Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior

Manuel Rudolph(✉), Denis Feth(✉), and Svenja Polst(✉)

Fraunhofer IESE, Kaiserslautern, Germany
{manuel.rudolph,denis.feth,svenja.polst}@iese.fraunhofer.de
http://www.iese.fraunhofer.de

Abstract. Privacy is a vital aspect of IT systems and services, and it is demanded from users and by law. Thus, most data-processing services provide interfaces for users to support transparency (e.g., privacy notices) and self-determination (e.g., privacy settings). In this paper, we present evidence that users do not make use of these privacy interfaces—although they generally would like to. Based on our findings, we present an intention model in order to explain this behavior. The model combines aspects such as privacy demands, motivation and barriers in order to argue about the resulting intention of the user regarding the application of privacy interfaces. We show the applicability of our model by instantiating it to a concrete use case.

Keywords: Human centered design and user centered design
Psychological application for user interface · Adaptive and personalized interfaces
Privacy · Motivation · Intention

1 Introduction

Every day, users share information while using digital services. As this data is typically person related, it is of high value for users and service providers. Users benefit from data sharing by highly customized and easy-to-use services. On the other hand, providers use collected data for user profiling, personalized advertisements and other lucrative analyses. Thus, many users have a variety of privacy concerns regarding the use of these data-centric services. In order to protect users, authorities passed legal regulations to empower the users to take protective measures for personal data according to their privacy needs. For instance, the European legislature passed the General Data Protection Regulation (GDPR) [6], which imposes (among others) these two requirements:

- *Transparency:* Users must be able to understand how companies collect, use and share data in order to have a basis for decision-making.
- *Self-determination:* Users must be able to configure their own privacy needs in an easy-to-use way in order to stay in control of their personal data.

M. Kurosu (Ed.): HCI 2018, LNCS 10901, pp. 587–598, 2018.
https://doi.org/10.1007/978-3-319-91238-7_45

Since similar laws are already in place and GDPR becomes effective in 2018, many service providers already provide corresponding privacy controls for the users. However, we are facing a so-called privacy paradox [10]: Users frequently do not make use of these means, even if they say they want to [18] and have the opportunity to do so. For example, only about 20% of the European population fully read privacy notices and claim to understand how service providers use their data [5]. Unfortunately, the reasons for this paradox, their interrelations, and their underlying causes are not yet completely researched, and so far, the user's intention has not been addressed in a systematic manner [10].

1.1 Ideas and Contributions

In this paper, we present a study that investigates the reasons for not taking appropriate privacy actions. We asked more than 1,000 persons about their usage behavior regarding privacy settings and privacy notices, including the burdens they are facing. The results confirm that users rarely take available actions to protect their privacy. Half of the participants check their privacy settings only sporadically or never. Moreover, half of the participants state that they never read privacy policy notices at all, and only eight percent are reading them carefully for each service. The main reasons are similar in both cases: It takes too long to perform the privacy tasks, and the tasks are too complicated.

Before we can find solution strategies to mitigate these issues, we need to identify and understand the obstacles faced by the user. Based on the study results and previous investigations, we propose a generic intention model that contributes to the explanation of the privacy paradox. This model borrows concepts from psychology to explain the user's behavior regarding privacy interfaces. The core element in the model is intention, which is a combination of the user's motivation and different kinds of barriers. As privacy is a very individual need, we focus our work on the private user and assume that extrinsic motivation barely plays a role for privacy decisions regarding personal data. Thus, we focus on intrinsic motivation. In addition, the barriers depend on the individual user, since they arise if the user's resources do not meet the requirements emerging from the properties of privacy enhancing technologies (such as privacy settings, privacy notices). Obviously, the prerequisite for using privacy interfaces is that the user's own resources (e.g., security knowledge, cognitive load capacity and available time) exceed the required resources. If the required resources exceed the available resources, the resulting barriers will prevent the user from actually performing the actions. We identified various relevant resources for users and privacy interfaces, which we discuss in the paper. However, intention is not only a matter of available resources. Additionally, the user's motivation (i.e., cost-benefit ratio) is an important factor that needs to be considered. We claim that even if the user has a strong motivation to perform privacy actions, he frequently squanders the potential to optimize his privacy.

