DOI: https://doi.org/10.5007/2175-8077.2021.e67839

Submetido: 30/09/2019

Aceito: 29/04/2021

Future Intention to disclose personal information via mobile apps

Intenção futura de divulgar informações pessoais por meio de aplicativos móveis

Sady Darcy da Silva Júnior
Instituto Federal do Rio Grande do Sul (IFRS), Campus Restinga.
email: sady.junior@restinga.ifrs.edu.br

Edimara Mezzomo Luciano
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
email: eluciano@pucrs.br

Rafael Mendes Lübeck
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
email: rafael.lubeck@gmail.com

ABSTRACT

This study analyses the future intention to disclose personal information in order to use apps and the framing effect in relation to privacy concerns. To test the effects, an experiment was conducted involving 405 participants, using a single-factor design with independent groups and covariates. The results indicate concern about privacy is negatively related to the future intention, confirming the effects of framing on future intention, with the effect being negative in relation to the negative framing of trust beliefs and positive in relation to the positive framing of risk beliefs, while the moderating effect was not confirmed. This paper contributes to two areas: 1) privacy, because it confirms the relationship between information privacy concerns and future intention (new proposed scale); and 2) decision-making, as it demonstrates the effects of framing on risk and trust beliefs in future intentions, which, as far as is known, has not previously been shown.

Key-words: Information privacy, Apps, Risk beliefs, Trust beliefs.

RESUMO

Este estudo analisa a intenção futura de divulgar informações pessoais para usar apps e o efeito de enquadramento em relação a privacidade. Foi realizado um experimento envolvendo 405 participantes, utilizando um desenho de fator único com grupos independentes e covariáveis. Os resultados indicam que a preocupação com a privacidade está negativamente relacionada à intenção futura, confirmando os efeitos do enquadramento na intenção futura, sendo o efeito negativo em relação ao enquadramento negativo das crenças de confiança e positivo em relação ao enquadramento positivo das crenças de risco, enquanto o efeito moderador não foi confirmado. Esse artigo contribui para duas áreas: 1) privacidade, porque confirma a relação entre preocupações com a privacidade da informação e a intenção futura (nova escala proposta); e 2) tomada de decisão, pois demonstra os efeitos do enquadramento nas crenças de risco e confiança em intenções futuras, que não foram demonstradas anteriormente.

Palavras-Chave: Privacidade da informação, Aplicativos, Crenças de risco, Crenças de confiança.

22 INTRODUCTION

Individuals, groups and institutions demand information privacy so that they can determine for themselves when, how and to what extent information about them is communicated to others (Westin, 1967; Westin, 2003). Information privacy can also be defined as the ability of individuals to control information about themselves (Stone, *et al*., 1983).

Based on an understanding of information privacy as the ability to control information about oneself (Smith, *et al*., 2011), this paper addresses the concerns associated with maintaining personal information privacy, especially on mobile devices, since mobile applications (apps) may pose a threat to user privacy, to the point of discouraging users from installing apps (Mitchell, 2019; Degirmenci, *et al*., 2013). The framing effect argues that variations in the formulation of options (for example, gains or losses) can systematically produce different preferences between options of choice (Tversky And Kahneman, 1986).

This is an important matter for study because there is growing concern among the users of mobile devices regarding information privacy (Gu *et al*., 2017). The fact they usually download and install apps from centralized official repositories (Choi and Land, 2016) makes such platforms true vectors for attacks on security and privacy. In such situations, the user is delegated the decision regarding the authorization of third party access to resources that should be protected, which makes the installation of apps a risky procedure. Another concern is the complacency of users who trust the application repository, and consequently fail to enable security controls and may even disregard the issue of security when selecting and installing apps (Mylonas, *et al*., 2013).

The concerns of app users regarding information privacy is justified as various normative and descriptive theoretical developments have not been addressed in the empirical research on privacy (Wottrich, Van Reijmersdal and Smit, 2018). To date most of the research that has attempted to explain and predict this phenomenon, besides being conducted in the United States, which limits the ability to generalize the results, has been theoretical in nature.

