Shizuoka University
Graduate School of Integrated Science and Technology

Thesis submitted for the degree

Master of Informatics

Task-based Assessment to Evaluate Instagram Users' Capabilities for Personal Information Leakage Prevention

by

Chen Hongchao

Supervisor: **Yusuke Yamamoto**
Co-Supervisor: **Teppei Koguchi, Tetsushi Ohki**

August 2021

Abstract

Task-based Assessment to Evaluate Instagram Users' Capabilities for Personal Information Leakage Prevention

This paper posits a task-based assessment of the skills of Instagram users in preventing the leakage of personal information via photographs. Users cannot appropriately discern and avoid privacy risks posed by their real-world image uploaded on social media platforms such as Instagram without the inculcation of such practical abilities. The proposed test not only asked participants to identify privacy-risky photos from a predetermined set of photographs but also required respondents to specify the possible risks for each of the risky photographs picked by themselves. An aggregate of 192 participant responses was collected through a Japanese crowdsourcing service, and the performance of the respondents were appraised based on three aspects: privacy skills, familiarity with the Instagram privacy function(privacy skills and familiarity with the Instagram privacy function are adopted as two indicators for practical abilities), and attitude toward privacy. The analysis made the situation of people's generally weak privacy-protection capability clear. Besides, it was indicated that the practical abilities of users were unrelated to their attitudes toward privacy. Relating to specific privacy risk categories, people in general, and younger generations in particular, were not found to be adept at identifying the privacy risks posed by photographs that displayed their activities and disclosed job-related information.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Many people now use social networking services (SNSs) to share information with friends and families. Instagram is one of the most popular photo-sharing services. Instagram's official website reports that more than 500 million people use Instagram every day [1]. Instagram enables users to freely upload and share their photos on the Web, but users often reveal personal information unintentionally on Instagram [20].

The most general post on Instagram is often a combination of text and photographs. Privacy information could be leaked both by texts and graphics. Nevertheless, photographs receive fewer privacy cautions from posters when they are uploaded compared with text which takes time and conscious thinking to generate. Thus, this paper mainly focused on privacy information leakage prevention related to photographs.

People accidentally disclose personal information on SNS platforms for several reasons. First, they may be unwilling to prevent the leakage. Several studies have reported that younger users are less aware of privacy risks and disclose information more generously on the Web [19]. They often behave as if they do not intend to protect their privacy, even if they desire to do so. This phenomenon is known as the privacy paradox [14].

Second, users may lack the requisite practical skills to protect their privacy online. They cannot successfully transform intentions into actions even when they are strongly motivated to reserve their personal details on SNS sites. To do so, they require the competence to recognize privacy risks in the content they share on SNS platforms [4]. This paper designates the term *privacy protection capability* for the practical ability to recognize specific privacy risk categories and identify the places in which they may occur vis-à-vis images posted on SNS sites.

The present study proposes a task-based assessment (TBA) of the skills displayed by Instagram users with respect to the prevention of the unintentional disclosure of personal information in photographs, i.e., their *privacy protection capability on Instagram*. The proposed test is designed to make respondents specify the possible risks posed by each image of a prearranged set depicting material that typifies the leakage of personal information on SNS sites. The activity history of an individual or personal preferences can be revealed from such photographs, for example, a movie ticket.

This study utilized the proposed test to survey the categories of privacy risks peo-

[1] https://business.instagram.com

ple could/could not adequately detect in photographs uploaded on Instagram. It also analyzed the correlations between the privacy protection capabilities(which include privacy skills shown in TBA and Instagram-function familiarity level) and the information privacy concerns scale (IUIPC) [11] of Internet users.

The extant surveys have focused primarily on the exploration of the attitudes of Internet users vis-à-vis privacy [12]. However, only a few studies have attended to their practical skills, which are indispensable to rational decision-making regarding their confidentiality [9]. The proposed test enabled the assessment of the actual practical skills of the participants by checking precisely how much and how accurately they could identify the potential risks posed by real-world images uploaded on social media platforms.

Chapter 2

Related Works

2.1 The discrepancy between privacy attitudes and behaviors

[10] and [2] reported that Internet users are concerned about their privacy. However, according to [15] and [6], such privacy concerns do not directly affect the online self-disclosure behaviors of users. Acquisti et al. conveyed similar results: Participants displayed sophisticated attitudes toward privacy but failed to make rational choices in actual instances [1].