In this paper, we describe and interpret the user study about the user's behavior with respect to privacy-related actions in Sect. 2. Based on these results, we propose an intention model in Sect. 3. The model is exemplarily instantiated in Sect. 4. The paper ends with a discussion about related work in Sect. 5 and a conclusion in Sect. 6.

2 Usage Behavior Regarding Privacy Settings and Notices

As stated above, we mainly focus on two aspects: transparency and self-determination. While transparency focuses merely on information provision, self-determination enables users to actively control data usage. In practice, privacy notices are the most common means to ensure transparency, and many services provide privacy settings to give the user (some kind of) control. However, it remains an open question whether users really use these means and what the major burdens are for them.

2.1 Setup

One of the main goals of our study was to cover a cross section of society—i.e., to include also people without any special expertise in security and privacy. To this end, we integrated a survey in a public museum exhibition about privacy and data protection in Kaiserslautern, Germany. This gave us access to a wide range of people with different backgrounds that have at least a basic interest in security and privacy. The survey was included into an interactive security awareness quiz in order to provide an interesting exhibit. The exhibit setting prevented us from requesting text input, which limited us to questions with multiple choice answers. We used German language in the exhibit. In addition, we had little control over the participants, as they were not supervised when visiting the exhibit. For example, we cannot rule out the possibility that some visitors have participated multiple times, or dropped out early. Although this poses a threat to validity, the number of participants (1,391 within five month) minimizes the risk of invalid results.

2.2 Usage of Security and Privacy Settings

Our first question targeted the usage of security and privacy settings, as found in many online services. We asked the participants: "How often do you check your security and privacy settings?" As Fig. 1 shows, the results vary—however, only 41% 1,391 participants state that they check their security and privacy settings regularly (always or multiple times per year).

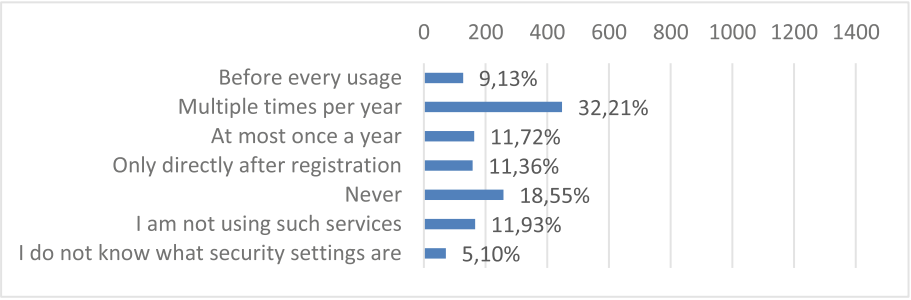

Fig. 1. How often do you check your security and privacy settings? (n = 1,391; one answer allowed)

As we were also interested in the reasons why users do not use security and privacy settings, we asked those participants that use these settings less than once a year: "Why don't you use security and privacy settings more often?" We did not ask this question to those participants who are updating privacy settings multiple times per year or more often, as we consider this behavior as acceptable. Figure 2 shows that most of the 558 participants are interested in general, but either do not think it is necessary to take action or find the provided tools too time consuming or complicated. Participants were allowed to choose multiple answers from the given five options.

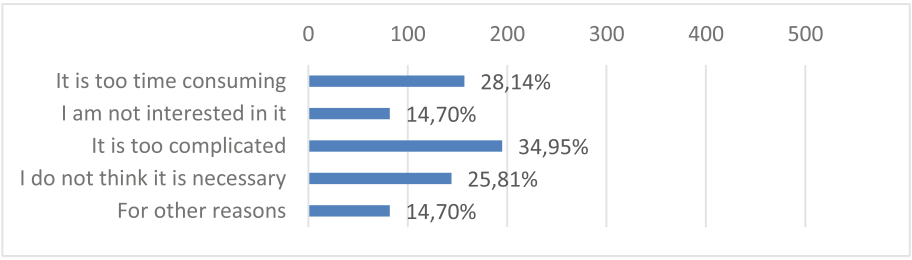

Fig. 2. Why don't you use security and privacy settings more often? (n = 558; multiple answers allowed)

This leads us to the conclusion that many users apply security and privacy settings in general—but only sporadically. The two major reasons are either that users do not think it necessary to do it more often or that the provided tools are too complicated and time consuming.