Hence, the authors recommend future research should consider different levels of analysis, as well as the effects these different levels have on information privacy (Bélanger and Crossler, 2011). In addition, addressing the issue of information privacy in the context of using apps is complicated, since the values proposed to users - such as the ability to customize, for example - often explicitly involve the use of their information. And it is precisely this aspect that is at the root of user concerns with information privacy (Sutanto, *et al*., 2013).

Moreover, a gap exists in terms of scientific publications since, while several types of beliefs about personal information privacy have been studied in the literature (Xu, Gupta, et al., 2012; Stewart and Segars, 2002; Malhotra, Kim and Agarwal, 2004), their distinctions, relationships and behavioral impacts have not yet been systematically analyzed (Li, 2014).

Another relevant point of the present study is the introduction of a new variable called 'future intention to disclose personal information' and its relation with concern regarding the disclosure of personal information, trust and risk. From a methodological point of view, this study involved an experiment in the area of Information Technology Management, demonstrating its pioneering nature, which may open new perspectives for future studies in the area.

In experimental procedures the direct applicability of results needs a certain care, because the method in applied in controlled conditions. The uncontrolable conditions of the outside can make a bias in experiments, evew in field experiments. The applicability of results depends of a absortion of the knowledge by decision makers and, the addaptability to specific contexts. This papers provide insights to decision makers and academics to be used in others context and the insights is applicable to construct more knowledge.

Considering the explicit context, the present study aims to analyze future intentions to disclose personal information and the framing effect and on user decisions regarding the disclosure of personal information on mobile applications (apps) in relation to their privacy concerns.

23 THEORETICAL BACKGROUND

The concerns of app users regarding information privacy is characterized as a challenge for stores and apps providers, to the point of preventing users from installing mobile apps or even uninstalling them (Degirmenci, 2020). Although, the author relates which, despite factors like the previous privacy experience, the anxiety with use of computer use and the perceived control have significative effects in privacity issues. The concern with permission requests of the mobile apps there is approximately twice predictive value than the three previous factors combined to explain the general privacy concerns of mobile users' information.

Regarding the intention to disclose personal information, through mobile applications, in a study that examined the factors that influence the decision between receiving perceived benefits and being penalized with perceived risks (Wang, Duong & Chen, 2016). This was demonstrated that self-presentation and personalized services influence positively the perceived benefits, which in turn positively affects the intention to disclose personal information. Perceived severity and perceived control serve as a direct antecedent of perceived risks that negatively affect consumers' intention to disclose personal information. Compared to the perceived risks, the perceived benefits most strongly influence the intention to disclose personal information.

Considering the advent of the Internet of Things (IoT), in relation to the concern with the privacy of information in the context of the internet, many users perceive the proliferation of IoT as convenience and important informational utility. They are not aware of the unintended results of this wide accumulation data through breaches of personally identifiable information (Menard & Bott, 2020). In an experiment conducted by the authors, it was identified that IoT users process privacy issues related to their IoT devices differently from issues related to Internet use. That increasing respondents' awareness of data sharing practices influenced their perceptions related to privacy and intentions regarding the future use of IoT.

23.1Hypotheses development

Based on the Theory of Privacy Management in Communication (Petronio, 2002), the Mobile Users' Information Privacy Concerns (MUIPC) is defined as the concerns regarding possible loss of privacy, as a result of the disclosure of personal information to a specific external agent (Xu, Gupta, *et al*., 2012). As with the Concerns for Information Privacy (CFIP) (Smith, Milberg and Burke, 1996) (Stewart and Segars, 2002) and the Internet Users' Information Privacy Concerns (IUIPC) (Malhotra, Kim and Agarwal, 2004), an investigation was conducted to see whether the MUIPC had a predictive effect on behavioral intention. This was motivated by the fact that individuals with higher levels of concern for privacy are more likely to refuse to disclose personal information as well as refuse to use technology that requires data collection.

