Mitigating Privacy Concerns by Developing Trust-related Software Features for a Hybrid Social Media Application

Angela Borchert[1], Aidmar Wainakh[2], Nicole Krämer[3], Max Mühlhäuser[2] and Maritta Heisel[1]
[1]*Software Engineering, University of Duisburg-Essen, Duisburg, Germany*
[2]*Telecooperation Lab, Technical University of Darmstadt, Darmstadt, Germany*
[3]*Social Psychology, University of Duisburg-Essen, Duisburg, Germany*

Keywords: Hybrid Social Media, Information Privacy Concerns, Trustworthiness, Requirements Engineering.

Abstract: As the past has shown, many providers of social media services consistently demonstrate an insufficient commitment to user privacy. This has led to an increase in users' privacy concerns. Several privacy-preserving alternatives were proposed in the research community and the market. However, these platforms face the challenges of proving and demonstrating that users' privacy concerns are addressed within their scope as well as gaining users' trust. In this work, we mitigate privacy concerns and enhance the trustworthiness of privacy-preserving social media, in particular a hybrid social media application. For that, we develop trust-related software features elicited with the TrustSoFt method. We evaluate the impact of the specified features on the privacy concerns as well as on the trustworthiness of the examined application by conducting an extensive user study. Furthermore, we analyze the relationships between *information privacy concerns*, *trusting beliefs*, *risk beliefs*, and *willingness to use* in the context of hybrid social media. Results reveal the special importance of addressing particular concerns, such as "Awareness of Privacy Practices".

1 INTRODUCTION

In today's society, social media is one of the essential means of communication. People use it for online self-presentation, the exchange of information, and social interaction. Unfortunately, social media providers (e.g., Facebook) have shown consistently insufficient commitment to user data and privacy protection in the past (McCandless, 2019). Data scandals like the Facebook tokens hack in 2018 (Guardian, 2018b) and Cambridge Analytica (Guardian, 2018a) revealed that user data was prone to unauthorized access, has been used without consent against terms of use, was passed on to third parties like data brokers, or has been misused in various other ways. Especially the Cambridge Analytica breach has increased people's privacy awareness leading to more privacy concerns and less trust in social media providers (Kozlowska, 2018).

To address the users' privacy concerns, several privacy-preserving social media technologies were proposed (Salzberg, 2010), (Daubert et al., 2014), (Wainakh et al., 2019). These proposals aim to empower users by eliminating the centralized control of the service providers. This goal is achieved mainly through establishing distributed installations or Peer-to-Peer networks, where the content (posts, profiles, likes, ...) is encrypted and stored in a distributed fashion (Wainakh et al., 2019). Although the underlying technologies used in these solutions are designed to mitigate several privacy concerns, they often fall short of gaining the users' trust. This is due to multiple reasons, such as the novelty of their concepts (Wainakh et al., 2019); users often refrain from using novel technology as they cannot be sure it is safe and works as expected. In addition, some of these solutions lack to adequate explanations of the privacy-preserving practices they follow, or use poor user interfaces, which leave a negative impact on the user experience.

In this work, we aim to enhance the trustworthiness of privacy-preserving social media. We attain this objective by developing trust-related software features, which focus on the graphical user interface. By applying the software engineering method Eliciting Trust-Related Software Features (TrustSoFt) (Borchert et al., 2020b), features are specified that address users' privacy concerns (Malhotra et al., 2004). We showcase the validity of our approach by conducting a user study with over 2300 participants, who use an exemplary privacy-preserving social media application, which is hybrid social media (HSM) (Wainakh et al., 2019). In

Borchert, A., Wainakh, A., Krämer, N., Mühlhäuser, M. and Heisel, M.
Mitigating Privacy Concerns by Developing Trust-related Software Features for a Hybrid Social Media Application.
DOI: 10.5220/0010450302690280
In *Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2021)*, pages 269-280
ISBN: 978-989-758-508-1

this study, first, we analyze the relationships between the privacy concerns, trust beliefs, risk beliefs, and the willingness to use an HSM application. Then, we measure the impact of the elicited features on the privacy concerns and the trustworthiness of the application.

2 HYBRID SOCIAL MEDIA

Social media sites mostly offer their services without (monetary) costs to their users. However, the providers rely on making profits from their users' data, mainly by realizing targeted advertisements. Pioneer commercial social media (CSM) have attracted a massive number of users. By that, those CSMs dominate the market and impose themselves as almost inevitable tools in our modern society. While being inevitable, the service providers show consistently insufficient commitment to the privacy of their users (Larson, 2017; Larson, 2018; Tufekci and King, 2014). The privacy-preserving social media (PPSM) alternatives (Salzberg, 2010; Graffi et al., 2008) focus on avoiding the intrusion of their users' privacy; however, these systems are not well-adopted by the users due to many reasons (Wainakh et al., 2019), such as poor functionality (Luo et al., 2011), high usage complexity (Salzberg, 2010), and low scalability (Daubert et al., 2014).

The main idea of HSM is to combine CSM and PPSM (Wainakh et al., 2019). That combination enables users to profit from both the market penetration of the commercial one and the privacy of the privacy-preserving one. CSM provides the user base as well as the connectivity between these users, while PPSM is established logically above. It provides users with additional means of private communication beyond the knowledge of the provider of CSM. In other words, the objective of HSM is providing the users of commercial media with additional functionality to empower them to preserve their privacy by establishing a privacy-preserving network on top of the CSM.

One of the key techniques of PPSMs to achieve privacy is the elimination of central entities. As such, there is no central company that controls all user data. Thus, PPSMs should be mainly based on distributed technologies to realize the three essential functionalities for social media: (1) storage, (2) access control, and (3) connectivity. In addition, PPSMs should provide high transparency. Therefore, the design of the system should be public, and the implementation of the software should be open source. All procedures and operations need to be explained and clearly articulated in easy-to-understand materials.