2.3 Usage of Privacy Notices

The second aspect we analyzed is the usage of privacy notices. They are an inherent part of most websites and services (also because they are partially required by law) and provide information about how a provider collects, processes and shares personal-related information. Thus, our question was "How often do you read online privacy notices?" Some participants stopped the survey before this question. As shown in Fig. 3, more than half of the 1,195 participants never read privacy notices at all. Another 25% reads them only in at most fifty percent of the cases. This means that—although privacy notices

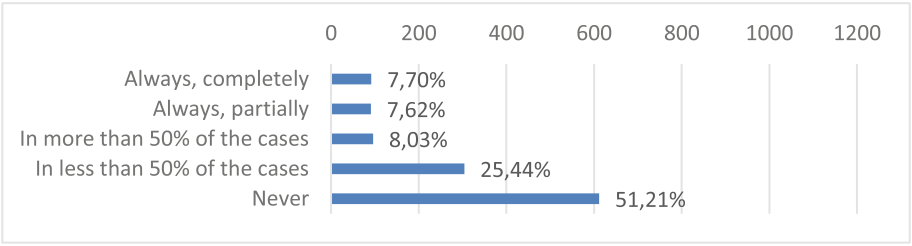

Fig. 3. How often do you read online privacy notices? (n = 1,195; one answer allowed)

are often the only information source regarding privacy—less than a quarter of the users actively use them.

As this result is quite unequivocal, we again asked for the reasons: "Why don't you read online privacy notices more often?" Although the majority stated that they don't read privacy notices, only 10% stated that they are not interested in them. The reasons for their inadvertence seem to be clear, as Fig. 4 shows: 72% of the 1,006 participants that do not regularly read privacy notices perceive privacy notices as too long. 43% also stated that privacy notices are too complicated. Multiple answers were allowed.

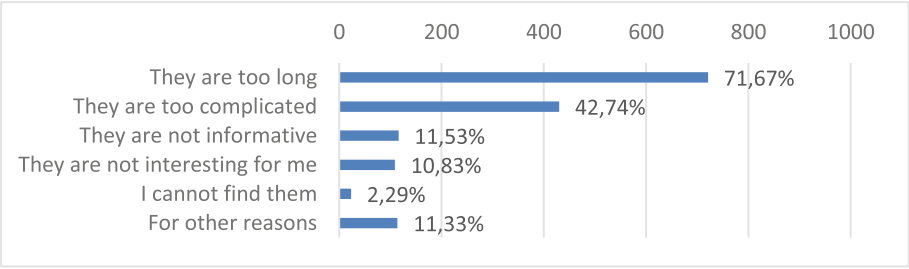

Fig. 4. Why don't you read online privacy notices more often? (n = 1,006; multiple answers allowed)

2.4 Conclusion

The study shows that many users have a basic interest in transparency and privacy control measures. However, only a minority of users can make use of these measures. Privacy settings are only applied rarely, and they are perceived as too time consuming and complicated. The same applies to privacy notices, although the gap is even more severe. Although the majority of the users is interested, almost nobody reads the notices, as they are perceived as too long and complicated.

Overall, the findings underpin the privacy paradox: Users want to protect their privacy, but they do not take action regarding this respect. We want to understand and explain this effect in order to mitigate it as part of our future work.

3 An Intention Model Explaining the Usage Behavior

The study described above confirms previous studies [14, 15], according to which users, on average, take only moderate efforts to improve their privacy settings or to retrieve information on the use of their own data in the privacy notice. In many cases, this contradicts the user's own need for privacy, which is one of the key drivers for performing privacy related activities. We consider the need for privacy as part of the humans' basic needs in terms of safety and security [12]. We concentrate on those users who are not able to carry out these tasks (i.e., configuring privacy settings and reading privacy notices) appropriately despite their existing needs. Thus, we ignore potential

unawareness of privacy issues (i.e., the lack of privacy needs). Lacking need for privacy could be compensated by awareness measures.

We developed an intention model (see Fig. 5) that abstracts existing problems (e.g., privacy paradox, too high complexity, too much time necessary) to a generic level. The model explains the discrepancy between the user's demand for the protection of his privacy (desired result) and the reality of the user ignoring his options of interaction (actual behavior).

