privacy, yellow is medium privacy and red is low privacy settings while driving conditions.

Another screen which may be constantly used by the driver while driving would be the overview screen, which displays what current applications are running and using data, and also how they fair on the privacy scale, is given on the screen. This screen can be accessed by the user anytime while driving to recall their current settings, but it is not possible to change the settings while driving.

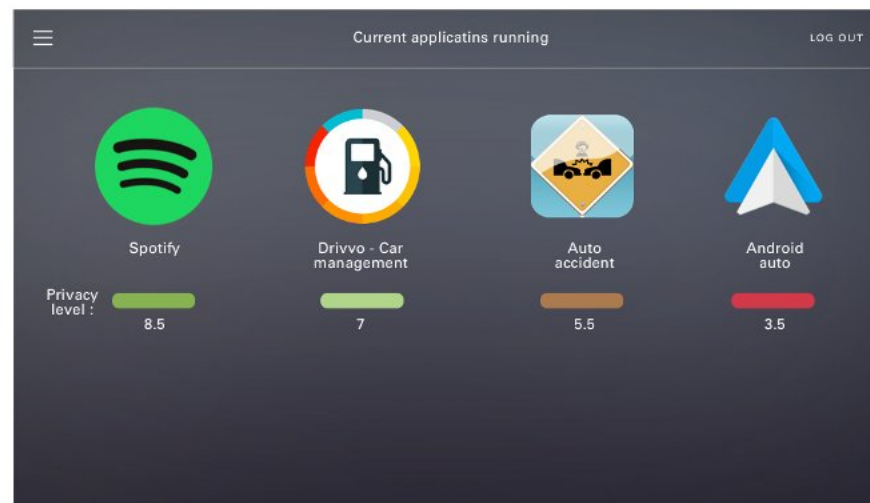


Figure 27: Overview screen which shows the applications/ services running and their privacy status



## 5.9 User testing for applications

A test was conducted while designing the user interface to decide what information is to be presented to users by providing two screenshots of the interface and asking them about the concerns for the two situations. The user profiles and their responses are recorded in table 7. The screenshots of the test are presented in Appendix G.

Table 7: The demographics of the users and also the responses when asked about the differences they would want in the current options of app overview information and app full view options

User	1	2	3	4	5
Age	33	26	29	24	24
gender	M	F	F	F	M
Driving license?	yes	Yes	Yes	No	Yes
Driving experience	10 years	10 years	11 years	1 year	5 years
Wifi in board/ Mobile mirroring/ None	Mobile Mirroring	None	Mobile Mirroring	None	Mobile Mirroring
Level of automation (0,1,2)	0	0	0	1	0
Overview options	Apps which are already sharing data should be on the top, Indicate type of App on the top	No category required, tell type of data used, and tell privacy score and how it came	Display core data being used only, and privacy score	Display privacy rating	Category is important, and the privacy rating should be colored
Full view options	The order and individual settings of data types are good. Should be on the top	reason of sharing is mostly clear, no need for that	Show trust info first, Duration is not clear	All is clear	Didn't understand purpose. Can be explained better

---

## 6 Conclusion and discussion

---

### 6.1 Requirements catalogue analysis

This section will discuss which requirements are being fulfilled by the concept, which requirements are still not fulfilled and what is the scope of improvement that can be done for the requirements. Please refer to Table 8 with the explanations against every requirement mentioned earlier in Table 1.

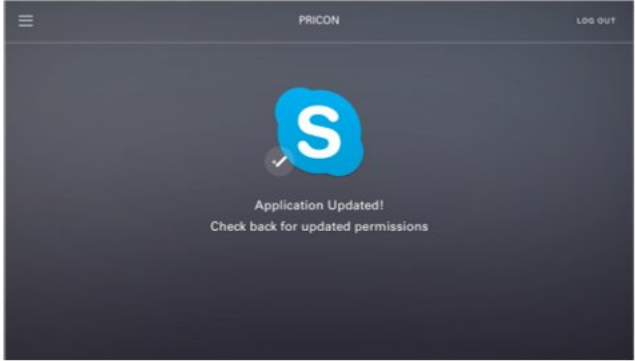
Color codes for Table 8:

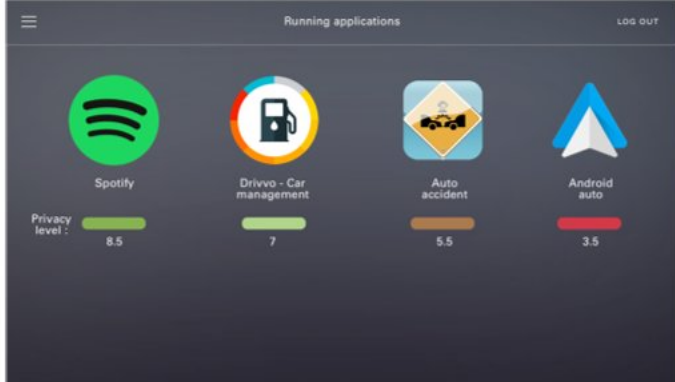
	The concept satisfies the requirement
	The concept partially satisfies the requirement
	The concept does not satisfy the requirement

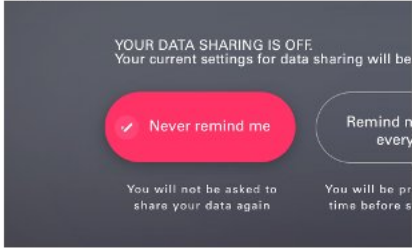
Afterwards the possible future steps are suggested and the usability testing of the application is suggested.