Wainakh et al. (Wainakh et al., 2019) have realized a prototype to prove the viability of the HSM concept. They have built an Android app on top of Twitter, and it was later called *hushtweet*. The main functionalities of hushtweet are:

1. Anonymous like: a user can like a tweet without disclosing their identity. Thus, this like cannot be used to track their behavior or preferences on Twitter.
2. Private tweet: a user can tweet to a private network, where only their followers can access the tweet. In the private network, the tweet is encrypted and stored on a distributed database.
3. Statistical information: hushtweet collects information about the user population that are unlinkable to individuals. Example: 30% of hushtweet users mentioned the U.S. election in a tweet. This information is passed to Twitter as a compensation for using their services by hushtweet users.

More technical details on hushtweet can be found in (Wainakh et al., 2019).

3 PRIVACY CONCERNS, TRUST, AND RISKS

Information privacy describes "the ability of the individual to personally control information about one's self" (Stone et al., 1983). In the last few years, an increasing number of people are concerned about their information privacy (Kozlowska, 2018). This supports the belief of many researchers that information privacy is one of the most important ethical issues of the information age (Mason, 1986; Smith et al., 1996). Smith et al. (Smith et al., 1996) and Malhotra et al. (Malhotra et al., 2004) have identified the most prominent information privacy concerns, which are introduced as follows.

Awareness of Privacy Practices. This means the degree to which an individual is aware of organizational information privacy practices. It relates to justice, which can be distinguished in interactional and informational justice. While interactional justice relates to transparency and the propriety of information during interoperating processes, informational justice denotes the disclosure of specific information. The awareness of privacy practices has an impact on people's perception of fairness.

Collection. People are concerned about the amount of personal data possessed by third parties. They weigh the costs of disclosing personal information against the gained benefit of the received service. Again, perceived fairness is impacted.

Control. Control concerns encompass whether individuals are able to decide on certain procedures concerning their personal data like approving, modifying, rejecting or opting-out. Control relates to the principle of procedural justice and exercising freedom.

Errors. Concerns about errors involve the apprehension that organizations make too little effort in minimizing problems originating from errors in personal data. Such errors may be accidental or intentional like maliciously falsifying data.

Improper Access. This concern focuses on people, who access data but are not authorized to do so. Improper access relates to technological issues on the one hand and to organizational policies on the other hand. In general, people should only have access to personal data, if they "need to know" it.

Unauthorized Secondary Use. Here, people are concerned that personal data is used for a different purpose than they have authorized. This may happen internally by the organization that the data has been entrusted to or by involved external parties.

In a questionnaire study via interviews, Malhotra et al. (Malhotra et al., 2004) examined the relation of privacy concerns with trusting beliefs, risk beliefs and behavioral intention to disclose personal information. The context of the study was e-commerce, where marketers asked consumers for their willingness to use a free shopping membership in return for personal information like their shopping preferences or financial information. They found that the greater the information privacy concerns are expressed, the less trust people have in online companies (see Figure 1, H1) and the greater the perceived risk of data disclosure is (H2). Moreover, trusting beliefs have a positive impact on the behavioral intention to disclose information (H4), while risk beliefs affect it negatively (H5). Trusting beliefs and risk beliefs are also negatively related (H5).

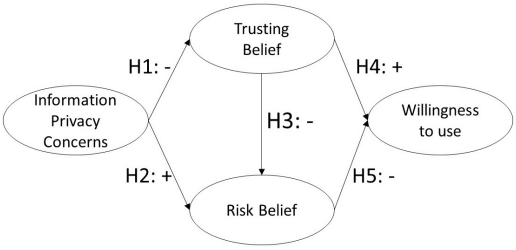

Figure 1: Overview of hypotheses H1 - H5 based on the work of Malhotra et al. (Malhotra et al., 2004).

3.1 Hypotheses on the Constructs' Relationships in HSM

Understanding the underlying mechanisms of the constructs privacy concerns with trusting beliefs, risk beliefs and the behavioral intention to make use of a technology is crucial for developing privacy-preserving applications. Hence, we reanalyze the work of Malhotra et al. (Malhotra et al., 2004) by transferring their hypotheses to the context of HSM. This results into the following hypotheses:

- H1: Privacy concerns are negatively related to trusting beliefs in an HSM application.
- H2: Privacy concerns are positively related to risk beliefs in an HSM application.
- H3: Trusting beliefs is negatively related to risk beliefs in an HSM application.
- H4: Trusting beliefs is positively related to the willingness to use the HSM application.
- H5: Risk beliefs is negatively related to the willingness to use the HSM application.

4 ELICITING TRUST-RELATED SOFTWARE FEATURES WITH TrustSoFt

In addition to analyzing the relationships between privacy concerns and the other aforementioned constructs, we also aim to mitigate the concerns by developing adequate software features. For that reason, we use the method of Eliciting Trust-Related Software Features (TrustSoFt). Originally, TrustSoFt is a step-wise, iterative method devised for the development of social media that is characterized by the introduction of strangers for offline encounters. As its focus lies on developing user-centred social media applications (Borchert et al., 2020b), it can also be applied for developing HSM applications which aim to mitigate users' privacy concerns. TrustSoFt is based on the theoretical background that users build trust in (1) the application, (2) the service provider, and (3) other social media users (Borchert et al., 2020a). Trust established when users evaluate whether these parties possess so-called trustworthiness facets (Borchert et al., 2020a). Trustworthiness facets describe traits by which the trustworthiness of these parties is assessed. These are for example ability, integrity, privacy, reputation or performance (Mayer et al., 1995), (Mohammadi et al., 2013), (Borchert et al., 2020a). Applications developed with TrustSoFt shall support users in their trustworthiness

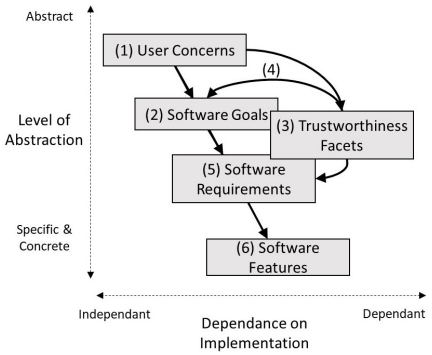

Figure 2: Overview of the TrustSoFt (Borchert et al., 2020b).

assessment. It is assumed that the better a trustworthiness assessment can be carried out, the likelier it is to reduce risks associated with application use.