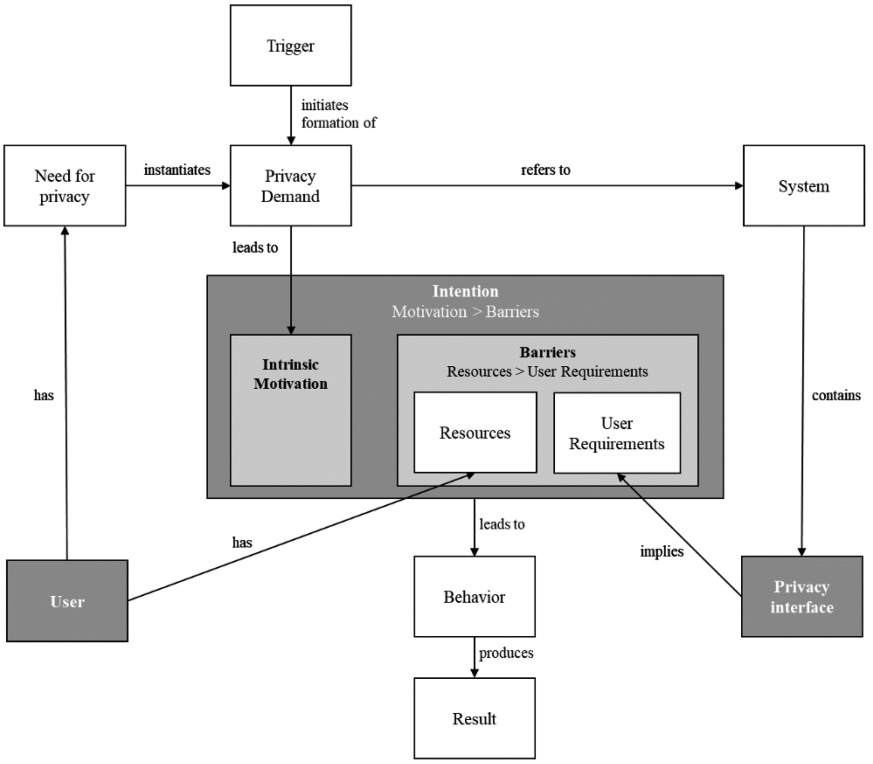

Fig. 5. Intention model

The baseline for our discussions is a private user who uses a system that processes personal-identifiable information. Processing includes collection, usage, distribution and sharing. As required by law and demanded by end-users, the system includes privacy interfaces. These privacy interfaces enable privacy-related information exchanges between the system and its users (e.g., privacy settings, privacy notices) and target transparency and self-determination. However, the utility of these interfaces depends on the behavior of the user. If the user does not use or does not want to use privacy interfaces, transparency and self-determination will not be achieved. Thus, we want to achieve a specific user behavior (i.e., usage of privacy interfaces) in order to obtain a result (e.g., specified privacy settings, understood privacy notices).

The actual behavior depends on the user's intention. The intention and its relationship to behavior is the focus of our work. Thus, we do not consider the quality of the result, as it is not directly depending on the intention.

In an ideal world, the user's intention is a direct consequence of his motivation. As the personal-identifiable information the system processes directly belongs or relates to the user, he typically has in intrinsic motivation to protect it.

Unfortunately, pure motivation is not the only factor influencing the intention. In addition, barriers come into play as a counterpart of motivation. Intention arises when the user's motivation exceeds the barriers he faces. The intention leads to the behavior of executing privacy-relevant actions. We will refine the barriers later and focus on the motivational part first.

The motivation for using privacy interfaces typically stems from situation-dependent privacy demands. These concrete demands are based on a general need for privacy and arise when the user experiences a certain trigger. The privacy demand could be, for instance, the desire to protect his personal data from abuse in a social network or to gather information about the data usage by third parties. In comparison to the need for privacy, the privacy demand does not describe a holistic need, but it refers to a certain system. Examples for a trigger are the use of a new service, a change in functionality or in the privacy notice of an existing service, or a request for additional personal data.