Table 8 : Comparison for requirements catalogue

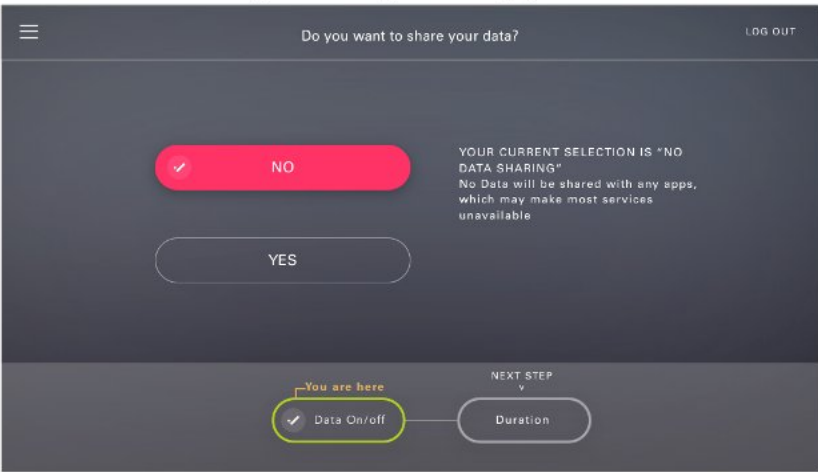
Nr	Descriptipn of the requirement	Remarks about the fulfillment of the requirement	Code
1	The displayed text should not be continuously moving text.	This is a per-se lock out requirement(applies only to driving situation) and the design for driving situation does not include any moving text	
2	A driver should not enter more than six button or key presses during a single task.	This is a per-se lock out requirement(applies only to driving situation) and the design for driving situation does not include any steps which require more than two steps for the completion of an action	

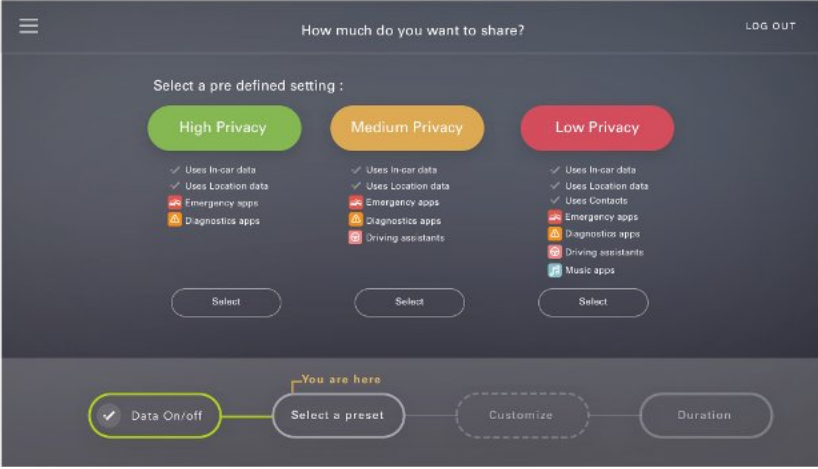

3	There should not be more than 30 characters of visually presented text.	 <p>As shown above, during per-se lockout situation, no more than 30 characters are presented.</p>	
4	When manual device controls are placed in locations other than on the steering control, no more than one hand should be required for manual input to the device at any given time during driving.	This is a per-se lock out requirement(applies only to driving situation) and the design for driving situation does not include any steps which require more than one hand for manual input, as the screen is placed in the central display area and the application offers only limited functionality during the driving scenario	
5	The maximum device response time to a device input should not exceed 0.25 second.	Yet to be tested in a driving simulation	
6	A TICS dialog shall regulate the flow of information so that it can be easily perceived	Usual dialogues while driving will update the user with any new updates, which can be easily read and understood. Refer to figure in column 3.	
7	The driver must be able to override any intervention of the system towards driving functions	The app does not let the driver change the privacy settings during driving, as the driver is asked to make a decision before driving.	
8	Systems that are not intended to be	The application does not allow the user to make changes while driving. The viewer may	

	used while driving must be deactivated or the manual must contain an appropriate warning	only view the settings as it may also prove to be distracting	
9	Glances of 1.5 seconds shall be sufficient to gather relevant information	Yet to be tested in a driving simulation	
10	System reaction time should not exceed 250 ms.	Yet to be tested in a driving simulation	
11	Displays supporting dialogue should only present symbols, signals, tell-tales, graphical elements and terminology (terms, abbreviations, etc.) likely to be understood by the driver	<p>The driving situation display does not contain extra information and a typical screen may look like the following, which is very graphic :</p>  <p>The screenshot shows a dark-themed interface titled 'Running applications' with a 'LOG OUT' button in the top right. It displays four application cards: Spotify (green icon, privacy level 8.5), Drivvo - Car management (fuel pump icon, privacy level 7), Auto accident (car crash icon, privacy level 5.5), and Android auto (blue arrow icon, privacy level 3.5). A 'Privacy level' indicator is visible on the left side of the Spotify card.</p>	
12	The particular input required to reach the intended goal should be made obvious to the driver.	Cues such as "Next step" and "You are here" are used to ensure the driver knows what is the intended goal.	
13	If the same information is presented in more than one display, at least one of the information displays shall meet the requirements of the International	The information is intended to be displayed at two screens, the dashboard and the central display. The central display complies with the international standards	

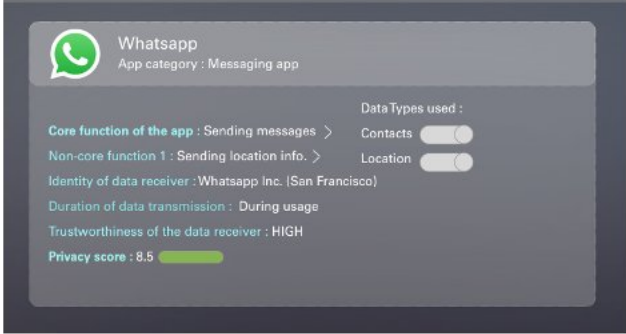
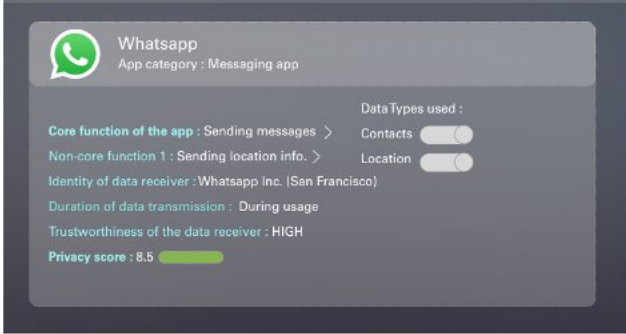
	Standard.		
14	Dynamic text, especially text related to messages that are urgent in nature, should be set in mixed or lower case, unless otherwise required by the national body.	<p>All text presented is in mixed case, such as:</p> 	
15	The x-height of the font must be atleast 70% of the Cap height of the font	The font Used, Univers LT Std fulfills the criteria.	
16	Typefaces selected should not be too light or too bold. The proportion of the stem width to the ascender height should range between 10 – 20 %.	The font Used, Univers LT Std fulfills the criteria.	
17	Typefaces selected should not be too narrow or too wide. The proportion should be between 65 – 80 %	The font Used, Univers LT Std fulfills the criteria.	
18	Typefaces selected shall be evenly and proportionately spaced and the space between vertical strokes (such as between l and m) should range between 150 – 240 % of the stem width. The space between diagonal characters and a vertical	The font Used, Univers LT Std fulfills the criteria.	