2.2 Nudge

A nudge is defined as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any option or significantly changing their economic incentive" [5]. Several researchers have postulated methods of using the concept of a nudge to assist the online privacy-related decision-making procedures of Internet users.

Minkus et al. proposed a Facebook interface warning parents that their posts risk disclosing the personal details of their children's privacy if their child's face is detected on a photograph [13]. Song et al. posited a novel scheme comprising descriptive, predictive, and prescription components to let social media users know who can view private information from their posts [18]. Orekondy et al. designed a nudge that alerts users on the discrepancy between their predicted objective of preventing the disclosure of personal details on their posts and their subjective privacy preferences so that the behaviors of users can suit their self-reported privacy preferences [16].

All the nudges mentioned above aim to raise the privacy-related awareness of Internet users. However, nudges could fail to assist users in transforming their inclinations into appropriate behaviors if users do not command the requisite practical skills to understand the places and actions that pose specific privacy risks. It is believed that practical skills are pivotal to the effective operation of nudges. To the knowledge of this study's authors, very few studies have measured the skills of Internet users in handling online privacy-related risks.

Thus, the current paper proposes a task-based test to investigate and measure individual practical Internet-based capabilities to augment online confidentiality and facilitate the prevention of the unintentional disclosure of personal information via social media.

Chapter 3

Method

This section describes an online study conducted between February 2 and 15, 2021, to develop a task-based test and a survey subsequently administered to ascertain the privacy protection skills, their familiarity with Instagram functions, and their attitudes apropos online privacy. Participants were asked to perform a TBA and answer questionnaire items regarding Instagram functions and online privacy attitudes. This study was conducted in Japanese, and CrowdWorks.jp, a Japanese crowdsourcing service, was used to recruit participants.

3.1 Participants

A total of 202 participants aged between 20 and 60 years were recruited via CrowdWorks.jp for the online study. Most participants were aged between 20 and 50 years. Of them, ten participants were excluded from the analysis because they did not seriously attempt or complete all set tasks. Hence, the study examined responses obtained from an aggregate of 192 participants. Table 4.1 displays the details of the age distribution of the sample. Each participant received approximately $1.00 (100 Japanese yen) as a reward after the completion of the study.

3.2 Procedure

The online investigation followed the procedure described below: (1) user registration, (2) task-based test, (3) questionnaire on familiarity with Instagram functions, (4) questionnaire on attitudes about online privacy, (5) demographic questionnaire.

First, the participants registered with CrowdWorks.jp to join this study. They were then moved to the survey website created on Google Forms. Next, they completed the task-based test of their privacy protection skills. After this assessment was accomplished, the participants were asked to respond to questionnaires on their familiarity with Instagram functions and their attitudes about online privacy. Finally, the demographic questionnaire was administered to determine the genders and ages of the respondents.

Table 3.1: Privacy-sensitive attributes and number of photos used in the task-based test. Some images possess multiple attributes.

Privacy-sensitive attribute	**#Photos**
Relationship	5
Birthplace and birth date	6
Education information	5
Living area	11
Personal preference	7
Job information	6
Activity history	19
Name	5
Portrait	10
No risk	25

3.3 Material

3.3.1 Task-based Assessment

The present study primarily proposes the design of a TBA to determine the extent to which Instagram users can detect the leakage of confidential personal information via uploaded photographs.

Orekondy et al. [16] and Han et al. [7] were referenced for the selection of the types of confidential information that could be revealed (privacy risk attributes). Orekondy et al. listed 68 user-sensitive attributes for the handling of personally identifiable information. The present study focused on 18 attributes from Orekondy's list that were related to Instagram and Han et al. also considered these characteristics to be sensitive. The *address information* in Orekondy's list was replaced by *living area attribute* because the former concept is too sensitive to find enough reflecting material photos on Instagram. Further, the *portrait* feature was added to the final list because it was observed that many images shared on Instagram revealed the facial features of people. The 18 attributes comprising the initial list are: *sexual orientation*, *relationship*, *political views*, *SNS links*, *hometown*, *profile photo*, *education*, *emotions*, *family/friend information*, *religion*, *postal code*, *birthday*, *favorites/likes*, *job*, *address information* , *real name*, *phone number*, and *email address*. For the survey, these 18 attributes were finally classified into the nine privacy-sensitive categories presented in Table 3.1:

The TBA employed photographs posing privacy risks to examine how well Instagram users could detect confidentiality threats posed by uploaded images. Instagram was searched for photographs related to the nine privacy-sensitive categories mentioned above. Attempts were made to ensure that each of the nine privacy-sensitive attributes was reflected in at least five photographs in the pre-set album.