In this respect, the negative effect of privacy concerns on behavioral intention has previously been empirically tested (Xu and Teo, 2004). As a result, a negative relationship between the MUIPC and the behavioral intention to disclose personal information was found (Xu, Gupta, *et al*., 2012), showing that the MUIPC influences behavioral intention, in the same way as had already been found in relation to the CFIP (Smith, Milberg and Burke, 1996) and the IUIPC (Malhotra, Kim and Agarwal, 2004).

In terms of predicting the behavioral intention to disclose personal information, the CFIP (Smith, *et al*. 1996); (Stewart and Segars, 2002), IUIPC (Malhotra, *et al*., 2004) and MUIPC (Xu, *et al*., 2012) were found to have a significant negative effect on its variation (Xu and Teo, 2004). For the sake of clarity, since behavioral intention scales are always constructed with questions referring to the future, in this research we created a construct called 'future intention to disclose personal information' based on the combination of the above-mentioned scales. Based on the above, the first hypothesis defined for this study is the following:

H1: Concern for privacy (MUIPC) will be negatively related to the future intention to disclose personal information.

In addition to the MUIPC, the other constructs consolidated in the nomological networks of the existing scales, and therefore addressed in this study, are the following: a) Risk Beliefs and Trust Beliefs: IUIPC (Malhotra *et al.*, 2004) and IPC (Hong and Thong, 2013); b) Intention to Disclose Personal Information: CFIP (Smith, *et al.*, 1996); (Stewart and Segars, 2002), IUIPC (Malhotra, *et al.*, 2004) and MUIPC (Xu, *et al.*, 2012).

In terms of the relationships between the constructs, as previously mentioned, the intention to disclose personal information has been tested in other studies, with privacy concerns as its predictor - CFIP (Smith, *et al.*, 1996); (Stewart and Segars, 2002) and MUIPC (Xu, *et al.*, 2012). However, in the IUIPC (Malhotra, *et al.*, 2004), the tested predictors were trust beliefs and risk beliefs, constructs also used in the IPC, although not as predictors of the intention to disclose personal information. Thus, the present study has adopted the form used by the IUIPC, since it also addresses the constructs of trust beliefs and risk beliefs in its nomological network.

To achieve the study's objectives, besides the study of the constructs, the Framing Effect (Tversky and Kahneman, 1981) was also considered, focusing on a specific type of framing (the Formulation Effect). With this type of framing effect, changing the phrasing of a question is expected to induce the respondent to make a clear shift in preference from risk aversion to risk attraction. In other words, individuals tend to adopt the descriptions of results as they are described in the question, and then assess the results in a similar way, corresponding to gains or losses (Kahneman and Tversky, 1984). As a result, considering the aforementioned characteristics regarding trust beliefs, risk beliefs and intention to disclose personal information, while taking into account the fact that risk beliefs are always described with negative connotations and trust beliefs with positive connotations, while seeking to identify the best possible relationships of these constructs with the framing effect in terms of formulating questions, the following study hypotheses were defined:

H2: Negative framing of trust beliefs will have a negative effect on the future intention to disclose personal information.

H3: Positive framing of risk beliefs will have a positive effect on future intention to disclose personal information.

Analyzing the three hypotheses above, it is perceived that concern for privacy (MUIPC) as well as both the negative framing of trust beliefs and the positive framing of risk beliefs act as predictors of the future intention to disclose personal information. However, as mentioned above, when using the framing effect, the respondent is expected to be induced to a clear change of preference, from risk aversion to risk attraction. That is, it is expected that the manner in which the questions concerning hypotheses H2 and H3 are written (the framing), whereby the original positive and negative connotations are reversed, respectively, will provoke a change in the future intention of the respondents to disclose personal information.

