Dynamic Privacy Hierarchical Design to Optimize the User Experience of Financial Management

Xiaoyun Jing, Junyao Fan, and Yunfei Liu

Hunan University, China

ABSTRACT

As the social attributes of fund financial products for young people have increased, users have begun to share financial management information in social circles, which has become a new way of privacy disclosure. Generally, users have a lower willingness to disclose financial information, but the social emotion gains become the benefit points of privacy fluctuations in this scenario. We looked forward to improving the user experience of financial income information-sharing services from the perspective of privacy protection. Dynamic privacy classification control could help users reduce the hidden dangers of privacy disclosure, which helped to overcome the above problem. We conducted semi-structured interviews and behavioral observations with young users (18-35 years old) who purchased financial products online to explore users' attitudes towards sharing financial information. We asked participants to rank the privacy sensitivity of their information shared online to establish a privacy classification standard for financial information sharing. According to the research, user roles, users' financial management capabilities, and the sharing scenarios of financial information would all affect users' privacy sensitivity. Therefore, we established a dynamic model. Finally, we showed the participants a design prototype of dynamic privacy classification control. Almost every participant found it perceivable and useful, improving their user experience of using financial income information-sharing services. Privacy classification protection research usually discussed user privacy rights and social ethics but thought less of the user's own experience. The study introduced dynamic privacy classification control to provide a reference for the optimization of user experience design.

Keywords: Privacy classification, Dynamically controls, User experience

INTRODUCTION

With the popularization of mobile internet, most users tend to use mobile financial apps to manage their finances. The younger generation is more likely to use mobile funds for financial management and to gain social approval, they are used to sharing daily life. In general, users have little incentive to disclose financial information, however, the social-emotional gain becomes the benefit point of privacy fluctuation in this scenario (Hu P.P., 2019). Face-to-face social communication has shifted to media-based network communication, where people need to take the initiative to disclose their information to enhance familiarity and maintain intimate relationships (Yiannis K., 2016).

For example, people obtain social-emotional value through sharing financial information, such as taking screenshots in financial apps and sending them to friends or sharing them on social platforms.

In the process of sharing financial information, Inevitably, there is a risk of privacy disclosure. For example, there may be a demonstration of the family's economic situation, exposure of personal financial situation in the screenshot, etc. The risks are obvious. A wealth of data shows that self-presented information and privacy in cyberspace can become a tool for criminals to profit, which directly affects users' experience of using mobile financial products. At the same time, it becomes the focus of the user's attention (Sun C.Q., 2021). So far, mobile finance platforms have not been optimized for complex social scenarios, and users' financial information is still exposed in an insecure social space.

In the view of the phenomenon that people are increasingly concerned about financial information privacy and the lack of corresponding privacy protection behaviors, One possible solution is to create a privacy hierarchy that dynamically changes according to the scenario. Privacy classification is ranked by the degree of privacy, covering all important aspects of privacy. Therefore, unnecessary disclosure of privacy can be reduced (Santi P., 2018, Ann C. and Michelle C., 2009,). To give full play to the role of privacy classification, It is necessary to study and formulate the ranking of financial privacy degree of financial privacy information in the social sharing scenario, understand the role of privacy classification in reducing users' perception of privacy risks, and enhance the user experience by improving privacy protection in the field of mobile finance.

Up to now, we've found that privacy classification is still in the preliminary research stage and implemented in user experience design. The existing privacy classification mostly focuses on users' social and personally identifiable information, and rarely considers financial information. However, the privacy of financial information is gradually becoming the focus of users' attention, which also affects users' social sharing and user experience of financial information.

THE RESEARCH METHODS

To study the privacy classification design in the mobile financial sharing scenario, three sets of methods are adopted: participatory observation and group interview, ranking scale, path analysis, and prototype test. In participatory observation, four observers completed eight sharing tasks, at the same time, we invited 5 young users (18-35 years old) with online financial management experience to conduct a focus group discussion to determine the problems of privacy disclosure in financial sharing scenarios. For semi-structured interviews, we designed the interview guide, and the interviewees were required to have the behavior of buying financial products online and the experience of sharing financial products online. Finally, young users (18-35 years old) (n = 12) were recruited to participate voluntarily, in the interview, they completed the ranking of private information in the financial sharing scenario (Pardis E.N. et al., 2019, Judith S.O., et al., 2005). In addition, we studied
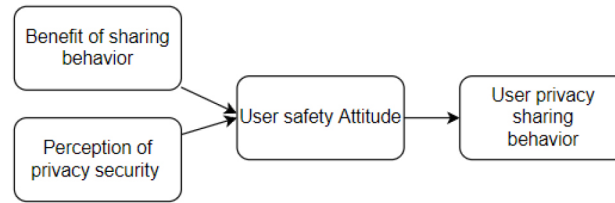
Figure 1: Path of privacy disclosure in financial social networking scenarios.