TrustSoFt has six major steps as depicted in Figure 2: (1) The users' concerns are identified. (2) For each concern, software goals need to be determined. (3) Trustworthiness facets must be specified by considering what quality involved parties should possess so that a concern is reduced. (4) Trustworthiness facets are then related to a software goal. (5) Afterwards, the requirements engineer shall define software requirements. They specify what the system should do in order to achieve the software goals and to address at least one of the related facets. (6) Lastly, software features describe in what way a requirement can be implemented. Usually, features are specific front- or backend elements.

4.1 Hypotheses on the Privacy Concerns Addressed by Software Features

By applying TrustSoFt, software features are elicited that aim to mitigate user concerns. Therefore, we assume that specified features dedicated to users' privacy concerns reduce those when implemented in an HSM application like hushtweet. This leads to the following hypotheses:

- H6: An HSM application that has software features implemented, which aim to reduce a particular privacy concern, has a positive impact on the user perception that this concern is countered.
- H7a & H7b: An HSM application that includes software features aiming to counter all privacy concerns is a) trusted the most b) perceived the least risky compared to HSM applications addressing less concerns by software features.

As we analyze the impact of an HSM application that aims to counter privacy concerns by software features here, an adoption of hypotheses H1 and H2 is necessary for this context.

- H1.1: Counteracted privacy concerns are positively related to the trusting beliefs in an HSM application.
- H2.1: Counteracted privacy concerns are negatively related to risk beliefs in an HSM application.

4.2 Applying the TrustSoFt Method

We apply the TrustSoFt method in order to elicit frontend software features to counter privacy concerns in the HSM application hushtweet. Our exact procedure is explained step by step below and is illustrated using the example concern "Errors".

User Concerns. Considering former research (Smith et al., 1996), (Malhotra et al., 2004), this work focuses on privacy concerns (see Section 3). We elicit features for each concern separately. As a first step, we revisit the definition of each concern and make ourselves aware of their identifiable characteristics and descriptive keywords. For the "Errors" concern, the keywords are *errors in personal data*, *deliberate and accidental errors* and *minimizing problems*.

Software Goals. Based on the concern definition, we derive a set of software goals that mitigate this concern, thus improving the overall satisfaction of the end users. For instance, to address the "Errors" concern, we need to insure that the data stored by hushtweet is accurate and error-free. Therefore, we identify *data accuracy* as a goal.

Trustworthiness Facets. In order to support users in their trustworthiness assessment, we specify a number of trustworthiness facets, which are then allocated to goals. For that reason, we distinguish who exactly is involved in the concern and consult literature as to which traits are desired these stakeholders to avoid or reduce the concern. For the "Errors" concern, we identify four facets for the hushtweet application as important: *data integrity*, *data reliability*, *data validity* and *failure tolerance* (Mohammadi et al., 2013). We assign the facets to the goal data accuracy.

Trustworthiness Requirements. Next, we define software requirements by describing what the system should do to achieve the software goals and meet the selected facets. Oftentimes, one requirement might address multiple facets simultaneously. For example, we define the requirement: *Verifying the correctness of the data*, to meet the facets data integrity, data reliability, and data validity.

Software Features. Lastly, we specify how to realize the requirements through a set of software features. For the evaluation in the later user study, we focus on features for the user interface of hushtweet rather the

backend system. We elicit two features to realize the aforementioned requirement: (1) An alert message on tweeting privately says: "Data is correctly and safely stored". (2) Two questions in the FAQ section: "How does hushtweet ensure the correctness and integrity of my data?" and "Does hushtweet modify my data?".

Applying TrustSoFt for hushtweet resulted in a long list of software features. Table 2, in Appendix, shows an extract of the identified features, which are later implemented in the HSM application hushtweet for the user study.

5 METHODOLOGY

In order to test the hypotheses, we conducted an extensive online survey via Amazon Mechanical Turk[1]. The structure of the study is explained below.

5.1 Experimental Design

The online survey follows a between-group design with nine experimental groups. The names of the groups are depicted in Table 1 on page 6. By means of a short description, hushtweet was introduced to all groups as well as its functioning based on the HSM concept. Afterwards, each group, except the HSM Concept group, interacted with a mockup version of hushtweet for at least five minutes. While the Basic App group received a mockup with only the basic functionalities of hushtweet (see Section 2), each of the other groups got a distinct version extended by software features elicited with TrustSoFt to address one privacy concern. The names of the experimental groups correspond to the concern the mockup addresses. The Full-featured group received a mockup including all the elicited features, i.e., addressing all the concerns.

5.2 Hushtweet Mockup

We developed eight mockup versions of hushtweet with the online design tool Figma[2]. From the eight versions, six were extended by three distinct features to address one privacy concern (see Table 2), one version received all selected features from the other versions and another version included none of the features. We carefully selected the implemented features to cover all trustworthiness facets identified during TrustSoFt. Due to comparability reasons, a software feature for each concern is a *FAQ* section answering questions that treat the nature of the respective concern. Figure 3 illustrates the mockup version for the Full-featured group as an example.

5.3 Scales

For questionnaire selection, we mainly adopted the scales used by Malhotra et al. (Malhotra et al., 2004), namely: General Information Privacy Concern (GIPC) (Smith et al., 1996), Internet Users' Information Privacy Concern (IUIPC), Concern for Information Privacy (CFIP) (Smith et al., 1996), trusting and risk beliefs (Jarvenpaa et al., 1999). Additionally, we added the scale for *perceived trustworthiness of online shops* (Büttner and Göritz, 2008) in order to measure how the trustworthiness of hushtweet is perceived. The scale includes subscales measuring *ability, benevolence, integrity*, and *predictability*. These have been partially considered as trustworthiness facets in the application of TrustSoFt. Finally, we asked participants about their willingness to use hushtweet by eight self-developed questions. For each questionnaire, we used a 7-point Likert scale (1="strongly disagree" to 7="strongly agree").

