PRICON: Self-determined privacy in the connected car motivated by the privacy calculus model

Jonas Walter
Bettina Abendroth
Technical University of Darmstadt
Darmstadt, D-64287
j.walter@iad.tu-darmstadt.de
abendroth@iad.tu-darmstadt.de

Nupur Agarwal
Industrial Design Center
Indian Institute of Technology,
Bombay, India
nupuraggarwal@iitb.ac.in

MUM 2017, November 26–29, 2017, Stuttgart, Germany

ACM ISBN 978-1-4503-5378-6/17/11.
https://doi.org/10.1145/3152832.3156627

Abstract
The advent of connected vehicles has increased the relevance of privacy in cars. Thus, a system is required that increases transparency and helps passengers to control their privacy in a self-determined manner. Here, we derive an interface based on the privacy calculus model and prove the validity of the theory-driven design approach in course of a usability test. Based on fourteen participants, we demonstrate an above-average usability of the theory-driven design which incorporates the visual comparison of functional benefits and privacy risks. Interviews reveal that users especially acknowledge this direct comparison and underscore the successful implementation of the privacy calculus model in a vehicular privacy user interface.

Author Keywords
vehicular user interface; self-determined privacy

ACM Classification Keywords
• Security and privacy~Usability in security and privacy • Human-centered computing~Empirical studies in ubiquitous and mobile computing • *Human-centered computing~Empirical studies in HCI*

Motivation and related work

Informational privacy gets more important in modern cars. While the advent of connected cars promises new functional benefits, it might turn the vehicle transparent [8]. Accordingly, the General Data Protection Regulation (GDPR), which will be the legal framework for the development of solutions for the connected car from 2018 on, demands transparency and intervenability for privacy aspects in connected vehicular services. However, common privacy interface approaches do not fulfill these requirements in a satisfactory manner [1]. In the face of unhandy privacy terms and a low controllability of data disclosure, most users do not understand the implications of their privacy decisions. Therefore, an informed decision based on a transparent communication of the privacy policy cannot be assumed [12]. Thus, a usable approach is required that enables users to decide on their informational privacy in the connected car in a self-determined manner.

Previous studies in the smartphone context have revealed promising approaches to usable privacy interfaces. While individual permissions for various data types in single services have been shown to overstrain users [7], profiles of privacy policies did support users in their privacy control [11]. Hence, profile-based privacy settings might also be an adequate solution for a vehicular privacy interface. However, especially in profile-based approaches the question of which privacy relevant information should be presented in which format still remains open. One possible solution might be provided by the consideration of the process underlying human privacy decisions. A dominant model in user-centric privacy research that attempts to describe human privacy decisions is the privacy calculus model [3]. As depicted in Figure 1, the privacy calculus model describes a privacy decision as a weighing up between perceived risks and personal interest that come with the adoption of a privacy-relevant service. A large number of studies has used this model to explain privacy disclosure in e-commerce [4], social network sites [8], location-based services [16], mobile devices [6] and the adoption of healthcare wearable devices [9]. In case of a connected vehicular application, perceived privacy risks arise with the disclosure of private data and depend on the amount and the sensitivity of data being released. In contrast, personal interest can be associated with the perceived benefits of the functions which are provided by a privacy-relevant service. Hence, the privacy calculus model predicts that informed privacy decisions in the connected car rely on the provision and relation of functions (benefits) and data being released (risks). Anticipating the current lack in usable and GDPR compliant privacy interfaces, we designed the vehicular privacy user interface PRCION that relied mainly on privacy profiles and which is strictly based on the privacy calculus model. In this paper, we present the core function of this interface

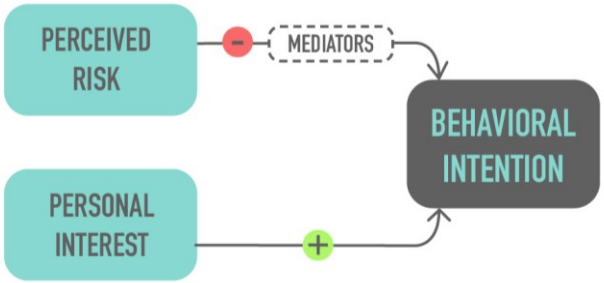

Figure 1. Simplified privacy calculus model. Adapted from [3].

and assess the hypotheses that the theory-driven design leads to an above-average usability.