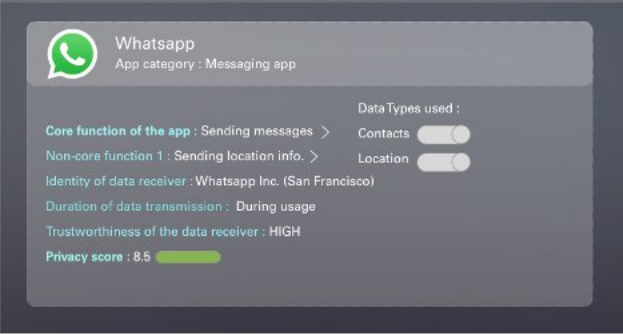
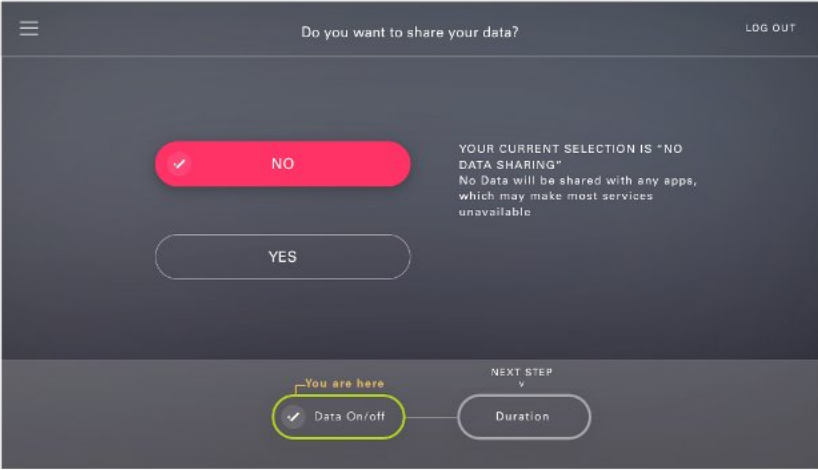
	(such as between v and l) should be a minimum of 85 % of the stem width. Two diagonal characters shall not touch. The words space is related to the intercharacter spacing of the typeface. The proportion of word space to intercharacter space can range between 250 and 300 %.		
19	The sound level must be loud enough to be well perceived but shall not startle the driver	It is decided against using the sound system for this application.	
20	The timing shall be appropriate for the type of information	It is decided against using the sound system for this application.	
21	To ensure good audibility also in case of age related hearing loss a frequency range from 400 Hz to 2000 Hz is recommended	It is decided against using the sound system for this application.	
22	For important warnings redundant visual information is required.	It is decided against using the sound system for this application.	
23	The speech recognition interface should use a broad and shallow hierarchy structure.	It is decided against using the sound system for this application.	
24	The interface should provide visual feedback and memory aids	It is decided against using the sound system for this application.	
25	The interface should provide quick access to a final speech recognition	It is decided against using the sound system for this application.	

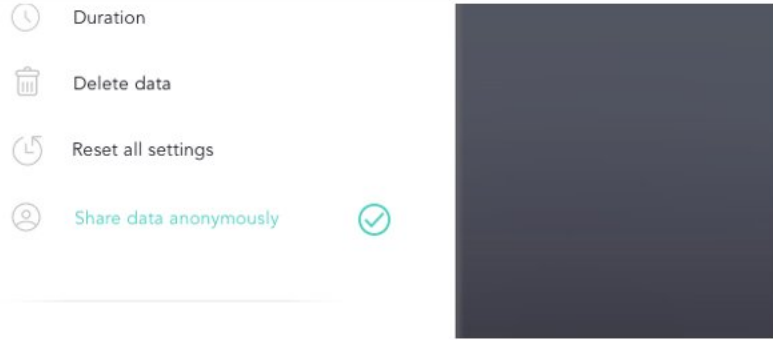
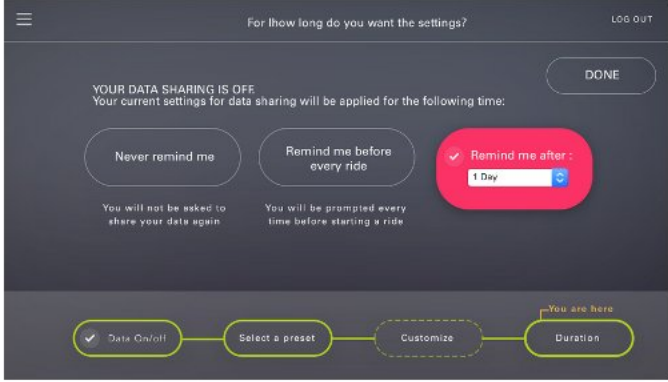
	command, by providing vocal shortcuts.		
26	The functions that the user needs immediate and quick access to should be activated by hard keys or steering wheel controls.	It is decided against using hard keys for this application	
27	The user should decide if they want to share their data.	<p>That is possible by selecting yes or no :</p> 	
28	The user should be provided with all relevant information to make a decision about sharing their data.	Information is provided at every stage of making a decision, such as the following example :	