All experimental groups received the same questionnaires. The only exception is the IUIPC scale; while the HSM Concept group received the IUIPC in order to state their privacy concerns regarding hushtweet, all other experimental groups received a modified IUIPC, in which they should evaluate to what extent the hushtweet mockup they were confronted with has addressed the privacy concerns.

The questionnaires were adapted in the wording to the hushtweet context. As an example, we replaced words like "online companies" and "computer databases" with "hushtweet" and "distributed databases". In order to measure the addressed privacy concerns, the IUIPC and CFIP do not include the expectational modal verb "should", but are phrased as hard statements.

5.4 Procedure

The procedure is nearly the same for all experimental groups. After briefing partidicants about the context of the study, they received the GIPC scale to answer questions about their general privacy concerns. Then, they were introduced to the concept and basic functionalities of hushtweet by a short descriptive text. Afterwards, we checked their comprehension of hushtweet with six questions. The purpose of this check is to include only the participants, who understood the concept of hushtweet for the follow-up analysis. As a next step, every experimental group–except the HSM Con-

[1]https://www.mturk.com
[2]https://www.figma.com

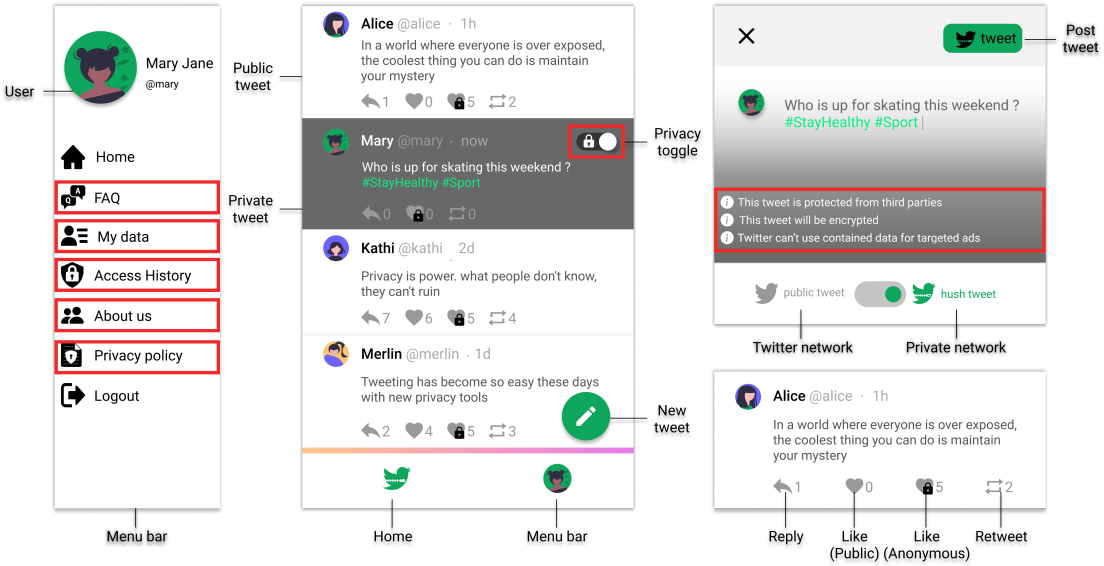

Figure 3: Overview of the hushtweet mockup for the Full-featured group. The red frames highlight included software features.

cept group– received a modified task to use hushtweet depending on the respective hushtweet mockup version. The task includes hints regarding the privacy concern features. Each participant had a minimum of five minutes to interact with the mockup. Afterwards, all groups received the remaining scales in following order: perceived trustworthiness scale, the IUIPC and CFIP, trusting beliefs scale, scale for risk beliefs and the questions regarding the willingness to use. Finally, the participants were also asked about their gender, age, and education level.

6 RESULTS

In this section, we report details on the population of the participants, as well as our findings concerning the descriptive analysis and our hypotheses H1-H7b.

6.1 Population

We conducted the study with 300 participants for the HSM Concept group and 250 participants for each of the other experimental groups via Amazon Mechanical Turk. As a qualification requirement for participation, subjects were allowed to take part in only one of the experimental groups and have an experience of more than 1000 accepted surveys on Amazon Mechanical Turk. Thereby, we try to obtain high quality data, which is filled in properly and without haste. For further analysis, we only considered complete data sets and those whose participants had three or less mistakes in the hushtweet comprehension test. Based on that, between 7% and 19% of the population of each experimental group had to be deleted. Table 1 shows the final population of each experimental group along with information on their gender, age, and education level. With an average rate of 62,3% male and 32,8% female participants, the experimental populations resemble the gender imbalance of Twitter users worldwide in January 2021 with 68,5% men and 31,5% women (Noyes, 2021).

Table 1: Overview of the experimental groups and characteristics of the surveyed populations.

Group	Population (n)	Men (%)	Women (%)	Age (M)	Bachelor's degree or higher (%)
Basic (control)	205	68.3	31.2	33.6	84.5
Awareness	222	63.1	36.0	33.5	67.1
Collection	223	63.2	36.3	35.6	66.9
Control	223	58.3	39.5	37.6	70.8
Errors	211	58.7	39.8	32.6	87.7
Improper Access	202	58.4	41.6	35.9	72.8
Unauthorized S. Use	216	64.8	35.2	33.8	83.8
Full-featured	233	63.9	35.2	35.6	68.3

6.2 Descriptive Analysis of the Studied Constructs

To investigate users' privacy concerns regarding HSM, we conducted a descriptive analysis for the "HSM Concept" group. The GIPC has a mean of M=4.89, SD=.93. In comparison, the mean of the IUIPC is M=5.73, SD=.74. Both types of concerns are strongly related ($r=.561$, $p<.001$).

Having a look at the individual privacy concerns, the participants rated that hushtweet should consider the concerns in the following order (from high to low):

(1) Unauthorized secondary use (M=6.26, SD=.93), (2) awareness for privacy practices (M=6.16, SD=.84), (3) improper access (M=5.89, SD=1.03), (4) control (M=5.87, SD=.86), (5) errors (M=5.14, SD=1.30), and (6) collection (M=5.04, SD=1.17).
Concerning the other constructs, trusting beliefs have a mean of M=5.14, SD=1.08. Hushtweet's overall trustworthiness is rated with M=5.24, SD=.97. Concerning the trustworthiness facets, integrity is rated the highest (M=5.42, SD=1.12), followed by benevolence (M=5.40, SD=1.11), ability (M=5.33, SD=1.02), and predictability (M=5.07, SD=1.07). Lastly, risk beliefs are rated with M=3.58, SD=.94.