Finally, 25 images encompassing some of the nine privacy-sensitive attributes were manually collected. Additionally, 25 risk-free photographs were randomly collected from Instagram. These 50 photographs ultimately denoted the materials utilized for

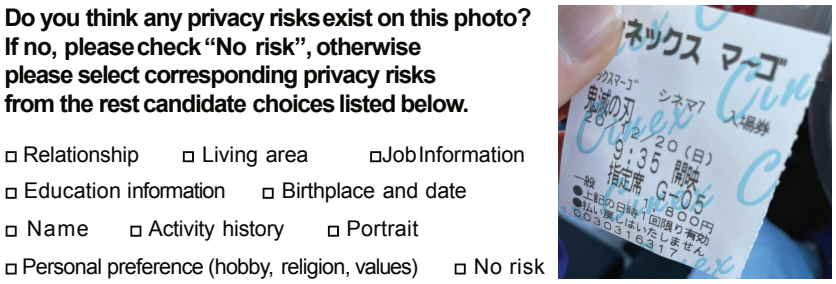

Figure 3.1: Task-based assessment sample

the TBA. Table 3.1 evinces the number of photographs that were finally arranged according to their privacy-sensitive attributes for the task-based test, each of those 50 photos was presented to participants in random orders.

It was necessary to give ensured privacy risks for each privacy-risk material photo in advance which were used as benchmarks for measuring participants' performance on TBA. Initially, two candidate standard answer sheets were prepared independently by two authors of this paper. Then those two candidate sheets were compared and their overlapped parts were taken as the final standard answers for material photographs. For example, in one candidate answer sheet, the answer for a photo was this photograph reveals Activity History and Personal Preference information. While in another candidate answer sheet, the same photograph was considered as only disclosed Personal Preference information, in this case, we set the final correct answer as Personal Preference for this photograph; In another case, if in one candidate answer sheet, a photograph was considered as no risk, while in another candidate answer sheet, this photograph was perceived to have Living Area information leaked, then the final benchmark answer was set as no risk. This benchmark answer sheet was applied to score each participant's TBA performance. As long as the participant's answers include the benchmark answer, this participant will be given one score for the corresponding material photograph.

In the experiment, the participants were required to judge which of the nine attributes were displayed on each photo (they also could answer "no risk"). Such a mixed set encompassing both risky and risk-free photos delivered the advantage of enabling an experimental environment approximating real-world instances representing the coexistence of both threat-free and unsafe photographs. Figure 3.1 illustrates an item from the administered TBA.

After the participants had completed the TBA, the accuracy of their judgment vis-à-vis the 50 photographs was calculated. The accuracy of participant p TBAs rendered for privacy-sensitive attribute a was defined via the following equation:

$$ACU(p,a) = \frac{|I_{user}(p,a) \cap I_{test}(a)|}{|I_{test}(a)|} \tag{3.1}$$

Here, $I_{test}(a)$ represented a set of photograph images encompassing the adjudged privacy-sensitive attribute a. $I_{user}(p,a)$ denoted a set of the photograph images adjudged by the participant p as incorporating attribute a. $|S|$ signified the number of elements in set S. It was posited that the higher the TBA accuracy of a participant, the

higher were the practical online privacy protection skills displayed by the participants on SNS sites.

3.3.2 Familiarity with Instagram functions

Being able to properly employ available functions is considered as an indispensable part of privacy protection capability. Instagram offers several functions to users for the protection of the privacy of their accounts and profiles. The official Instagram Privacy and Safety Center [1] was inspected, and clear statements were discovered on the following five functions available on Instagram for privacy protection:

1. Private account
2. Permission controls for being tagged by others
3. Permission controls for being mentioned by others
4. Permission controls for photo-sharing by other users
5. Controls to display the member's activity status to others

The present study investigated the extent of familiarity participants evinced vis-à-vis the five functions designed to protect their privacy on Instagram.