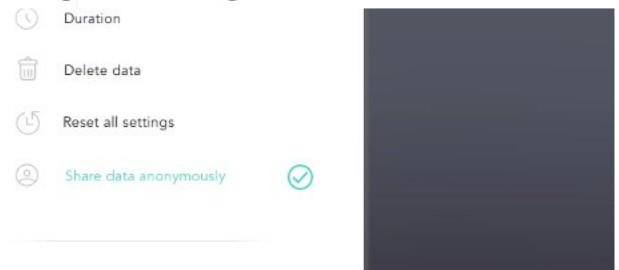
			
29	<p>The kind of party receiving the data externally should be revealed to the user</p>	<p>The kind of party using the data is revealed to the user through the app overview as well as app's profile:</p> 	
30	<p>The identity of the data receiver should be revealed to the user.</p>	<p>The identity of the receiver is mentioned:</p>	



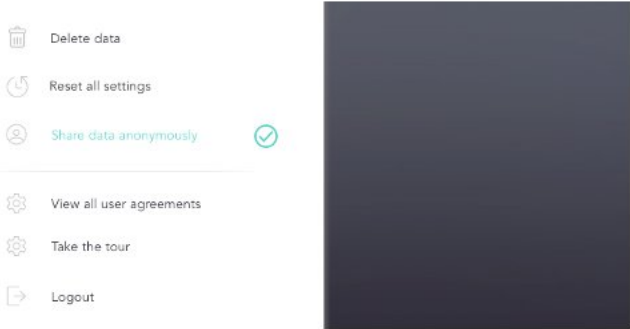
				
31	The location of the data receiver should be revealed to the user.		<p>The location of the receiver is revealed:</p> 	
32	The user should be able to decide the level of how “personal” the data is to them	The system does not decide if the data is personal to the user or not. The user is told which data is used and the user can decide for themselves		
33	The data sharing should be based on the type of function of the application.	The type of function of the application is revealed to the user in the form of core and non		

		<p>core functions :</p>  <p>The screenshot shows the WhatsApp privacy settings page. At the top, it says 'Whatsapp' and 'App category : Messaging app'. Below that, it lists 'Core function of the app : Sending messages &gt;' and 'Data Types used :'. Under 'Data Types used', there are two toggle switches: 'Contacts' (turned off) and 'Location' (turned off). Other information includes 'Non-core function 1 : Sending location info. &gt;', 'Identity of data receiver : Whatsapp Inc. (San Francisco)', 'Duration of data transmission : During usage', 'Trustworthiness of the data receiver : HIGH', and 'Privacy score : 8.5' with a green progress bar.</p>	
34	<p>The user should be able to switch off/ on all data sharing.</p>	<p>By selecting NO the user can shut off all communication:</p>  <p>The screenshot shows a dark-themed dialog box titled 'Do you want to share your data?' with a 'LOG OUT' link in the top right. There are two large buttons: a red 'NO' button with a checkmark and a white 'YES' button. To the right of the buttons, it says 'YOUR CURRENT SELECTION IS "NO DATA SHARING"' and 'No Data will be shared with any apps, which may make most services unavailable'. At the bottom, there is a progress indicator with two steps: 'Data On/off' (selected, circled in yellow, and labeled 'You are here') and 'Duration' (labeled 'NEXT STEP').</p>	
35	<p>The user should be able to share data anonymously.</p>	<p>The user can select this option in the menu :</p>	

			
36	The user should be able to choose the duration for which the data being shared with any party.	<p>The user can select the duration in the last step:</p> 	
37	Privacy protection has to be compatible with the core functions of the concerned apps as well as with the driving task.	Yes, it is compatible with the core function of the app and does not interfere with the driving task.	
38	Privacy should not reduce the usability of the general usage of the vehicular HMI.	The app does not interfere with the general usage of other applications or services	
39	The hmi has to be in line with	Yet to be tested in a driving simulation	

	current situational, cognitive and security-relevant circumstances in the car		
40	Data deletion should be possible and it should be ensured that data cannot be recovered after deletion.	<p>It is possible using this function in the menu:</p> 	
41	The HMI of the privacy app (here: wrapper app) should be intuitive and usable. Distraction should be minimized.	Yet to be tested in a driving simulation	
42	For each data usage, the data receiver has to convey the reason for data collection.	It can be verified, both internally by the programmed system, and also display it to the user in terms of core and non core functions.	
43	All affected persons must be able to control data transmission.	The possibility of creating user profiles is present, so each affected person can control data transmission	
44	Opportunities for privacy control should be laid out such that prior knowledge and situational factors like cognitive workload or motivational influences do not hinder control.	Yet to be tested in a driving simulation	
45	The user has to be aware of all control possibilities.	The possibilities of changing the privacy settings are always displayed to the user on each step	

46	The user should be informed right in the situation in which he/she has to make his/her privacy decision	This is included in the concept as the "Privacy rating" algorithm, which can be employed to rate the apps and services	
47	The car must be able to categorize the recorded, used or processed data according to its person-relatedness (relatable to a person, not relatable)	This is included in the concept as the "Privacy rating" algorithm which categorizes every app to justify how privacy compliant it is. However it still needs to be implemented.	
48	The car must be able to identify if for each single datum an user agreement is available	This is beyond the scope of the application design, to be taken care of when programming the system.	
49	Per default, each datum has to be labeled as "not agreed on".	The default settings are always set to "No"	
50	It has to be verified technically that the agreement was indeed done by the effected person and that the agreement is only applied to him/her.	This is beyond the scope of the application design, to be taken care of when programming the system.	
51	The car has to inform the user on which datum is recorded/processed/used, for what, from whom? how long/often? what are the consequences of denial?	It is informed to the user at every stage, including while making the custom choices for single applications or services, and the frequency of collection of that data and the reasons are stated at every instance.	
52	The car has to inform the cooperating system in case of data	This is beyond the scope of the application design, to be taken care of when programming the system.	

	transmission about the presence or absence of an user agreement.		
53	All agreements have to be saved in the car. the user has to be able to recall the agreements at any time point and make a denial. He or She has to be informed about the consequences of denial. The denial must not influence the application at a whole.	<p>The user can recall agreements at any time using the menu:</p> 	
54	For each data transmission the presence of an user agreement has to be verified.	This is beyond the scope of the application design, to be taken care of when programming the system.	