In general, it can be said that the participants show moderated general privacy concerns with high variance. Still, they agree that hushtweet should address privacy concerns. The participants lightly trust hushtweet and slightly disagree that it is risky. It is worth mentioning that the relatively high values of the standard derivations of all the constructs show the diversity of the participants' opinions. This indicates a realistic representation of the user population.

6.3 Hypotheses H1-H5

In order to test hypotheses H1-H5 (including H1.1 and H2.1), we calculated a Structural Equation Model (SEM) model for each experimental group. For each SEM, we neither considered items that did not contribute to an acceptable internal scale consistency of at least α =.70, nor constructs with factor loadings less than .700. Omitted items do not measure the scale construct in a valid way, while omitted constructs do not contribute much to people's total privacy concerns. Based on that, the privacy concern "Collection" had to be excluded from every SEM. The privacy concern "Errors" was only relevant for the experimental groups "Control", "Errors" and "Improper Access". Moreover, we checked the model fit of the SEMs by calculating a confirmatory factor analysis (Hu and Bentler, 1999). All are at least acceptable with a comparative fit index (CFI) and Tucker-Lewis index (TLI) higher than .90, a root-mean-square error of approximation (RMSE) lower than .80 and a normed chi-square (X^2/df) lower than 5.

As an example, we present the SEM of the HSM Concept group in Figure 4. Its model fit is good (X^2/df=1.943, TLI=.949, CFI=.956, RMSEA=.062). Concerning the hypotheses, hypothesis H1 cannot be confirmed. The relation between privacy concerns and trusting beliefs is not significant. However, privacy concerns have a small positive effect on risk beliefs (H2). Hypothesis H3 is also supported as trusting beliefs highly negatively influence risk beliefs. Last but not least, the willingness to use hushtweet is positively impacted by trusting beliefs with a medium effect (H4), while it is negatively influenced by risk beliefs with a small effect (H5).

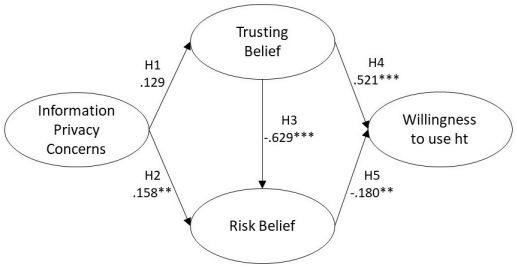

Figure 4: SEM for hypotheses testing for the HSM Concept group.
* p<.01, *** p<.001

For the experimental groups that were confronted with the hushtweet mockups, the addressed privacy concerns positively affect trusting beliefs (H1.1), and trusting beliefs impact the willingness to use hushtweet (H4)–both in a strong way. Therefore, hypotheses H1.1 and H4 are confirmed. In case of hypothesis H2.1, the relation between addressed privacy concerns and risk beliefs was not statistically significant for any experimental group. Thus, hypotheses H2.1 cannot be confirmed. Hypothesis H3 is only significant in the Full-featured group but in none of the other experimental groups. Therefore, a negative impact from trusting beliefs on risk beliefs can only be partly supported. Concerning H5, in some of the experimental groups, risk beliefs do not significantly influence the willingness to use hushtweet. However, in the groups where the influence is statistically significant, it is always positive with a weak effect. This is the case for the groups Basic App (r=.208, p=.001), "Control" (r=.178, p=.007) and "Unauthorized Secondary Use" (r=.110, p=.044). Therefore, hypothesis H5 can partly be falsified.

6.4 Hypotheses H6, H7a & H7b

To test hypotheses H6, H7a and H7b, all experimental groups that interacted with a hushtweet mockup are analyzed. Therefore, the "HSM Concept" group is out of scope. We based our hypotheses testing on two-factor ANOVAs (Anderson and Gerbing, 1988) in order to examine differences in perceived countered privacy concerns between the experimental groups. We expect that an addressed concern is rated highest by the experimental group that was exposed to the corresponding hushtweet mockup. Only privacy concerns whose internal consistency has a Cronbach's alpha higher than α >.70 are considered. Based on that, the privacy concern "Collection" is not further analyzed for any

experimental group. The privacy concern "Control" has an unsatisfying internal consistency in the experimental groups "Collection", "Control", and "Improper Access".

Hypothesis H6 can only be supported for the privacy concern "Errors". The "Errors" group rated the errors concern to be addressed the most ($F(7,1727)=4.249$, $p=.000$, partial $\eta^2=.017$). However, only 1.3% of the variation of the addressed errors concern around the total mean value can be explained by the implemented errors software features (adjusted R-square). The effect size of the model is f=.13 and can be interpreted as weak. Post-hoc tests with the Bonferroni correction show significant differences ($p< .05$) between the "Errors" group (M=5.34, SD=.98) with the groups "Awareness" (M=4.95, SD=1.11), "Collection" (M=4.97, SD=1.05), "Control" (M=4.82, SD=1.06), and "Unauthorized Secondary Use" (M=4.95, SD=1.21).

Furthermore, ANOVA has shown that the privacy concern "Control" is also evaluated significantly different by the experimental groups ($F(7,1727)=2.063$, $p=.044$, partial $\eta^2=.008$). However, contrary to what is assumed in H6, it is not the "Control" group that evaluates hushtweet the highest in providing users control (second place with M=5.83, SD=1.01), but the "Awareness" group (M=5.86, SD=.91).

For hypotheses H7a and H7b, we also calculated two-factor ANOVAs for the Full-featured group. For reasons of interest, we also calculated it for the other experimental groups. Concerning hypotheses H7a, the ANOVAs for trusting beliefs and the trustworthiness of hushtweet are not statistically significant for any of the experimental groups. Thus, hypotheses H7a cannot be confirmed. The only significant ANOVA model in the context of trust is for the trustworthiness facet *integrity* ($F(7,1727)=2.017$, $p=.05$, partial $\eta^2=.008$). There, the "Awareness" group has rated integrity the highest (M=5.89, SD=.93), while the "Errors" group rated it the lowest (M=5.60, SD=.97).