Table 1. User requirements vs. user resources

User requirement/ User resource	Description
Domain knowledge	Required vs. actual knowledge of the service's use cases and the personal data provided to the service necessary in order to be capable of making privacy-related decisions
Security & privacy knowledge	Required vs. actual knowledge of potential and actual use of personal data by the service and potential threats that arise from this use necessary in order to be capable of making privacy-related decisions
Technical knowledge	Required vs. actual knowledge of the functionality of the service and its privacy interfaces
Available time	Required vs. available time to apply the privacy interface
Cognitive capacity	Amount of privacy related information the user needs vs. is capable of processing simultaneously
Physical capacity	Required vs actual accessibility to a device that allows the use of a privacy interface in the respective system

As described above, barriers influence the intention. They emerge from the interrelation of the resources available to the user and the user requirements of the privacy interface. If the user has sufficient resources, he does not experience barriers. However, if the user's resources do not meet the user requirements, he experiences barriers towards using the privacy interface. As described above, the size of barriers does not directly determine the intention, but has to be exceeded by the motivation. The instantiation of the user resources and the user requirements and thus the identification of barriers strongly depends on the concrete system or privacy interface, respectively. In response

to the question regarding the reasons for the moderate use of privacy settings, users responded by about 30% each that these are too complicated and time-consuming (cf. Sect. 2.2). Both reasons represent barriers to setting the privacy settings.

We identified multiple categories for requirements, resources and barriers resulting from a discrepancy between user resources and user requirements: Domain knowledge, security and privacy knowledge, technical knowledge, available time, cognitive capacity and physical capacity. In Table 1, we explain the trade-offs between user requirements and resources for each category.

Summarizing, our intention model explains the behavior of people who have a general need for privacy, but do not take appropriate actions to enforce it. Thus, the model approaches the privacy paradox. In the following, the model is instantiated for a specific application.

4 Case Study

We instantiated the behavior model for the two main privacy interfaces on Twitter: privacy notices and settings. Twitter provides different options that are relevant from privacy perspective. Most content (e.g., tweets, likes, shares) is public by default, and there are many privacy-relevant options to connect your contact book (e.g., from Gmail), get SMS notifications, and so on. Although Twitter's primary purpose is interaction with other users, and thus, the general need for privacy might be comparably low, profiling, tracking and customized advertisements can be strong motivators for privacy. Concrete

Table 2. Potential user barriers on Twitter

Barriers	Description
Domain knowledge	The user does not know or does not remember the provided personal information and does therefore not know what to specify
Security & privacy knowledge	The user does not understand how the personal data can be used by third parties in order to decide on the individual privacy settings
Technical knowledge	The user does not know about technical possibilities for tracking his usage behavior, for example via sensors on smartphones
Available time	As it is unclear which settings should be checked how often, the user would need to check all settings on every use, which is time consuming Privacy notice has approx. 4,000 words, and is not categorized according to user tasks
Cognitive capacity	The (privacy) settings overwhelm the user with many options and much textual information Information in privacy notices are distributed over the whole text and they do not relate to concrete user tasks (e.g., what happens when you tweet)
Physical capacity	Privacy settings can be done on mobile apps and browsers and are synchronized for all devices, which could be misleading (although explicitly stated) Privacy policies are hidden in app and not optimized for navigation on mobile devices

triggers for privacy demands can stem from the usage itself (e.g., visibility of sensitive tweets), reminders by Twitter (e.g., to update your phone number after login) and external triggers (e.g., press articles about Twitter).

On the other hand, we have barriers. The privacy notice is quite long (approx. 4,000 words), formulations are vague and information is distributed throughout the document. This increases the burdens for the users regarding cognitive load, needed time, etc. and prevents them from reading the privacy notice. In addition, the settings are distributed over 15 categories, which makes it time and effort consuming to maintain them. In response to the question regarding the reasons for the moderate use of privacy settings, users responded by about 30% each that these are too complicated and time-consuming. Both reasons represent barriers to setting the privacy settings. In Table 2, we show examples for burdens we identified in the categories presented in Sect. 3.

Of course, this instantiation is not a comprehensive evaluation and lacks certain details, as we could not perform large-scale user studies regarding Twitter's privacy interfaces. This is part of our future work, in which we analyze the applicability and completeness of our model in depth.