Upon the analysis of the requirements catalogue, it is revealed that some actions are still to be tested. These are mentioned in the next subsection.

## 6.2 Next steps for testing and future scope

The subsequent step would be testing the prototype with users, for the above mentioned pointers in the Requirements catalogue analysis in Table 8. It will include testing for the following requirements from the catalogue which need to be tested:

1. The maximum device response time to a device input should not exceed 0.25 second. (for driving situation)
2. Glances of 1.5 seconds shall be sufficient to gather relevant information (for driving situation)
3. System reaction time should not exceed 250ms. (for driving situation)
4. The hmi has to be in line with current situational, cognitive and securityrelevant circumstances in the car
5. The HMI of the privacy app (here: wrapper app) should be intuitive and usable. Distraction should be minimized.
6. Opportunities for privacy control should be layed out such that prior knowledge and situational factors like cognitive workload or motivational influences do not hinder control.

All the above requirements need to be tested for, in a driving simluation that will ensure that the application created is usable and passes all the safety norms of driving.

The scope of the project defines a privacy scale but it is yet to be materialised so that it can be incorporated in the system and the sorting of applications can become a part of the concept.

The concept has generated good interest amongst users who feel that this application is of great interest for those who are concerned about their privacy, especially in an ecosystem of connected cars which poses great threats to privacy of crucial data.

The project is based on the research done in Germany, but why and how it can be implemented in India is discussed in the next sub-section.

### 6.3 Privacy concerns in India vs Germany vs Rest of the world

To compare the behavior of smartphone users in India and Germany and their outlook towards privacy, following is a detailed elaboration of previous work done in the field. Such a literature review has enabled to draw similarities and differences in the user behavior, eventually helping to understand what fits best to the respective demographic and how should systems adapt themselves to better serve the needs of two culturally different user bases.

#### 6.3.1 India

**A User Study about Security Practices of Less-Literate Smartphone Users – Doke, P. & Lobo, S. (2016) :** This paper published the results of a user study conducted over 70 android smartphone users (37 metro, 33 rural) in India with low literacy levels to understand security and privacy behaviors while using the device

- For less literate smartphone users, such as those whose primary language is not English, the vulnerability of security and privacy cyber-attacks, as well as, the tendency of misinformed use of controls leading to a compromise of privacy and/or security is latently high
- While mitigation of automated security threats are developed using a counter reactive approach, they typically boil down to be less usable, making it especially difficult for less literate smartphone users and leading to tremendous cognitive load that adds to their inherent issues of learning and understanding
- Users do realize that smartphones are efficient information storage devices in addition to being a tangible electronic device to own, which makes them inherently interested in protecting the shared information, evident from use of vault applications and password locks to safeguard data and maintain privacy
- Although users take interest in privacy and data security, they largely depend on unreliable sources of information such as peers to understand ways to exercise the interest leading to misconceptions and sub optimal use
- Recalling passwords, especially in English, is a task with significant cognitive load, leading to compromised choices that affect overall privacy and security. Despite such easy choice of passwords, the users are completely oblivious to the fact that passwords need to be stronger and difficult to guess
- In such cases as forgotten password, the users prefer to create new accounts, thus defeating the entire concept of identity
- In cases where the user experience leads to repeated frustration, the users consider abandoning passwords altogether wherever possible, leading to highest vulnerability of security and privacy



- In case of phones shared by family members, there are certain privacy options exercised to keep objectionable content at bay, although the behavior among peers is much more open. Also, privacy options are used to ration the use of internet data as it is treated as a scarce and expensive resource
- In addition to protecting smartphone as a physical commodity, users mitigate the risk of data loss using backup measures such as creating a physical copy of digital information or backing up on some other device. The valuation of this digital data in consideration is proportional to its volume present in the device
- In conclusion, it seems that the devices and associated software are not designed for less literate users, and users have found ways to either circumvent the built security features, or avoid them entirely

**Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites – Wang, Y., Norcie, G. & Cranor L. F. (2011) :** This paper investigates the attitudes and practices of social media site users across America, China and India based on a survey and analytical comparison of the sanitized results obtained

- A survey was designed to understand behavior of social networking sites (SNS) users towards privacy. The assumption made here is that users' inherent behavior towards privacy of sensitive personal data would resonate on both SNS's as well as smartphones
- Indian users are found to be the least sensitive to privacy concerns as compared to other global peers, which is evident from the privacy sensitivity score for each respondent, obtained by averaging her/his response to the questions of the survey
- Out of all the information exposed on social networking sites, Indian users were most sensitive towards their contact numbers as a data point, while they were relatively unconcerned about residence street address, photo, email ID and employer information
- With other demographic aspects being constant, users without technical knowledge, female users, old age users and less frequent users are wary of their personal information being exposed as compared to their peers
- Another questionnaire with a different agenda from before aimed to measure the privacy concerns related to what others can do with their data on the platforms. These included questions like whether the platform has too much information about you, whether data being shared with third parties is a big concern, whether the data shared is secured
- While Indian users were still pretty less concerned about such issues, they were comparatively more worried about what others can do with their data, than what they expose their data to
- Indian users generally had the least lack-of-trust towards the system that they share their personal information on
- However, going against the general trend, Indians have a desire to restrict their personal information and wish to exercise control of information visibility so that certain people (like parents, family, co-workers) can or cannot access it

- The Indian society is considered to be between an absolutely individualistic society and a collective society, thus bringing out a cultural trend in behavior towards information privacy