The same can be observed for hypothesis H7b concerning risk beliefs ($F(7,1727)=10.364$, $p=.000$, partial $\eta^2=.040$). The "Awareness" group believes hushtweet to be the least risky compared to the other groups (M=3.32, SD=.11), while the "Errors" group evaluates it the most risky (M=4.35, SD=.11). It should be mentioned that the Basic App group has the second highest value in their risk beliefs (M=4.11, SD=.11). Nonetheless, hypotheses H7b is rejected.

7 DISCUSSION

This work tackles two major research objectives. First, we examined the relationships between privacy concerns, trusting beliefs, risk beliefs, and the willingness to use in the HSM context. Second, we applied TrustSoFt to elicit trust-related software features to address users' privacy concerns in an HSM application. In this section, we discuss the results of our user study on (1) the relevance of the privacy concerns, (2) the relations between the constructs, and (3) the impact of the developed features on privacy concerns. Next, we discuss some remarks on the application of TrustSoFt. Lastly, we conclude the section by describing the limitations of this work and articulating suggestions for future work.

7.1 Relevance of Privacy Concerns

Our survey suggests that "Unauthorized Secondary Use" is the most important concern, followed by "Awareness of Privacy Practices" and "Improper Access", while "Errors" and "Collection" were the least relevant. These findings are aligned with the work of Smith et al. (Smith et al., 1996), where they found that "Unauthorized Secondary Use" and "Improper Access" affect privacy concerns more than "Errors" and "Collection". The prominence of "Awareness of Privacy Practices" in HSM supports the suggestion that the context slightly impacts the relevance of privacy concerns (Ebert et al., 2020).

In addition, our SEM analysis supports the low expression of the two concerns "Collection" and "Errors", as their factor loadings weakly contribute to the representation of privacy concerns For the "Collection" concern, we assume, based on unacceptable internal consistency, that the scale used is not sufficient to validly measure the construct. In case of the "Errors" concern, the HSM context can be a reason why it is weakly manifested. HSM leverages encrypted and distributed data storage, which contributes to lower risk of malicious attacks on personal data. Therefore, people might be less concerned about errors in their data.

7.2 Relationships of the Constructs

The relationships of privacy concerns with trusting beliefs, risk beliefs, and the willingness to use an HSM application were partly unexpected. It cannot be confirmed that privacy concerns regarding hushtweet affect trusting beliefs negatively. It seems as if privacy concerns are detached from trust in hushtweet. This finding conforms with a study on a sample of Facebook

users (Kusyanti et al., 2017), where it is discussed that the trust in Facebook and in its privacy policy exceeds the privacy concerns. For our context, we argue that although the participants expressed inherited concerns about hushtweet, as yet another social media application, its purpose leads to trust given in principle and thus is detached from the concerns. This argumentation is additionally supported by our results, which show that addressing privacy concerns by software features does have an impact on the trust in hushtweet.

For risk beliefs, on the one hand, our findings suggest that privacy concerns slightly increase risk beliefs in hushtweet. This conforms with the conclusions of Malhotra et al. (Malhotra et al., 2004). On the other hand, we found that addressing privacy concerns does not necessarily reduce the risk beliefs. A possible explanation for this might be that users are still aware of the existing risks accompanying information processing during social media use as the implemented software features refer to their existence. Risk awareness is identified as a relevant factor in research about privacy concerns (Olivero and Lunt, 2004).

Interestingly, we observe that sometimes participants are a bit more willing to use hushtweet the higher their risk beliefs are. Curiosity can be one reason for this phenomena, because it induces people to tolerate more risk, which in turn promotes the willingness to use (Dowling, 1986). However, a positive relation of risk beliefs to the willingness to use hushtweet is not always confirmed.

Another salient finding is that trusting beliefs reduce risk beliefs in two cases; first, when the participants are only introduced theoretically to the concept of HSM. Second, when they interact with the application where all privacy concerns are addressed. We conclude that the principle of HSM is essential to establish the relationship between trusting and risk beliefs. For this, an application should convey the HSM concept in an encompassing way so that the benefits are emphasised and a multitude of concerns are addressed.

7.3 Impact of Software Features on Privacy Concerns

Looking at the impact of the software features on the users' opinions regarding the extent to which privacy concerns are addressed, the results differ from our expectations. Only features that address concerns about errors in data processing were rated as most strongly addressing those concerns. Features that address a different concern greatly affect other concerns for which they were not intended. We assume that this relates to the way a particular feature addresses a concern. One of the used "Errors" features directly confronts users with the targeted concern as we included an error in the application to present how the application deals with it. In contrast, other features indirectly present concerns by displaying the way they are handled with. Therefore, we assume that concerns need to be emphasized stronger in order to make it more apparent to users that they are being taken into account. In general, we rate features addressing errors as special, because they are associated with undesired software behaviour. Therefore, it is not surprising that such features were perceived the lowest concerning the trustworthiness facet "Integrity" compared to other features.

In contrast, the "Awareness for Privacy Practices" features are rated the highest concerning integrity and the lowest regarding risk beliefs. Surprisingly, these features are also found to be remarkably mitigating the "Control" concern. Thus, we conclude that raising the users' awareness positively contributes to an enhanced feeling of control, stronger trusting beliefs, and weaker risk beliefs. This conforms with the research of Kani et al. (Kani-Zabihi and Helmhout, 2011), who pointed out that software features creating privacy awareness also support users in managing their privacy concerns.

7.4 Lessons Learned on TrustSoFt

We applied TrustSoFt to mitigate the privacy concerns – identified in the literature – by specifying adequate software features. With that, we implicitly assume that all the concerns are equally relevant to users. However, our results show otherwise. As argued in Section 7.3, addressing the "Awareness for Privacy Practices" has a larger impact than addressing other concerns - not only in its impact strength but also in its range. For the TrustSoFt application, this means that concerns need to be chosen carefully in order to achieve the best possible effect for the software to be developed. In the light of this observation, we highly recommend the requirements engineers, who apply TrustSoFt, to use qualitative approach in order to gain deep insights in the users' concerns as well as to consider the significance and potential trans-concern impacts of elicited software features.