Thus, the framings proposed in both hypotheses, depending on the degree, could even change the relationship between the concern for privacy and the future intention to disclose personal information. This would characterize a moderating effect (HAIR *et al.*, 2009), which occurs when a third variable or construct alters the relationship between two related variables/constructs. Based on these observations, the following hypothesis was defined:

H4: Framing trust beliefs negatively and risk beliefs positively will moderate the relationship between concern for privacy and the future intention to disclose personal information.

24 METHODOLOGICAL PROCEDURES

This study consisted of three steps: the first involved validating the scales; the second pre-testing scenarios; and finally, the experimental third step involved testing the proposed relationships. To validate the scales, a focus group was formed with six experts in information privacy and factor analysis. The adjustments suggested by the specialists and the factor analysis were made to the initial version of the theoretical model and the scales used in the research. Thus, the first phase was completed with the definition of the model and the scales. For the data collection, it should be noted that specific software was developed by a company based in Brazil, which will have its name omitted for ethical reasons.

The scales used to compose the experimental model were: MUIPC - Mobile Users' Information Privacy Concerns (Xu, *et al.*, 2012); scales of risk beliefs with negative connotations and trust beliefs with positive connotations, according to the original versions used in the IUIPC (Malhotra, *et al.*, 2004) and IPC (Hong and Thong, 2013); scale of future intention to disclose personal information, according to its original versions, namely CFIP (Smith, *et al.*, 1996); (Stewart and Segars, 2002), IUIPC (Malhotra, *et al.*, 2004) and MUIPC (Xu, *et al.*, 2012).

A later study validated the MUIPC scale (Degirmenci *et al.*, 2013), and recommended the exclusion of only a single question from the Perceived Surveillance dimension. In the present study, the results pointed to the need to exclude the same question from the same dimension. However, this factor showed very low total explained variance. Hence, a new EFA was required, in which the question was excluded from perceived surveillance dimension and the number of factors set at three, based on earlier MUIPC studies (results in the appendix).

24.1 Experimental procedures and pre-test

The initial procedure in the second phase of the study was to decide on the experimental design. The independent variable was the individual's belief regarding risk and trust, which was manipulated and the effects measured and compared (Malhotra, 2006). While, the independent variable (future intention to disclose personal information), the values of which depend on manipulation of the independent variables by the experimenter, represents the criterion or standard by which the results of the experiment will be judged (Aaker, Kumar and Day, 2004).

After defining the independent variable and the dependent variable, the next step was to define the levels of experimental treatment to be used, which means the alternative manipulations of the independent variable under investigation (Aaker, Kumar And Day, 2004). In this study, the framing of the risk beliefs and trust beliefs of mobile application users, which characterizes the manipulated independent variable, will have two types of experimental treatment: negative framing and positive framing, with a control group. As for the distribution of the test units in groups, as well as the respective treatments applied to the manipulated independent variable, the experiment was composed of three groups with their respective treatments, as shown in Table 1.

Control group	Trust beliefs	Positive framing
	Risk beliefs	Negative framing
Experimental Group 01	Trust beliefs	**Negative framing (inverted)**
	Risk beliefs	Negative framing
Experimental Group 02	Trust beliefs	Positive framing
	Risk beliefs	**Positive framing (inverted)**

Considering the randomness guaranteed by the software developed for the experiment, as well as the levels of experimental treatment for the manipulated independent variable cited in Table 1, each participant that finished answering the questions in the MUIPC scale was automatically directed to one of the groups shown in Table 1, randomly, in the sequence 1) Control Group (Sentences with risk beliefs framed negatively and trust beliefs framed positively) ➔ 2) Negative Framing Group (Sentences with risk beliefs and trust beliefs framed negatively) ➔ 3) Positive Framing Group (Sentences with risk beliefs and trust beliefs framed positively), and so on, in accordance with the respective treatments shown in Table 1.