### 6.3.2 Germany

**Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications – Bal, G. :** While smartphone users' privacy behavior is studied in different aspects, there is no strong method to evaluate the long-term implications of privacy decisions users make. This paper aims to introduce and leverage privacy-impacting behavior patterns to detect this long term impact

- Smartphones information processing practices are not conveyed to give a complete clarity on what the user is actually signing up for, which leads to a biased conception in the users with respect to the perception of smartphone privacy
- There is very limited knowledge of the long term effects of the lapses in privacy protection and how to effectively communicate them to the users considering the variety of sensitive resources exposed within a smartphone
- Privacy affecting behavior patterns are a central concept to reveal the privacy affecting practices in smartphones based on sensitive information flow monitoring and privacy assessment systems
- The property of specific resource being accessed by from a smartphone, like Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications, etc determine the long term impacts to a large extent
- To ensure that the above characteristics are conveyed, the privacy affecting behavior pattern is introduced with the following ideas, covering sample resource used, frequency of use, time/duration of use etc
  - Movement Profiler – example: Location information
  - Communication Profiler – example: Call history
  - Activity Profiler: example: Accelerometer
- The proposed system architecture for assessing long term impacts covers the following design principles at it's core
  - Differentiation of sensitive information flow
  - Comprehensible information
  - Sustainable awareness raising
- The key components of the system described above, that make it effective in the long term assessment are as follows –

- Monitoring – Any sensitive information flow triggered by applications in the smartphones need to be monitored via the monitoring component of the system
  - Information Flow History – Any sensitive information flow should be logged to archive a history of the same
  - Pattern Detection Engine (PDE) – This component analyses the behavior observed over a period of time to study patterns and develop insights
  - Pattern Collection – This component is a set of patterns defined prior to collection of pattern, to recognize information such as quality and quantity of information flows
  - Notification Component – This component tallies the observed activities of a system with the patterns defined above, leading to increased awareness of the long term impacts
- As a bottom-line, this exercise helps in drawing a fine balance between reducing the lack of transparency of practices that process sensitive information and avoiding cognitive overload due to high quantum of information to be processed

**Too much Information! User Attitudes towards Smartphone Sharing – Hang, A., Zezschwitz, E., V., Luca, A., D., Hussmann, H.:** This paper focuses on the attitudes and behaviors towards smartphone sharing and how it impacts the privacy of owners via a focus group & user study. The idea is to motivate strong privacy practices in smartphones that can introduce the concept of privacy-sensitive sharing of devices

- Today’s content intensive smartphones are prone to store huge amounts of sensitive user data as it acts as a personal storage device. At the same time, due to multiple relevant use cases, users have varying motivations to share their smartphones with others
- The present authentication mechanisms are all or none in their approach, making the personal data available at the disposal of those who access the device sue to sharing
- A focus group of 7 individuals (aged 22 – 27, two females) was carried out to study the current sharing behavior among smartphone users, yielding the following results
  - Access to internet was the primary motivation to share smartphones
  - The sharing behavior is categorized into two – owner initiated sharing and borrower initiated sharing
  - While the typical timespan of such sharing was limited to a few minutes, the users were concerned about the exposure of personal push notifications to borrowers
  - Most importantly, the users are concerned about intentional and unintentional changes done by the borrower
  - Theft is a concern when sharing with strangers while leakage of sensitive information is a concern when sharing with peers
  - The relation with the borrower is also an important metric determining the extent of concern over privacy issues

- Further, a user study was conducted with 18 users (average age 28, 7 females) to dive deep into the appropriate privacy practices like which application and application features would the users be willing to share. It consisted of 18 interviews lasting 60 mins each
  - 4 of the 18 participants had experienced negative impacts of sharing smartphones. This was attributed to intentional as well as unintentional actions such as changing phone settings, abusing accounts, writing text messages, or altering recommendations based on searching behaviors of the borrower (example: amazon.com). However, the negative experiences did not deter the users from sharing their devices
  - When it came to contact grouping to elaborate on sharing behavior, the average number of groups in which people categorized borrowers were 5, and the most commonly names groups included friends, family, acquaintances, myself and colleagues. Most groups had a rational or social relationship
  - While communication, organization and social media were the mJOR categories of most used applications and application features, email, notes, contacts, photos and text messages were categorized to be the most critical
  - While 68% of the applications were shared as a whole, 32% were shared based on specific application features, suggesting the need for feature level control by the device owner to grant access to partial parts of the application
  - Each group as defined above had 11 applications/features assigned to them, with most assigned to family (81), followed by friends (70) and colleagues (47). Different users have varying needs to assign application/features to groups
- The above pointers motivate the strong need for a departure from the all-or-nothing approach of sharing smartphones and address the concerns and needs of the owners to carve out an effective solution

### 6.3.3 Anonymous Users - All over the world

**AppProfiler: A Flexible Method of Exposing Privacy-Related Behavior in Android Applications to End Users – Rosen, S., Qian, Z., & Mao, Z., M.:** The research presented here conducted an analysis of 80,000 android applications to build an app called AppProfiler that was downloaded by ~1500 users aimed at allowing users to make informed privacy decisions by inducing contextual meaning to the ineffective permission system built within android

- While the permission system in android allows users to know which permissions are being asked, they are usually in the dark to understand their implications. This is being tackled here by creating profiles of privacy related application behavior. While the users are forced to believe that they are in control of privacy, just asking permissions turns out to be a false positive in creating that perception and there is a need to separate understanding application behavior from just being in control of privacy
- The permissions on an android device are usually API driven and to leverage these API calls, a series of rules are being created to interpret API calls as digestible application behaviors. These rules are termed as a “knowledge base”. Such a knowledge base helps create behavior profiles that provide more insightful information
- Such a process has multiple outputs & advantages –
  - Technical API calls are used to develop easily understandable knowledge base and behavior profiles
  - An automated script helps analyze large number of applications to judge their use of android permission systems
  - Tangibly determine the actual perceptions built by users over privacy permissions, for example high concern over the privacy implications of ad libraries & how asking for multiple permissions than necessary leads to unnecessary loss of trust in users
  - A lot of permissions are not entirely consistent with providing the information that the users need to make informed privacy related decisions
- Major limitations of the android permission systems –
  - Due to excessively widespread use of certain permissions like “Internet Access”, users majorly tend to ignore their relevant implications
  - Some permissions are very broad in nature covering vague categories and hence fail to provide the actual relevant information needed to make informed decisions. For example, “Read Phone State” gives a range of information from phone number to OS software version