In general, applying TrustSoFt yields in a large number of software features that also consider users' trustworthiness assessment of the application. In case of the "Awareness" features, we targeted to present the integrity of the application. This was effectively perceived by users and resulted in increased trustworthiness of the application.

7.5 Limitations and Future Research

HSM is a relatively complex technology that is not widely known and not easy to understand for non-experts (Wainakh et al., 2019). Therefore, we have decided to introduce study participants to the hushtweet app that represents the HSM technology. This facilitated conducting the survey and elaborating the specified software features by TrustSoFt. However, it also limits our work to the scope of hushtweet, because the participants only indirectly responded to the HSM technology. Their answers could be biased based on the design and usability of hushtweet. Nonetheless, we are optimistic that people really reacted to the HSM technology as we have only considered those participants, who have understood the concept.

Regarding the design and usability of hushtweet, particpants gave us positive feedback that also implied fun during usage and liking the application. Former research found that an appealing interface positively affects the users' perception and performance regarding software use (Sonderegger and Sauer, 2010). Therefore, the effect of such intervening variables on the impact software features have on privacy concerns, trusting beliefs, and risk beliefs regarding an HSM application needs to be addressed in future work.

Another potential limitation is our choice of privacy concerns and software features that we have examined. We have chosen the particular privacy concerns, because they were identified as relevant when it comes to information processing. As this is one major factor of HSM, the privacy concerns constitute a good starting point for analysis in this context. However, the participants in this work have also stated additional concerns, for example, economical aspects of the service provider that might impact information processing. For future work, it is indispensable to elicit further user concerns, which are then also considered during the development of HSM applications. Moreover, the evaluated software features originate from a long list of features, which resulted from the TrustSoFt application. We carefully selected three features for each concern that are similar to some extent. By implementing multiple and similar features, we wanted to make sure that each concern is clearly addressed and that resulting study values are comparable. Nonetheless, the features might still differ in their impacts on people or contribute differently to the various concerns. Here, it is interesting to examine each feature and its impact individually rather than a part of a holistic application. In addition, it is also interesting to consider the features' impact on different user types. While the population tested in this work resembles the one of Twitter and is framed by the users of Amazon Mechanical Turk, focusing on cultural, social, gender or individual user differences might provide further insights.

8 CONCLUSION

Due to frequent data breaches and misuse cases in the area of social media, the people's concerns about their data storage and processing have increased. Hybrid social media applications provide an alternative solution that allows users to enjoy the benefits of social media in a more safe and controlled environment. Therefore, it is especially important to also address information privacy concerns during the development of such applications by specifying software features for the user interface. In doing so, a social media experience can be ensured that is satisfactory on the backend and frontend level.

This work has shown that addressing information privacy concerns in hybrid social media applications increases their trustworthiness. The more people trust the application, the higher is their willingness to use it. It is especially effective to address users' awareness of privacy practices as it not only can affect the perceived integrity of the service provider but also provides users with a feeling of control. Moreover, it became apparent that the choice of concern to be dealt with in the application development should be wisely made. Some concerns, such as the awareness of privacy practices, seem to be more important than others.

ACKNOWLEDGEMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - 251805230/GRK 2050 and GRK 2167.

REFERENCES

Anderson, J. C. and Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin*, 103(3):411.

Borchert, A., Díaz Ferreyra, N. E., and Heisel, M. (2020a). Building trustworthiness in computer-mediated introduction: A facet-oriented framework. In *Int. Conf. on Social Media and Society*, pages 39–46.

Borchert, A., Ferreyra, N. E. D., and Heisel, M. (2020b). A conceptual method for eliciting trust-related software features for computer-mediated introduction. In *ENASE*, pages 269–280.

Büttner, O. B. and Göritz, A. S. (2008). Perceived trustworthiness of online shops. *Journal of Consumer Behaviour: An Int. Research Review*, 7(1):35–50.

Daubert, J., Bock, L., Kikirasy, P., Mühlhäuser, M., and Fischer, M. (2014). Twitterize: Anonymous microblogging. In *2014 IEEE/ACS 11th Int. Conf. on Computer Systems and Applications (AICCSA)*, pages 817–823. IEEE.

Dowling, G. R. (1986). Perceived risk: the concept and its measurement. *Psychology & Marketing*, 3(3):193–210.

Ebert, N., Ackermann, K. A., and Heinrich, P. (2020). Does context in privacy communication really matter?—a survey on consumer concerns and preferences. In *Proc. of the 2020 CHI Conf. on Human Factors in Computing Systems*, pages 1–11.

Graffi, K., Podrajanski, S., Mukherjee, P., Kovacevic, A., and Steinmetz, R. (2008). A distributed platform for multimedia communities.

Guardian, T. (2018a). Facebook to contact 87 million users affected by data breach. https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach. Online; accessed 07.12.2020.

Guardian, T. (2018b). Huge Facebook breach leaves thousands of other apps vulnerable. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens. Online; accessed 18.11.2020.

Hu, L.-t. and Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1):1–55.

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2):JCMC526.

Kani-Zabihi, E. and Helmhout, M. (2011). Increasing service users' privacy awareness by introducing on-line interactive privacy features. In *Nordic Conf. on Secure IT Systems*, pages 131–148. Springer.

Kozlowska, I. (2018). Facebook and data privacy in the age of cambridge analytica. *Seattle, WA: The University of Washington. Retrieved August*, 1:2019.

Kusyanti, A., Puspitasari, D. R., Catherina, H. P. A., and Sari, Y. A. L. (2017). Information privacy concerns on teens as facebook users in indonesia. *Procedia Computer Science*, 124:632–638.

Larson, S. (2017). Every single Yahoo account was hacked - 3 billion in all. http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html. Online; accessed 07.12.2020.