Each participant was offered a TRUE or FALSE choice (*TRUE/FALSE* in parentheses indicate correct answer for each question) to ascertain user-familiarity related to the above functions by answering the following questions:

1. People must send you a follow request to see your posts if you set your Instagram account as private, but they can view the list of your followers and the people you follow without issuing a request. (FALSE)
2. You can remove tags set by others on your own if you do not like being tagged. (TRUE)
3. The system will automatically allow only the people whom you follow to mention you if your Instagram account is private. (FALSE)
4. No one can share your photos and videos on their stories if your Instagram account is private. (FALSE)
5. You will no longer be able to see the activity status of other accounts if your activity status is turned off. (TRUE)

The percentage of correct answers to the above five questions was calculated to score the participant's familiarity with Instagram functions (hereinafter, *IF familiarity*). It was assumed that the higher/lower IF familiarity evinced by a participant, the more/less familiar the participant was with Instagram's privacy functions.

[1] https://www.facebook.com/help/instagram

3.3.3 Online privacy attitudes

Naresh K's Internet users' information privacy concerns index (IUIPC) was deployed to evaluate participant attitudes toward online privacy [11]. The IUIPC aims to understand and score the sensitivity of users to their online privacy. Further, some indicators were adopted from Sim et al.'s Information privacy situation awareness (IPSA) to supplement the Instagram-targeted survey. This instrument can especially reflect the privacy-related attitudes of people in interactive social network environments [17].

The present study used six general awareness-related indicators from the IUIPC and four social network-related IPSA markers to determine the general attitudes of Instagram users toward privacy protection. Participants answered the IUIPC and IPSA questionnaires on a 5-point Likert-like scale (1: strongly disagree; 5: strongly agree). The ten selected indicators (statements) are listed below:

- It usually bothers me when online companies ask me to divulge personal information.
- I am concerned that online companies are collecting too much personal information about me.
- Companies seeking information online should disclose the way they collect, process, and use data.
- A good online consumer privacy policy should display disclosure-related information clearly and conspicuously.
- Being aware and knowledgeable about the ways in which my personal information will be used is very important to me.
- Consumer online privacy is really a matter of the right of consumers to exercise control and autonomy over decisions regarding the manner in which their information is collected, used, and shared.
- I think privacy control settings are easy to use.
- I believe I am competent in terms of the knowledge and skills required to protect my privacy.
- I know exactly who can currently view the information I share.
- I know how to configure my privacy settings so that only selected groups of people can view the information I share.

The total value of the ten indicators was calculated, and the normalized total value was used as an index representing the willingness of users to protect their online privacy (hereinafter, *PA intensity*)[2]. It was hypothesized that the higher (lower) the PA intensity of participants, the more (less) sensitive they were to online privacy.

[2]The total value of the ten indicators was divided by 50 for the purpose of normalization.

Chapter 4

Results

Response data were obtained from 192 participants and analyzed. Table 4.1 displays by age the means of the participant scores on the TBA parameters of accuracy (*TBA accuracy*), familiarity with Instagram privacy functions (*IF familiarity*), and intensity of attitudes toward privacy (*PA intensity*). More detailed results attained for these three indicators are discussed in the following sections.

4.1 Performance on task-based assessment

The TBA accuracy of individual participants was evaluated to ascertain how well people could recognize specific privacy risks posed by uploaded images. Table 4.1 evinces that the study's participants identified privacy risks denoted in photographs with about 51% accuracy. In terms of age, participants in their 50s performed the best. However, no significant difference was discovered between ages.

The TBA accuracy of the participant responses was also appraised according to their sensitivity to privacy concerns. Figure 4.1 presents the respective means of TBA accuracy achieved by participants for the nine privacy-sensitive attributes. The results indicated that the participants could competently identify the privacy risks involving portraits and names. Conversely, the respondents were inadequate at identifying the risks posed by the inadvertent disclosure of job information and activity history through photographs (job information: 47.5 % accuracy; activity history: 33.9 % accuracy).