Pricon

PRICON is dedicated to increase transparency in vehicular services and to enable self-determined privacy decisions (for a comprehensive description of the underlying approach, see [14]). Therefore, the application guides the user through a multistep process in which a tailored privacy setting can be chosen. Users can globally control which data are shared and can grant access permissions to individual services. In order to enable a smooth start with PRICON, an initial tour is provided for novice users. Subsequent to the tour, users can choose among predefined privacy policies or create their own custom policy. Finally, the user decides on the duration of the validity of the selected policy (ranging from "until the next ride" to "infinite"). For the sake of parsimony, we focus here on the description of the core settings, that is, the predefined policies.

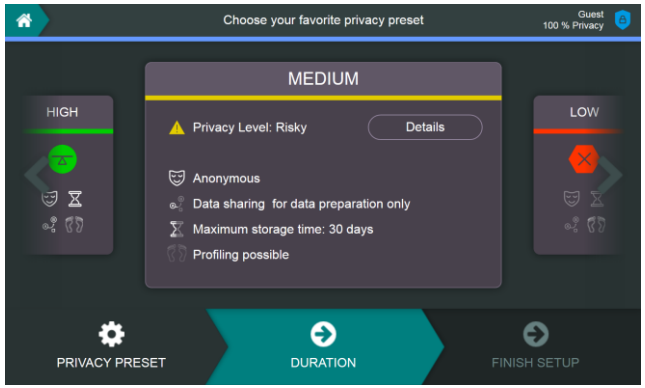

Figure 2. Selection of predefined privacy policies in the PRICON user interface.

In PRICON, privacy policies represent a comprehensive set of privacy rules that are applied on all services that are installed in the connected vehicle. As shown in Figure 2, privacy policies are described by four privacy categories "Anonymity", "Data sharing", "Storage Time" and "Profiling". The privacy factors were derived from an expert workshop with judicial privacy experts, IT experts and experts for human factors (N=7). Each privacy policy consists of a unique combination of these factors and thus allows different levels of privacy disclosure, while the amount and the quality of functions varies accordingly. As depicted in Figure 3, users can easily retrieve the effects on function availability by choosing a detailed view of the respective privacy policy. The layout of the detailed view was strongly influenced by the privacy calculus model. As both risks and benefits were theoretically predicted to be relevant for privacy decisions, we opposed risk-related privacy criteria with an overview of the available functional benefits on the same screen. However, while privacy policies are glob-

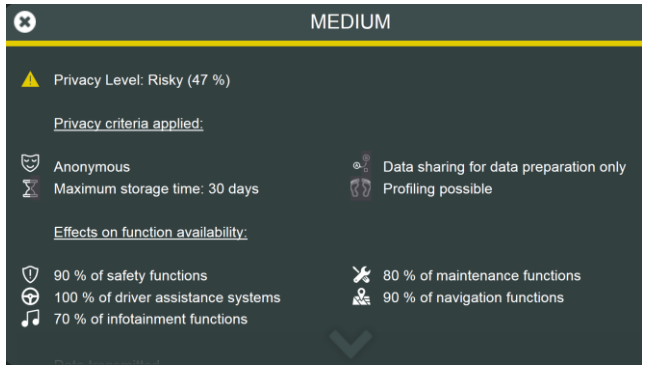

Figure 3. Detail view of a privacy policy. Privacy criteria and available functions are presented together on one screen.

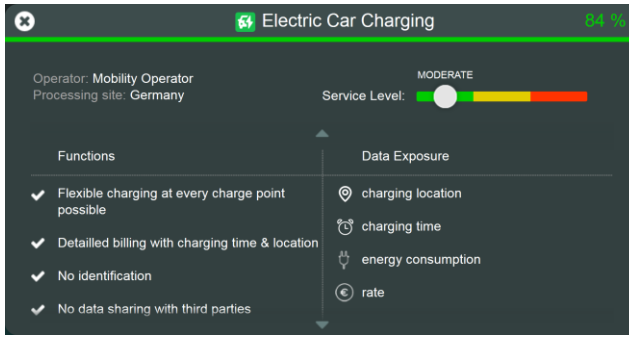

Figure 4. Service details – A tabular presentation enables the weighing up between benefits and costs.