5 Related Work

Studies regarding the frequency of use of privacy notices have been performed by Moallem [14] and Obar and Oeldorf-Hirsch [15]. Our study confirms the results of these studies, but has eight/2.5 times more participants, respectively, cross-sectional through society. To improve the acceptance of privacy notices, there exists work targeting readability [4, 13], understandability [17] and design [20] of privacy policies. All these improvement aspects are important and could benefit from our intention model as a baseline for requirements. The consequences of lacking acceptance of privacy notices have been analyzed in different surveys [15, 18, 19]. This is relevant for our work insofar as the (expected) consequences affect on the user's intention towards privacy notices.

Boyd investigated reasons for users not to configure privacy settings in Facebook [3]. She found that both frequency and type of Facebook use as well as Internet skill influence the user behavior regarding privacy settings configuration. This underpins the prominence of the barriers in our model, as the increase of knowledge may influence the user's behavior. Research was also carried out to improve the usability of privacy settings and policy specification, respectively. Johnson, Karat, Reeder et al. proposed guidelines for the implementation of usable policy authoring interfaces [8, 16]. Their work includes amongst others the following guidelines, which we consider as relevant input for the user requirements of privacy interfaces: Limitation of expressivity, consistent terminology and communication of threats and risks. Ben-Asher found out that users behave differently with respect to system usage, if they are prompted with security warnings [2]. They behave more cautiously and adjust security settings more frequently if they are triggered appropriately. Liu et al. investigated the discrepancy between desired and actual privacy settings in Facebook [11], i.e., problems users are facing when their positive intention already made them specify their privacy requirements.

Our intention model was inspired by theories and models that try to explain human behavior, but are not focused on privacy. The key element 'intention' was inspired by the theory of planned behavior (TPB) by Ajzen [1] and by the behavioral model for persuasive design by Fogg [7]. The elements 'perceived behavioral control', 'intention' and 'behavior' of the TPB are included in our model. The perceived behavioral control is part of what we call 'barrier', intention is equivalent to 'motivation' and the term 'behavior' is used in the same way. Fogg's behavioral model inspired the interrelation of motivation and barriers. Fogg's model and especially its graphical representation illustrates that motivation need to be higher than the so-called simplicity factors. These simplicity factors are a positive formulation of barriers [8]. The element 'need for privacy' was inspired by the well-known hierarchy of needs by Maslow [12]. According to Maslow, "The organism is dominated and its behavior organized only by unsatisfied needs [12] ". We consider the need for privacy to be a subset of Maslow's need for safety/security. In our model, we assume that users whose need for privacy is satisfied will not take action for protecting their privacy.

The Privacy Paradox describes the dichotomy between the need for privacy and the actual behavior of users with respect to taking privacy-relevant actions. Kokolakis et al. conducted a meta study in order to summarize all findings from the state of the art regarding the privacy paradox [10]. They outlined multiple explanations for this phenomenon, but not the challenge of mastering barriers that we claim in our paper and which is underpinned by our study results.

6 Conclusion

In this paper, we presented the results of a study regarding the situation of users dealing with privacy-related actions, proposed an intention model to explain the findings of our study and applied this model to an example application. In our study, we asked more than one thousand visitors of a museum exhibition on security and privacy how strictly they carry out privacy-related actions. Half of the participants check their security and privacy settings in online services only once a year or less—mainly because those settings are too time consuming or too complicated. Regarding the attention to privacy notices of online services, only half of the participants read them at all, although only 10% claimed that they are not interested in them. Similar to settings, participants perceived privacy notices as too time consuming/long (70%) and too complicated (41%). We conclude that many users have a basic interest in privacy-related actions (privacy settings and privacy notices). However, a significant number of participants encounter barriers when it comes to taking actions regarding privacy.

Therefore, we wanted to find out what those barriers are and how they influence and explain the user's behavior of not taking appropriate privacy actions. To this end, we developed our intention model. The model explains the relationships between the user's need for privacy, his motivation, his intention and the resulting behavior of performing privacy actions. Mainly, we reason about how discrepancies in the user's resources and the usage requirements of the privacy interfaces lead to barriers that prevent users from performing privacy-related actions, regardless of his motivation. We defined the user's

intention to use privacy interfaces as his motivation being high enough to overcome potential barriers. Our model is based on observations and experience regarding users carrying out privacy actions, as well as on the results of the study described in this paper. It respects and partially reuses terms and relations from other psychological models.