- It's pretty usual a practice for applications to request access to permissions that are quite not required for effective functioning leading to false application behavior perceptions in users
- The android OS is designed in a way that makes it rigid towards any potential improvements suggested for getting the permission systems reach their objectives
- Case Studies of application behavior profiles
  - Facebook –
    - Users are concerned over the ability to access the contact number and location, particularly as the location is accessed quite frequently
    - On the other hand, the unobtrusive use of internet did not bother most users
    - This behavior shows that the permissions that deal with direct activity of users (like location access, contact number access) raise more concerns than those that run in the background with limited knowledge from the user (like internet access)
    - Although, in actuality, the application is much less aggressive in it's use of privacy related functionality, as most of the unwanted behavior is triggered by certain actions the users perform in the app
  - Angry Birds –
    - Users object about use of cookies and permissions that compromise personal identity, although the app is overall not that privacy-intrusive
    - Most of the unwanted behavior is attributed to third party ad libraries, present in many free apps
  - Reddit –
    - This is the most accepted app in terms of behavior towards privacy related permissions
    - The biggest difference is that the app does not access user location at all
    - Also, the market write-up by its developers explains in detail the role of different application features, leading to increased user confidence
- While use of third party libraries (for example to service ads) is usually associated with malicious privacy behavior, there are examples of top libraries that have optimized their functionality to meet the expected standards of user privacy, while still being commercially viable. Also, in case the code is integrated within the native code, it causes way less privacy issues compared to third party library code being inserted in the main code
- Potential areas of improvement for permission systems
  - Permissions should be spread across detailed categories to cater to specific user expectations

- Permission actions performed in the background should be clearly differentiated and properly marketed upfront as compared to those that directly interact with user actions
- Third party library code occasionally monitors user data not just within a specific app but across apps install in the OS, which certainly needs to be limited

**Location Privacy: User Behavior in the Field – Fisher, D., Dorner, L., & Wagner, D. (2012)** : The research analyzes data across 300 iOS mobile devices, to study the details of how users behave towards location services privacy, and whether there can be a predictive method to understand user choices and reduce decision-making

- There is an increased awareness in the public of the ill consequences of sharing information (especially such as location) on smartphones, to the extent that there have been legal petitions against OS providers across platforms.
- A study of user behavior shows there is a widespread variety in making privacy pertaining decisions. While most users grant location access to more than two thirds of their apps, a small amount of users go to the extent of allowing access to every app.
- Many users are selective in their choice, disallowing more than half of the apps asking for location access with outlier cases disallowing every app in this regard.
- With most users making this decision of not allowing location access to at least one app, it becomes clear that users appreciate the control of deciding location access across apps, and are not reflexively allowing so.
- Even among the most popular apps that are frequently installed in most smartphone users, some have a very high tendency to be allowed location access (upto 97% users allowing), while some were comparatively ignored in this regard (more than 50% users disallowing). This is partially attributed to the role of using user location as a utility feature of the app, ie, if location is central to the apps' features, users tend to allow much more, proving the attention users pay to the potential value of sharing location they derive
- Based on past decisions made by a user towards sharing locations as well as other users' decision pertaining to sharing location for a particular app, based on some prediction algorithms, we can predict the future outcomes upto a modest accuracy (~85%)

These predictions can be used to redirect user attention to more essential functions of the app other than location sharing by providing relevant suggestions or taking default actions based on confidence levels of location prediction

## 6.4 Conclusion

In conclusion, As one would expect, India being a developing nation has seen a recent boom in the smartphone adoption numbers, because of which the users are at a nascent stage of being accustomed to the far-reaching impacts smartphones would have on every aspect of their lives. The same goes for privacy and its long-term implications, where users are pretty ignorant and unconcerned about their personal information being shared and accessed constantly. However, it is safe to assume that the Indian ecosystem would rapidly grow more and more aware of the entire concept of privacy and personal data protection to eventually demand robust technical infrastructure supporting international standard of privacy.

Germany, on the other hand, is a comparatively mature market where users have a fair understanding of what privacy is and how it impacts them. The users are quite affirmative of their privacy choices and know what works for them and what doesn't. However, we note that despite such an evolved mindset, the smartphones do not yet support the needs of sufficiently catering to the privacy needs and demands of smartphone users. This is mainly because of platforms having a globally common way of dealing with smartphone users by providing standardized operating systems and applications and their respective features.

However, as observed in the last section above, there are certain behaviors and needs that are common across countries and are not dependent on the cultural standing of the users. Such outcomes could act as starting points to tackle global level issues, while the respective country-specific points could help establish a strong regional footprint of applications.