Larson, S. (2018). Fitness app that revealed military bases highlights bigger privacy issues. http://money.cnn.com/2018/01/29/technology/strava-privacy-data-exposed/index.html. Online; accessed 09.05.2019.

Luo, W., Xie, Q., and Hengartner, U. (2011). FaceCloak Download. https://crysp.uwaterloo.ca/software/facecloak/download.html. Online, accessed 07.12.2020.

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS quarterly*, pages 5–12.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, 20(3):709–734.

McCandless, D. (2019). World's Biggest Data Breaches & Hacks. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks. Online; accessed 07.12.2020.

Mohammadi, N. G., Paulus, S., Bishr, M., Metzger, A., Koennecke, H., Hartenstein, S., and Pohl, K. (2013). An analysis of software quality attributes and their contribution to trustworthiness. In *CLOSER*, pages 542–552.

Noyes, D. (2021). Distribution of Twitter users worldwide as of January 2021, by gender. https://www.statista.com/statistics/828092/distribution-of-users-on-twitter-worldwide-gender/. Online; accessed 10.02.2021.

Olivero, N. and Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of economic psychology*, 25(2):243–262.

Salzberg, M. (2010). Diaspora - Kickstarter Pitch. https://web.archive.org/web/20110814222702/http://blog.joindiaspora.com/2010/04/27/kickstarter-pitch.html. Online, accessed 07.12.2020.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, pages 167–196.

Sonderegger, A. and Sauer, J. (2010). The influence of design aesthetics in usability testing: Effects on user performance and perceived usability. *Applied ergonomics*, 41(3):403–410.

Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, 68(3):459.

Tufekci, Z. and King, B. (2014). We Can't Trust Uber. https://www.nytimes.com/2014/12/08/opinion/we-cant-trust-uber.html.

Wainakh, A., Grube, T., Daubert, J., Porth, C., and Mühlhäuser, M. (2019). Tweet beyond the cage: A hybrid solution for the privacy dilemma in online social networks. In *2019 IEEE Global Communications Conf. (GLOBECOM)*, pages 1–6. IEEE.

APPENDIX

Table 2: Overview of the software features per privacy concern that resulted from the TrustSoFt method.

Concern	Goal	Facet	Requirement	Features
Awareness (of Privacy Practices)	Clarity of privacy practices	Transparency	Providing an overview of the privacy practices	FAQ: "*How does hushtweet protect my privacy?*"
	Clarity of privacy practices	Transparency	Informing users on the privacy practice for private tweets	Alert messages on tweeting (1) privately: "*This tweet will be encrypted*", and (2) publicly: *"Twitter has access to this data"*
	Clarity of privacy practices	Transparency, Provider integrity	Informing users on the legally binding commitments of hushtweet regarding privacy	"Privacy Policy" page that informs users on data collection and its purpose.
Collection	Fairness	Completeness, Transparency, Provider integrity	Showing users the statistical information that they are part of. Clarifying their gain from the collection of this information.	"My data" page that contains: (1) description of the statistical information and its purpose, and (2) a list of the statistical information that the user is part of.
	Awareness	Transparency, Provider integrity, Provider predictability	Informing users on their data usage by Twitter and hushtweet, and the services they receive in return	FAQ: "*How does hushtweet and Twitter use my data?*" FAQ: "*What is my benefit from hushtweet services in comparison to Twitter services?*"
	Awareness	Transparency, Provider integrity	Informing users on their data usage by Twitter and hushtweet	Alert messages on tweeting (1) privately: "*Twitter can't use contained data for targeted ads*", and (2) publicly: *"Twitter might use contained data for targeted ads"*
Control	Data control	Privacy (control)	Allowing users to decide how their data is shared	A toggle button to change the user's posted tweet status between private and public at any time
	Data control	Privacy (control)	Allowing users to delete all their data	FAQ: "*How can I delete my data?*" "My data" page that contains a button for deleting all user data (private tweets and anonymous likes)
	Procedure control	Privacy (control)	Allowing users to decide what data is used for statistical information	"My data" page that contains: (1) a list of the statistical information that the user is part of, and (2) a toggle button for each item of this information with which the user can opt-in/-out of collection.
Errors	Data accuracy	Data integrity, Data reliability, Datav validity	Verifying the correctness of the data	An alert message on tweeting privately: "*Data is correctly and safely stored*"
	Data accuracy	Data integrity, Data reliability, Data validity	Verifying the correctness of the data	FAQ: "*How does hushtweet ensure the correctness and integrity of my data?*" FAQ: *"Does hushtweet modify my data?"*
	Data accuracy	Failure tolerance	Maintaining the data accuracy on network disconnection	On tweeting while the network is disconnected, the tweet is stored locally and can be posted when the network is connected again. Informing the user with an alert message: *"Don't worry, your tweet is saved locally. Just retry when your network connection is back"*
Improper Access	Technical access control	Confidentiality	Protecting user data from unauthorized users or parties	Alert messages on tweeting (1) privately: "*This tweet is secured against unauthorized parties*", and (2) publicly: *"This tweet will be processed by Twitter & partners"*
	Technical access control	Traceability, Transparency	Showing users who had access to their data	"Access History" page that displays time of (1) user login, (2) data access for calculating statistical information by hushtweet, and (3) profile view by other users
	Organizational access control	Provider integrity	Clarifying the hushtweet policy in regard to the restricted access of developers to user data	FAQ: "*How does hushtweet protect my data from improper access?*"
Unauthorized Secondary Use	Authorization	Transparency	Informing users on their data usage by hushtweet. Requesting authorization for data access and usage.	"Authorization" page that contains: (1) description of data access and usage by hushtweet, and (2) authorization button with which users authorize hushtweet to access their data on Twitter and calculate statistical information
	Callrity of intent	Provider integrity, Provider benevolence	Informing users on the intent of hushtweet as a research project	"About us" page that informs users on the purpose of the research project of hushtweet, which is protecting users' privacy, and also listing the involved universities and researchers
	Clarity of data use purpose	Transparency, Provider integrity	Informing users on how hustweet uses the statistical information and which parties have access to it	FAQ: "*For what purpose is my data used?*" FAQ: "*Is my data shared with third parties?*"