In order to obtain first evidence for the applicability of the model, we instantiated it for Twitter's privacy interfaces. The case study shows that the model can explain correlations between user behavior, the users' need for privacy and their intentions. Obviously, this instantiation is not yet a comprehensive evaluation of our model. We will apply the model in a large-scale study in order to validate its correctness in near future. We plan to let different user types who have different sets of resources use different types of privacy interfaces. Next, we will correlate user behavior, user acceptance of the privacy interfaces and correctness of results in order to obtain evidence of potential barriers as well as to derive mitigation strategies for preventing barriers for specific user types.

Acknowledgements. The research presented in this paper is supported by the German Ministry of Education and Research projects "Nationales Referenzprojekt für IT-Sicherheit in der Industrie 4.0" (IUNO) (grant number 16KIS0328). The sole responsibility for the content of this document lies with the authors.

References

1. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)
2. Ben-Asher, N., Meyer, J., Moller, S., Englert, R.: An experimental system for studying the tradeoff between usability and security. In: International Conference on Availability, Reliability and Security, pp. 882–887 (2009)
3. Boyd, D., Hargittai, E.: Facebook privacy settings. Who cares? First Monday **15**(8) (2010)
4. Ermakova, T., Fabian, B., Babina, E.: Readability of privacy policies of healthcare websites. In: Wirtschaftsinformatik (2015)
5. European Commission: Special Eurobarometer 431 - Data Protection (2015). http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. Accessed 15 Feb 2018
6. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679. Accessed 15 Feb 2018
7. Fogg, B.J.: A behavior model for persuasive design. In: Proceedings of the 4th International Conference on Persuasive Technology, p. 40. ACM (2009)
8. Fogg, B.J.: What causes behavior change? (2016). http://www.behaviormodel.org/index.html. Accessed 15 Feb 2018
9. Johnson, M., Karat, J., Karat, C.-M., Grueneberg, K.: Optimizing a policy authoring framework for security and privacy policies. In: Cranor, L.F. (ed.) Proceedings of the Sixth Symposium on Usable Privacy and Security. The Sixth Symposium, p. 1, Redmond, Washington, New York, NY. ACM (ACM Digital Library) (2010)
10. Kokolakis, S.: Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Secur. **64**, 122–134 (2017)

11. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing Facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, pp. 61–70. ACM (2011)
12. Maslow, A.H.: A theory of human motivation. Psychol. Rev. **50**(4), 370 (1943)
13. Milne, G.R., Culnan, M.J., Greene, H.: A longitudinal assessment of online privacy notice readability. J. Public Policy Mark. **25**(2), 238–249 (2006)
14. Moallem, A.: Do you really trust "privacy policy" or "terms of use" agreements without reading them? In: Advances in Intelligent Systems and Computing, vol. 593, pp. 290–295 (2018)
15. Obar, J.A., Oeldorf-Hirsch, A.: The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. In: The 44th Research Conference on Communication, Information and Internet Policy (2016)
16. Reeder, R.W., Karat, C.-M., Karat, J., Brodie, C.: Usability challenges in security and privacy policy-authoring interfaces. In: Baranauskas, C., Palanque, P., Abascal, J., Barbosa, S.D.J. (eds.) INTERACT 2007. LNCS, vol. 4663, pp. 141–155. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74800-7_11
17. Reidenberg, J.R., Breaux, T., Carnor, L.F., French, B., Cranor, L.F., Grannis, A., Graves, J.T., Liu, F., Mcdonald, A., Norton, T.B., Ramanath, R., Russell, N.C., Sadeh, N., Schaub, F.: Disagreeable privacy policies: mismatches between meaning and users' understanding. Berkeley Technol. Law J. **30** (2014)
18. Symantec: State of Privacy Report (2015). https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf. Accessed 15 Feb 2018
19. Tsai, J., Egelman, S., Cranor, L., Acquisti, A.: The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study (2007)
20. Waldman, A.E.: Privacy, Notice, and Design (2016)