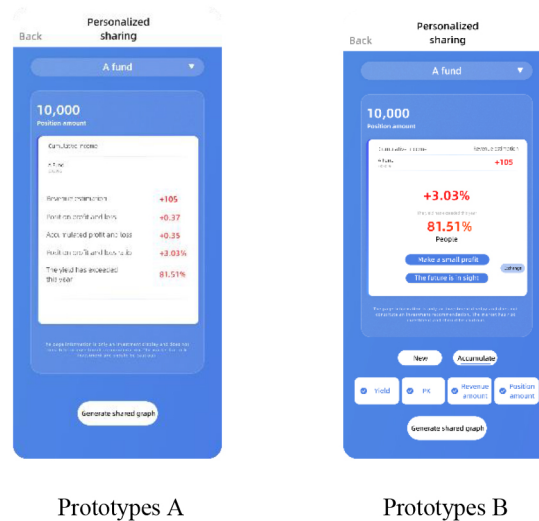Prototypes A   Prototypes B

Figure 2: The Interaction prototypes.

the usability and ergonomics issues in the privacy grading design evaluation, based on which we constructed a theoretical path of privacy disclosure in the financial sharing scenario, and verified the path with a scale. At the same time, we proposed two dimensions to test the effectiveness of the privacy grading design. Then we created a prototype APP interface. Each participant uses the prototype to perform a different sharing task on a pre-set scenario. Another 12 participants (18-35 years old) participated in our prototype testing experiment.

In the participatory observation and focus group discussion of financial management sharing scenarios, we found significant differences between the social scene of acquaintances and the social scene of strangers. This is consistent with research suggesting that social environments create differences in privacy sharing (Santi P., 2018). We mainly studied these two scenes in the semi-structured interview. The psychological causes of privacy disclosure are complicated. Therefore, it is necessary to explore human factors for the effectiveness of the design.

A recent study established the influencing factors model of privacy paradox behavior (Sun C.Q., 2021). The interaction and feedback of the platform will affect users' perception of privacy security (Zhang J.X., 2016). If the theoretical framework of mobile banking security perception is constructed,

Table 1. Privacy classification of stranger and acquaintances social scene.

Stranger Social Scene		
Privacy information	**Privacy level in strangers' social scenes**	**Frequency**
Fund name	Quite high	85%
Exceeding the ratio of fund buyer earnings	Quite high	83%
PK results	Quite high	79%
Essay case	Quite high	77%
Platform QR code	Quite high	72%
Platform logo	Quite high	68%
Time	Quite high	67%
Cumulative / yesterday's earnings	High	79%
Cumulative / yesterday yield	High	77%
Position amount	Moderate	92%
User Avatar	Moderate	89%
User nickname	Moderate	89%

Acquaintances Social Scene		
Privacy information	**Privacy level in strangers' social scenes**	**Frequency**
Exceeding the ratio of fund buyer earnings	Quite high	78%
PK results	Quite high	77%
Essay case	Quite high	73%
Platform logo	Quite high	71%
Fund name	High	84%
User Avatar	Moderate	91%
User nickname	Moderate	90%
Platform QR code	Moderate	86%
Time	Moderate	82%
Cumulative / yesterday yield	Moderate	73%
Cumulative / yesterday's earnings	Low	88%
Fund name	Low	87%

it is determined that interface design elements and feedback design are the two internal factors affecting mobile banking security perception, and users' security perception levels can be changed by changing these two factors.

In the study of the path of privacy disclosure in the financial sharing scenario, we design a perceived behavior model of privacy disclosure in the financial sharing scenario by combining the behavioral influencing factor model and the perceptual theoretical framework. In scale making, the Likert 7-point scale was used to decompose each variable into several measures and the user could choose the degree of agreement or disagreement according to the expression of the question (Geoff N., 2010). All the measures are directly or indirectly derived from the previous studies, thus, the reliability and accuracy of measure items are guaranteed. We will use these two dimensions in the following prototype test to evaluate the usability of the privacy classification design. We collected a scale of 327 people, and the data analysis shows

that perception of private security and the benefit of sharing behavior were two necessary conditional variables affecting user privacy sharing behavior (Figure 1). We will use these two dimensions in the following prototype test to evaluate the usability of the privacy classification design.