ally applied on all services that are installed on the current vehicle, users might want to define service-specific settings. Therefore, we integrated the option for more fine-grained settings on the level of single services. If an app provider allows for multiple privacy levels, users can choose again between multiple privacy levels. In contrast to the global privacy policies, this is enabled by a color-coded slider here. Critically, the privacy calculus model was again applied such that each privacy level is again described by the comparison of risks and benefits. Here, the available functions are opposed to the data being disclosed in a tabular format (see Figure 4). Anticipating the predictions of the privacy calculus model we designed a vehicular user interface that is thought to enable users to control their privacy in a self-determined manner. In order to prove the success of this theory-driven approach we assessed the usability of the interface and elucidated if the chosen design held its promises in substituting privacy decisions.

User test

To enhance environmental validity, the usability test took place in a high-fidelity simulator. Subsequent to the usability assessment, we conducted a short interview in which we assessed if PRICON in general and the theory-driven design in specific fostered self-determined privacy decisions.

Subjects

Fourteen participants (mean age: *M* = 29.1 years; six females) who possessed a valid driving license took part in the user test. All had normal or corrected-to-normal vision and provided written consent for participation in the user test.

Apparatus and materials

The fixed-base high-fidelity driving simulator was equipped with a 180° field of view (Figure 5). Three high definition projectors with a resolution of 1920 × 1200 pixels and a luminance of 6000 lumens are used to realize this field of view. The mockup consists of a full size Chevrolet Aveo. An 8 inch Axure 8 RP wireframe was presented on a tablet (screen size: 10 inch; resolution: 1920 x 1200 pixels) that was attached to the center stack (Figure 6).

Tasks

The virtual environment consisted of rural and urban sections. Participants started on an urban road and where navigated to a parking site. Here, they were presented with a task that required the interaction with the user interface. Their task was to (1) log in to PRICON, (2) take the introductory tour, (3) select a predefined privacy policy, (4) set a reminder before every ride and (5) to define a service-specific privacy rule.

Figure 5. IAD driving simulator

Figure 6. Experimental setup in the car

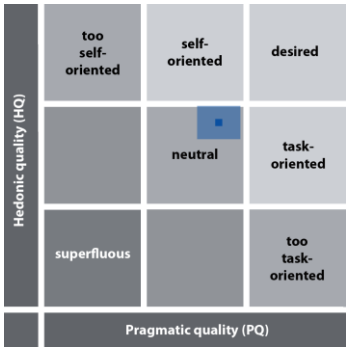

Figure 7. AttrakDiff 2 confidence rectangle for all eleven subjects

Measures

To capture the participant's thoughts while interacting with the wireframe we applied the thinking aloud method [e.g. 10]. The usability of the application was assessed using the System Usability Scale (SUS) [2], a well-established questionnaire to assess the usability of a system or product. However, usability only covers the pragmatic aspects of a user interaction with a product. In contrast, the concept of user experience offers a more holistic approach as it includes a hedonic component next to the pragmatic one. To capture both, the pragmatic as well as the hedonic components of the user interaction with PRICON, the AttrakDiff 2 [5], a questionnaire to assess the user experience of a product or system, was carried out. Finally, we conducted short interviews subsequent to the usability test. Thereby, we asked participants to recall privacy measures they are used to on their smartphone and to compare them with PRICON. Moreover, we asked how participants perceived the visual comparison of functions and data or privacy criteria, respectively.