The detailed analysis of the obtained results involved the investigation of the TBA accuracy of each privacy attribute by age. Table 4.2 reveals that across all ages, the participants in their 20s tendered the worst performances for the attributes of education

Table 4.1: Means of TBA accuracy, IF familiarity, and PA intensity by age group (numbers in brackets are SD).

	Age					
	Under 20	20s	30s	40s	50s	**Grand total**
#Participant	3	50	67	52	20	192
TBA accuracy	0.393 (0.19)	0.510 (0.12)	0.510(0.12)	0.505 (0.13)	0.519 (0.09)	0.508 (0.12)
IF familiarity	0.600 (0.20)	0.468 (0.22)	0.427(0.22)	0.369 (0.23)	0.320 (0.18)	0.414 (0.22)
PA intensity	0.713 (0.05)	0.724 (0.09)	0.710 (0.08)	0.693 (0.11)	0.747 (0.09)	0.713 (0.09)

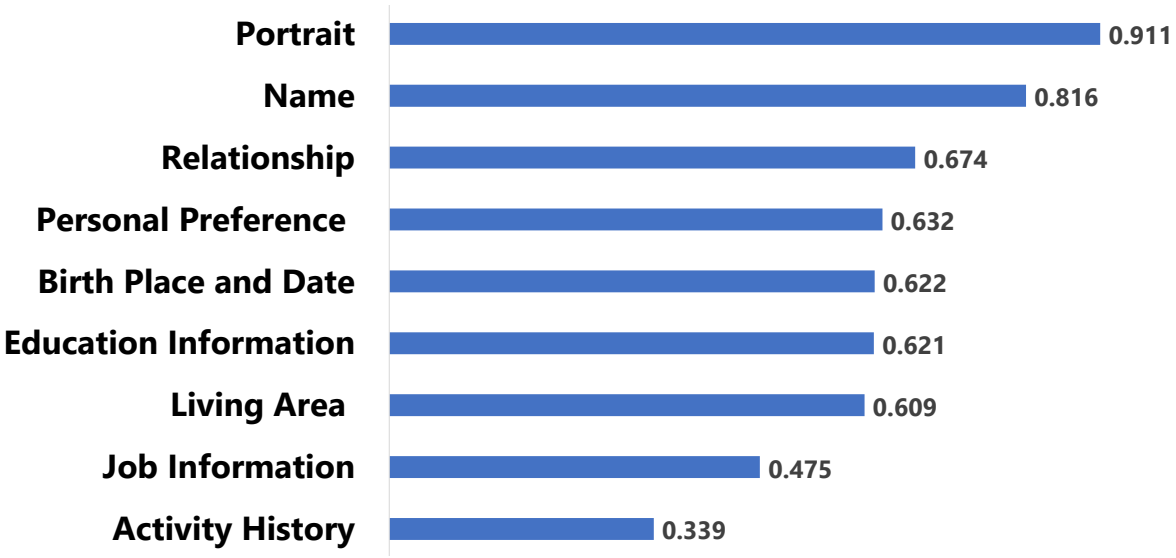

Figure 4.1: Task-based assessment accuracy by sensitivity to privacy

Table 4.2: Task-based assessment accuracy for each privacy attribute by age. Bold numbers signify minimum values across ages. The data pertaining to participants under 20 were eliminated from this table because this sample was very small.

Attribute	Age				Grand Total
	20s	30s	40s	50s	
Relationship	0.700	0.701	0.654	**0.600**	0.674
Birthplace and birth date	0.630	0.664	0.615	**0.500**	0.622
Education information	**0.550**	0.627	0.654	0.663	0.621
Living area	0.602	0.674	0.559	**0.532**	0.609
Personal preferences (hobby, religion, values)	0.603	0.689	**0.591**	0.621	0.632
Job information	**0.437**	0.463	0.503	0.550	0.475
Activity history	**0.297**	0.383	0.320	0.353	0.339
Name	0.868	0.824	0.765	**0.760**	0.816
Portrait	0.900	0.912	0.937	**0.875**	0.911
Grand total	0.510	0.510	0.505	0.519	0.508

information, job information, and activity history. In contrast, participants in their 50s represented the weakest age group in the detection of the privacy risks of revealing relationships, birth information, living area, name, and portrait.