We created two interaction prototypes, their size is the usual screen display size (iPhone12, 2532x1170 px). Prototype A is similar to the current mobile financial APP display information interface, similar to screenshot sharing. Prototype B is a piece of mobile financial information sharing interface with privacy classification (Figure 2). Each participant had to complete two tasks, the sharing task in the social scene of acquaintances and the sharing task in the social scene of strangers. After completing the task, each participant was asked to rate the two prototypes (Using another seven-point Likert scale).

In the semi-structured interview, we can see the difference between the privacy degree of users' mobile financial information in the social networking scenarios of acquaintances and strangers (Table 1). In the social networking scenarios of acquaintances, the privacy degree of information involving the total amount is higher, while in the social networking scenarios of strangers, the privacy degree of information involving personal identity is higher.

In conclusion, through the ranking mean analysis of private information, there are significant differences between the social scene of acquaintances and the social scene of strangers. Privacy security perception and privacy display benefit affect the privacy degree of users' privacy information in different situations.

In the path study, we confirm that users' privacy sharing behavior is influenced by the two variables of perceived privacy security and benefit of sharing behavior, and verify that the design of privacy classification can improve users' perceived privacy security in the prototype test.

CONCLUSION

The evaluation and analysis of the concept of privacy classification in the privacy sharing scenario show positive results. All users interviewed agreed that the concept of privacy gradation was a useful one. The privacy classification under the user evaluation system can make up for the matching between online privacy operations and different scenarios, and provide users with an information display and reference according to the specific situation. In addition, the respondents also agree that it is effective to improve the classification of privacy for the division of situations: to distinguish strangers from acquaintances in social situations. The privacy classification design can meet the needs of people's privacy-sharing behavior. However, the users interviewed also reported drawbacks and barriers to use the privacy grading design. A notable problem is that there are differences in the level of privacy information among users with different identities. To satisfy more people, privacy information should be divided with the maximum level of privacy.

For interaction prototype testing, the software should divide the scene effectively, and the reasonable division of the scene determines the satisfaction of users in the operation of privacy sharing. Therefore, a feature of the system

should be to adjust the privacy classification design in time according to the situation.

In this study, we establish a design prototype of privacy classification control so that each participant can find it perceptual and useful, and the use of financial revenue information sharing services can also improve their user experience. This study introduces dynamic privacy classification control, which provides a scientific reference for optimizing user experience design.

ACKNOWLEDGMENT

REFERENCES

Ann C., Michelle C.(2009), "Advancing privacy and security in computing, networking, and systems innovations through privacy by design". In: 2009 Conference of the Center for Advanced Studies on Collaborative Research (CASCON '09). IBM Corp., USA, 358–360.

Geoff N.(2010), Likert scales, "levels of measurement and the "laws" of statistics". Advances in health sciences education, 15(5),625-632.

Hu P.P.(2019), "The impact of new media technology on privacy concept in the Internet Era". (Master's thesis), Changsha: Hunan University.

Judith S. O., Jonathan G., Eric H.(2005), "A study of preferences for sharing and privacy". In: CHI '05 Extended Abstracts on Human Factors in Computing Systems (CHI EA '05). Association for Computing Machinery, New York: NY, USA, 1985–1988.

Pardis E.N., Henry D., Yuvraj A., Lorrie F. C.(2019), "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior". In: 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York: NY, USA, 534, 1–12.

Santi P.(2018), "Towards Privacy-Preserving Content Sharing for Online Social Networks". In: 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers (UbiComp '18). Association for Computing Machinery, New York: NY, USA, 1088–1095.

Sun C.Q.(2021), "Research on the influencing factors of privacy paradox on Weibo platform". (Master's thesis, Dalian: Dalian University of Technology.

Yiannis K.(2016), "Personalized Privacy-aware Image Classification". In: 2016 ACM on International Conference on Multimedia Retrieval (ICMR '16). Association for Computing Machinery, New York: NY, USA, 71–78.

Zhang J.X.(2016), "Research on mobile banking Design based on security Awareness". (Master's thesis), Guangzhou: South China University of Technology.