Results

On average, participants required 1:34 minutes in order to complete the interaction task. PRICON reached a SUS score that was significantly higher than the reported average of 68 [2] (M = 74.82; sd = 8.96; $t(13) = 2.85$, $p = .014$). Moreover, there was no item that showed obvious flaws. Results for the AttrakDiff 2 questionnaire were also above average. On a 7-point scale ranging from -3 to 3, PRICON scored significantly positive on the pragmatic (M = 0.74, sd = 0.59; $t(13) = 4.73$, $p \leq .001$) as well as on the hedonic quality (M = 0.63, sd = 0.46; $t(13) = 5.15$, $p \leq .001$). Accordingly, PRICON was mainly perceived as "neutral", with tendencies towards "self-orientation", "eligible" and "activity-oriented" (see Figure 7). In subsequent interviews we intended to elucidate the potential of PRICON in general and the contribution of the theory-driven design in specific to simplify user-controlled privacy measures. To assess the effect of PRICON in general, we asked participants to recall those privacy measures to which they are used on their smartphone (e.g. data permission interface when installing a new application) and to compare them with PRICON. All participants named exclusively the data permission interface which is shown when installing a new application. Moreover, all participants stated that PRICON would provide much more control over their privacy and would make privacy decisions more transparent. Interestingly, six participants named the visual comparison of functions and privacy information as especially helpful. When asked explicitly, all participants stated that the theory-driven approach would simplify their privacy decision.

Discussion and outlook

Since the advent of connected vehicles, informational privacy has gained relevance in cars. In this paper, we present a theory-driven approach to design a vehicular privacy application that is thought to foster self-determined privacy control. Thereby, we draw back on the privacy calculus model and present benefits and privacy risk-related information when users have to make privacy decisions. The results of a usability tests as well as subsequent interviews demonstrate the success of this approach. Importantly, users acknowledged the opposition of functional benefits and privacy-related risks. Though SUS scores indicate that there is still some potential in usability improvements, this paper shows that self-controlled privacy is possible in the car

and that the theory-driven approach is perceived as being promising by users. Thus, we provide a valid approach to tackle the usability shortcomings that have been identified in common privacy interfaces [1]. While user-centric tools that encourage accurate privacy decisions were sparse in smartphones [15] and, to the authors' knowledge, inexistent in connected vehicles, we empower users to control their privacy in a self-determined manner by providing clear information about the risks and benefits of their privacy policies. In further studies we intend to use eye tracking to derive additional information from gaze patterns. For example, eye tracking studies could research if the privacy behavior that is predicted by the privacy calculus model is reflected in specific gaze patterns.

Acknowledgements

This work is supported by the German Federal Ministry for Education and Research under the project "SeDaFa: Selbstdatenschutz im vernetzten Fahrzeug".

References

1. A. R. Beresford, A. Rice, N. Skehin, R. Sohan. 2011. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th workshop on mobile computing systems and applications*, 49-54.
2. J. Brooke. 2013. SUS: A Retrospective. *Journal of Usability Studies* 8, 2: 29–40.
3. T. Dinev, P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17, 1: 61-80.
4. T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti. 2006. Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, 15, 4: 389-402.
5. M. Hassenzahl, M. Burmester, F. Koller. 2003. AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In *Mensch & Computer 2003*, 187-196.
6. M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, C. Greer. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies* 71, 12: 1163-1173.
7. P. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, D. Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *Proceedings of the Proceedings of the 16th international conference on Financial Cryptography and Data Security*. Springer-Verlag.
8. H. Krasnova, N. F. Veltri, O. Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture*. Business & Information Systems Engineering* 4, 3: 127-135.
9. H. Li, J. Wu, Y. Gao, Y. Shi. 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics* 88: 8-17.
10. L. A. Liikkanen, H. Kilpi¨o, L. Svan, et al. 2014. Lean ux: The next generation of user-centered agile development?. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. (NordiCHI '14)*, 1095–1100.
11. J. Lin, B. Liu, N. Sadeh, J. I. Hong. 2014. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *Symposium on Usable Privacy and Security (SOUPS 2014)*, 199-212.

12. B. Liu, J. Lin, N. Sadeh. 2014. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?. In *Proceedings of the 23rd international conference on World wide web*, 201-212.

13. P Papadimitratos, A De La Fortelle, K Evenssen, R Brignolo, S Cosenza. 2009. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE Communications Magazine* 47, 11, 84-95.

14. C. Plappert, D. Zelle, C. Krauß, B. Lange, S. Mauthöfer, J. Walter, B. Abendroth, R. Robrahn, T. von Pape, H. Decke. 2017. A Privacy-aware Data Access System for Automotive Applications. In *15th ESCAR Embedded Security in Cars Conference*, Berlin.

15. N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, J. Rao. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* 13, 6: 401-412.

16. H. Xu, H. H. Teo, B. C. Tan, R. Agarwal. 2009. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems* 26, 3: 135-174.