4.2 Familiarity with Instagram functions

The study examined the extent to which participants were familiar with the Instagram functions offered to users for the protection of their privacy. Table 4.1 exhibits the statistics pertaining to the IF familiarity evinced by the participants. The mean of IF familiarity in the grand total was computed at 0.414. This result indicates that most participants were unfamiliar with Instagram's privacy protection functions and that they did not accurately grasp these functions.

The differences in IF familiarity were evaluated across age groups to accomplish a more detailed analysis. Table 4.1 shows that the older the participants, the less familiar

Table 4.3: Correlations between Task-based assessment accuracy of each privacy attribute and privacy attitude

Privacy Attribute	**Pearson's r**	**P value**
Relationship	0.014	0.843
Birth Place and Date	0.058	0.425
Education Information	0.095	0.189
Living Area	0.056	0.44
Personal Preference(hobby, religion, values)	0.076	0.297
Job Information	0.072	0.321
Activity History	0.142	0.05
Name	0.091	0.209
Portrait	0.055	0.451

they were with Instagram's privacy protection functions.

4.3 Attitudes toward online privacy

The willingness of the participants to protect their online privacy was also determined through the use of the IUIPC and IPSA questionnaires. Table 4.1 presents the means of PA intensity by age and indicates that most participants were willing to protect their online privacy. Also, no significant differences were discerned in PA intensity across age groups.

Further, a correlation analysis was performed between TBA accuracy, IF familiarity, and PA intensity to investigate the relationship between participant capabilities and attitudes with respect to the protection of privacy on the Internet. The Pearson's correlation coefficient between TBA accuracy and PA intensity was 0.2 ($r(190) = .02$, $p = .743$). The correlation coefficient between the IF familiarity and PA intensity was -0.04 ($r(190) = .04$, $p = .627$). The absence of correlations between practical capabilities and attitudes with regard to the protection of privacy on the Internet was thus confirmed.

A more detailed analysis was conducted to explore if any correlations exist between each single privacy attribute and PA intensity. Table 4.3 shows the Pearson's correlation coefficient between each privacy attribute's accuracy in TBA and PA intensity, which made it clear among those 9 privacy risk categories, there was no one specific privacy attribute that has significant correlation with privacy protection attitude.

Chapter 5

Discussion

5.1 Practical skills and inadequate privacy attributes

The experiment performed for the current study revealed a dismal view of the general state of practical abilities relating to the protection of user privacy on the Internet. On average, the study participants identified only around 50% of the risks posed by the photographic material selected for this study.

This result represents a warning that users should be less positive about their ability to recognize and manage the real-life privacy risks to which they are exposed. They must also become more aware of the need to ameliorate their practical online privacy-related skills in their daily lives. It is also considered the low-risk identification rate among participants could be partially caused by individual differences in defining "privacy risks". Since in the administration setting of this survey, participants were explicitly asked to pick out "privacy risks" from photographic materials. A participant might not think the personal information reflected in a material photo was severe enough to be called "privacy risk", even though this type of information's leakage was noticed and identified.

People born in the current millennium have grown up with the Internet and information and communication technologies, and Kezer asserted that they are more open to Internet-based self-disclosures [8]. In congruence, this study's age-group-based analysis of the TBA performance of the participants revealed that participants placed in the under 20 age group evinced the lowest average performance. However, it is unfair to claim that this cohort exhibited the lowest ability to recognize privacy-related risks because only three participants from the entire sample represented this age group.

The conducted experiment divulged that participants, especially those in their 20s, found it most problematic to recognize the privacy attributes of activity history and job information. Activity history indicates information that conveys when, where, and who did what. Job information incorporates all work-related details such as a person's professional skills or the industry in which a person is engaged. These types of information can be strong clues for the identification of individuals.

Several possible reasons could cause the low recognition rates for these two parameters. First, most people think sharing such information on SNS sites is natural and safe. Participants in their 20s may be considered the most active generation on Instagram. Their peers expose them to information about their daily activities, including

campus life at universities. It is therefore surmised that frequent exposure to activity and education information caused a low sensitivity in young participants toward the risks posed by activity history and education-related information.

Second, the participants engaged in this study found it difficult to grasp the implications of activity history and job information and should have been provided with clearer definitions during the administration of the survey.