---

## Bibliography

---

- Allabarton, R. (2016, December 31). The UX Design Process: An Actionable Guide To Your First Job In UX. Retrieved March 17, 2017, from <https://careerfoundry.com/en/blog/ux-design/the-ux-design-process-an-actionable-guide-to-your-first-job-in-ux>
- Brooke, J. (1995). SUS-A quick and dirty usability scale. *Usability Evaluation in Industry*, 189.
- Coppola, R., & Morisio, M. (2016). Connected Car: Technologies, Issues, Future Trends. *ACM Computing Surveys*, 49. <https://doi.org/10.1145/2971482>
- Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., & Tang, J.-M. (2002). Framework for security and privacy in automotive telematics. In *Proceedings of the 2nd international workshop on Mobile commerce - WMC '02* (p. 25). ACM Press. <https://doi.org/10.1145/570709.570711>
- Hua, Z., & Ng, W. L. (2010). Speech recognition interface design for in-vehicle system. In *Proceedings of the 2nd International Conference on Automotive User Interfaces and Interactive Vehicular Applications - AutomotiveUI '10* (p. 29). ACM Press. <https://doi.org/10.1145/1969773.1969780>
- Jaisingh, K., El-Khatib, K., & Akalu, R. (2016). Paving the way for Intelligent Transport Systems (ITS): Privacy Implications of Vehicle Infotainment and Telematics Systems. In *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications - DIVANet '16* (pp. 25–31). ACM Press. <https://doi.org/10.1145/2989275.2989283>
- <http://www.repairerdrivennews.com/wp-content/uploads/2016/07/sae-autonomy-standards.jpg>
- Schoettle, B., & Sivak, M. (n.d.-a). A survey of public opinion about autonomous and self-driving vehicles in the U.S., the U.K., and Australia. Retrieved from <https://deepblue.lib.umich.edu/handle/2027.42/108384>
- Schoettle, B., & Sivak, M. (n.d.-b). A survey of public opinion about connected vehicles in the U.S., the U.K., and Australia. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 687–692). IEEE, IEEE. <https://doi.org/10.1109/ICCVE.2014.7297637>
- Wang, W., Hou, F., Tan, H., & Bubb, H. (2010). A Framework for Function Allocations in Intelligent Driver Interface Design for Comfort and Safety. *International Journal of Computational Intelligence Systems*, 3, 531–541. <https://doi.org/10.1080/18756891.2010.9727720>
- (2016). [mycarmydata.eu](http://www.mycarmydata.eu). Retrieved 24 November 2016, from [http://www.mycarmydata.eu/wp-content/themes/shalashaska/assets/docs/FIA\\_survey\\_2016.pdf](http://www.mycarmydata.eu/wp-content/themes/shalashaska/assets/docs/FIA_survey_2016.pdf)

- Stanton, N. (2013). *Advances in human aspects of road and rail transportation* (1st ed., p. Chapter XX). Boca Raton, FL: CRC Press.
- U. (2015, December 22). Complete Beginner's Guide to Information Architecture | UX Booth. Retrieved March 17, 2017, from <http://www.uxbooth.com/articles/complete-beginners-guide-to-information-architecture/>
- Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices. (2016). Retrieved 24 November 2016, from <https://www.distraction.gov/downloads/pdfs/visual-manual-nhtsa-driver-distraction-guidelines-for-in-vehicle-electronic-devices.pdf>
- Bal, G., Rannenber, K., & Hong, J. I. (2015). Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns. *Computers & Security*, *53*, 187-202. doi:10.1016/j.cose.2015.04.004
- Doke, P., Lobo, S., Joshi, A., Aggarwal, N., Paul, V., Mevada, V., & Kr, A. (2017). A User Study About Security Practices of Less-Literate Smartphone Users. *Intelligent Human Computer Interaction Lecture Notes in Computer Science*, 209-216. doi:10.1007/978-3-319-52503-7\_17
- Fisher, D., Dorner, L., & Wagner, D. (2012). Short paper. *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices - SPSM '12*. doi:10.1145/2381934.2381945
- Hang, A., Zezschwitz, E. V., Luca, A. D., & Hussmann, H. (2012). Too much information! *Proceedings of the 7th Nordic Conference on Human-Computer Interaction Making Sense Through Design - NordiCHI '12*. doi:10.1145/2399016.2399061
- Rosen, S., Qian, Z., & Mao, Z. M. (2013). AppProfiler. *Proceedings of the third ACM conference on Data and application security and privacy - CODASPY '13*. doi:10.1145/2435349.2435380
- Wang, Y., Norice, G., & Cranor, L. F. (2011). Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. *Trust and Trustworthy Computing Lecture Notes in Computer Science*, 146-153. doi:10.1007/978-3-642-21599-5\_11

---

## Appendix

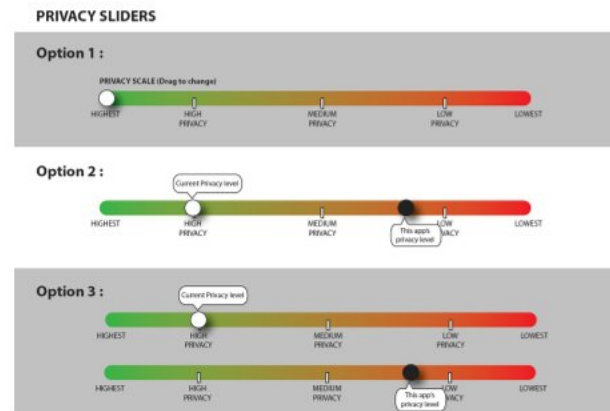
---

### A Colour specifications chart for foreground and background colour in the vehicle HMI

Background colour	Symbol colour						
	White	Yellow	Orange	Red <sup>a</sup> , Purple	Green, Cyan	Blue <sup>a</sup> , Violet	Black
White		–	o	+	+	++	++
Yellow	–		–	o	o	+	++
Orange	o	–		–	–	o	+
Red <sup>a</sup> , Purple	+	o	–		–	–	+
Green, Cyan	+	o	–	–		–	+
Blue <sup>a</sup> , Violet	++	+	o	–	–		–
Black	++	++	+	+	+	–	
++ Preferred + Recommended o Acceptable with high saturation differences – Not recommended							
<sup>a</sup> Pure red and blue should be avoided in view of the fact that the eyes may have trouble focusing on these colours because of eye chromatic aberration.							

## B Questions for Semistructured interview

7. Do you think the slider is helpful if it can show you the current state of privacy/ level of privacy whenever you make changes to any setting?
  - Choose one of the 3 options for slider :



8. Are the 3 defined modes self explanatory?
9. Are you able to find information easily and fast?
10. Do you find the product internally consistent?
11. Did you think that it was too much or too less of a cognitive load for you?
12. Did you understand the conceptual model of the app ?
13. Do you think it is easy to make changes to your decisions on this app?
14. Do you think it Is it easy to navigate around the application?
15. Do you think it should have multiple customised settings? You can create many types of settings and make changes to your decisions on this app?
16. Do you think the duration of the reminders is convenient? Default settings should be?
17. Any suggestions? general feedback?