5.2 The relationship between skills, familiarity with Instagram functions, and attitudes toward the protection of privacy on the Internet

The correlation analysis conducted for this study revealed no associations between TBA, IF familiarity, and PA intensity. These results indicate that some respondents lacked adequate practical skills in recognizing specific privacy risks posed by photographs even though they were strongly motivated to protect their online privacy.

An interesting phenomenon we observed is that even though some participants' attitudes toward privacy protection are not outstandingly motivated, it is still possible for them to have impressive performance on recognizing potential risks on TBA. Regarding this phenomenon, it is suspected those people have high reasoning abilities. Reason is the capacity of consciously applying logic to seek truth and draw conclusions from new or existing information [1]. Take the movie ticket photo in Figure 3.1 as an example, people who have high reasoning abilities are able to understand this photo poster's identification (who is neither a student nor a kid) by ticket's "General" type, while people who have inadequate reasoning abilities have difficulties in realizing it regardless of their privacy attitude.

The younger generation is more familiar with Instagram's protection functions. This observation is congruent with the results of Kezer's study [8], which verified that younger generations were more likely to activate protection measures. It is generally construed that this tendency is observed because younger Internet users are more technically adept at changing their privacy settings on SNS sites [3]. However, the outcomes of the present study underscore the importance of training privacy protection capabilities of youngsters even though they are more familiar with the technology.

5.3 Related work to be conducted in the future

The sample on which the survey was conducted for this study did not include enough participants in their 20s to support any reliable conclusions for this age group, which must be further studied to appropriately apprehend how well they can identify privacy risks in photographs. In addition, it should be noted that participants in this survey collected from the crowdsourcing platform are from a community where active and skilled online users are gathering together, which implied ordinary people's capabilities

[1] https://en.wikipedia.org

for personal information leakage prevention could be more upsetting than the worrying analysis outcome shown in this paper.

Another administrative setting needs to be improved is the way asking Task-based Assessment taker to judge privacy risks hidden behind material photographs. As mentioned in Section 5.1, the generally low-risk identification rate on Task-based Assessment was possibly caused by individual differences in defining "privacy risks", those people do not pick out the privacy risks in the photo that they have already recognized because they do not think some certain kinds of privacy information are severe enough to be called "risks" while others may regard those information as "risks". Since the aim of Task-based Assessment is to objectify test-takers' pure practical skills of privacy information protection with the least interference from their individual definitions on privacy risks, it is considered that instead of raising the question as "Do you think any privacy risks exist on this photo" where the "privacy risks" can be interpreted quite differently for each test-taker, presenting the task like "What kind of private information you can figure out about this photo's poster by taking a close look at this photo?" is hopefully a better way to maximally avoid the negative influence of participants' individual differences on privacy risks' definitions.

There is a method proposed by Yu et al. [21] available to be utilized in future studies to improve the predetermined photographs' credibility. iPrivacy is a system which makes it possible to accurately identify privacy-sensitive objects in a photo by deep learning on multi-class object extractor training. It is assumed the quality of material photographs could be confirmed if iPrivacy detected out the same privacy-sensitive objects in the photo as manual judgments.

This paper clarified the types of privacy risks which people are competent and weak to identify, but it is also worth researching the different types of privacy risks' severity levels. Not only are the risk categories with low recognition rates worth attention, some certain categories of privacy risks that can lead to particular serious damage are also worth being alarmed at.

Another challenge is to investigate the causes of observed differences in individual capabilities vis-à-vis the protection of privacy on the Internet. Further studies are also mandated for the determination of cultural differences, if any, with regard to privacy protection capabilities. Additionally, the discovery of efficient means of enhancing privacy-related abilities on the Internet may be facilitated if any related predictors significantly influencing the inculcation of such capabilities can be found.

The means to ameliorate the privacy protection capabilities of Internet users must finally be investigated so that people can smoothly transform their privacy protection intentions into rational privacy-related decisions. It is believed that the TBA implemented for this study can contribute to the design of courses and materials that can train users to imbibe the requisite Internet privacy capabilities.

Chapter 6

Conclusion

This paper studied the practical capabilities of Instagram in recognizing specific privacy risks represented by real-world photographs shared on the platform. It aimed to assist Internet users in exhibiting privacy-safe online behaviors aligned to their privacy intentions. The conducted experiment revealed the generally pessimistic state of the practical skills evinced by people regarding the protection of their privacy on the Internet. The experiment also demonstrated that participants, especially those in their 20s, found it most difficult to discern the privacy attributes of activity history and job information. These results issue a warning: People should be less positive about their ability to apprehend real-life privacy risks and should become more aware of improving their practical privacy-related skills in their everyday use of the Internet.

Challenges remain pertaining to the ways in which the privacy protection capabilities of users can be enhanced to enable them to easily transform their privacy protection intentions into rational privacy-related decisions. It is believed that the TBA applied for the current study can contribute to the design of educational courses and materials that can train Internet users to imbibe such capabilities.

Acknowledgment

Thank you to my supervisor, Professor Yusuke Yamamoto, for your patient and continuous support during the last two years. I have benefited a lot from your wealth of knowledge and your unique learner-centered education method. All the things I have learnt from you during this research procedure will not be deserted at the point of my graduation but will be carried forward and be applied throughout my following lifetime.

I gratefully recognize all the valuable suggestions provided by Professor Teppei Koguchi and Professor Tetsushi Ohki, I would not be able to realize several specific limitations of the proposed Task-based Assessment if they didn't help me.

Bibliography

[1] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE security & privacy*, 3(1):26–33, 2005.

[2] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-exposed? privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 357–366, 2007.

[3] R. N. Bolton, A. Parasuraman, A. Hoefnagels, N. Migchels, S. Kabadayi, T. Gruber, Y. K. Loureiro, and D. Solnet. Understanding generation y and their use of social media: a review and research agenda. *Journal of service management*, 2013.

[4] A. R. Brough and K. D. Martin. Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, 31:11–15, 2020.

[5] A. Caraban, E. Karapanos, D. Gonçalves, and P. Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2019.

[6] C. Hallam and G. Zanella. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68:217–227, 2017.

[7] K. Han, H. Jung, J. Y. Jang, and D. Lee. Understanding users' privacy attitudes through subjective and objective assessments: An instagram case study. *Computer*, 51(6):18–28, 2018.

[8] M. Kezer, B. Sevi, Z. Cemalcilar, and L. Baruh. Age differences in privacy attitudes, literacy and privacy management on facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1), 2016.

[9] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64:122–134, 2017.

[10] K. Liang, J. K. Liu, R. Lu, and D. S. Wong. Privacy concerns for photo sharing in online social networks. *IEEE Internet Computing*, 19(2):58–63, 2014.

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

[12] H. Masaki, K. Shibata, S. Hoshino, T. Ishihama, N. Saito, and K. Yatani. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2020.

[13] T. Minkus, K. Liu, and K. W. Ross. Children seen but not heard: When parents compromise children's online privacy. In *Proceedings of the 24th International Conference on World Wide Web*, pages 776–786, 2015.

[14] P. A. Norberg, D. R. Horne, and D. A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126, 2007.

[15] P. A. Norberg, D. R. Horne, and D. A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126, 2007.

[16] T. Orekondy, B. Schiele, and M. Fritz. Towards a visual privacy advisor: Understanding and predicting privacy risks in images. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 3686–3695, 2017.

[17] I. Sim, D. Liginlal, and L. Khansa. Information privacy situation awareness: Construct and validation. *Journal of Computer Information Systems*, 53(1):57–64, 2012.

[18] X. Song, X. Wang, L. Nie, X. He, Z. Chen, and W. Liu. A personal privacy preserving framework: I let you know who can see what. In *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*, pages 295–304, 2018.

[19] T. Taraszow, E. Aristodemou, G. Shitta, Y. Laouris, and A. Arsoy. Disclosure of personal and contact information by young people in social networking sites: An analysis using facebook profiles as an example. *International Journal of Media & Cultural Politics*, 6(1):81–101, 2010.

[20] M. H. Veiga and C. Eickhoff. Privacy Leakage through Innocent Content Sharing in Online Social Networks, 2016.

[21] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan. iprivacy: image privacy protection by identifying sensitive objects via deep multi-task learning. *IEEE Transactions on Information Forensics and Security*, 12(5):1005–1016, 2016.