Based on the hypotheses defined in this research, the of mobile application users' information privacy concerns (MUIPC) was used as a covariate. Thus, the experimental design in this study this is characterized as being a single factor with independent groups and the use of covariates (Boniface, 1995). Hence, each respondent participates in only one of the treatments, in contrast to the intra-subject design - repeated measures design, in which each respondent participates in all the experimental conditions (Boniface, 1995). The experiment is also a post-test-only control study group, characterized as a type of true experimental study because the participants are randomly allocated to the groups (Aaker, et al., 2004; Malhotra, 2006), with the experimental groups are exposed to treatments, while the control group is not.

As for the fifth and penultimate obligatory procedure for the characterization of an experimental design, the selection tendency was controlled to ensure the subjects participating in the experimental group did not differ from the subjects in the control group, nor did the experimental group not differ systematically of the population being studied, considering some relevant aspects (Aaker, *et al*., 2004). The first guarantee was ensured by randomly allocating the subjects to the groups, as previously explained.

Finally, the sixth and final procedure that characterizes an experimental design involves minimizing the influence of extrinsic variables (also known as strange variables or confounding variables) on the results of the experiment (Malhotra, 2006; Aaker, *et al*., 2004). This study, by adopting only one measurement per subject, by itself, eliminated some extrinsic variables, such as maturation, mortality effect, selection bias and instrumentation effect, the latter two being also avoided by the fact standardized software was used as the collection instrument for all the respondents. Therefore, the considerations regarding the experimental design of this research are closed, in accordance with the recommended procedures (Aaker, *et al*., 2004).

With the experimental procedures defined, it was possible to begin the pre-test, which was composed of respondents with the following characteristics: The mean age of the respondents was 34.84 years (σ=9.31 years), the minimum being 18 years and the maximum 66 years, while the majority was female (57.0%). In terms of the use of apps, measured in the number of average accesses per day, 50.5% accessed up to 15 times a day, 33.3% accessed from 16 to 59 times a day, and 5.5% accessed 60 times a day or more, while 10.7% reported the situation was not applicable.

This criterion for the number of daily accesses to apps was based on Flurry (2014), a company that analyzes the use of apps on 1.855 billion smartphones worldwide, and divides people into three groups: regular users, who open apps of 1 to 15 times a day; super-users, who open between 16 and 59 times a day; and "addicts," who open apps 60 or more times a day.

With a view to validating the reliability of the research instrument and comparing the structure of the Portuguese version with that of the original, the statistical techniques applied in the analysis of the collected data were the following (Malhotra, 2006): Cronbach's alpha, KMO and Bartlett tests, with Exploratory Factor Analysis using principal component analysis and varimax rotation (Hair *et al*., 2009). Since this is a very recent scale, it was back-translated into the Portuguese language and applied with Brazilian respondents, we opted for exploratory factor analysis (results in the appendix).

In terms of functionalities required for this study, the software was built respecting the following rules: a) to guarantee the random assignment that characterizes an experimental design (Aaker, Kumar And Day, 2004), each treatment given to the manipulated independent variable (Positive or Negative Framing) was conducted as the respondents in the group in the experiment room completed answering the items in the MUIPC scale – the step immediately preceding experimental process, randomly. Other rules were established, such as not digitally entering the information, not leaving any question unanswered or returning to previous questions, it was possible to give only one answer per question, the experiment was conducted in laboratory via a web interface.

An access link was made available, which was posted on the researchers' contact network and social networks, similar to the that carried out in the article that sought to validate the MUIPC (Degirmenci, Guhr And Breitner, 2013). People on the network were invited to access the software site and answer the questionnaire, while social network respondents were encouraged by a posting calling attention to the questionnaire and inviting them to answer it.

The sequence in which the items (total 3) were presented to the respondent in the software was as follows: MUIPC (8 questions); Framing - Random/ Experimental variable (8 questions); First attention check (1 question); Future intention to disclose personal information (5 questions); Socio-demographic and Control (8 questions); Second attention check (1 question); and Text field requesting criticisms and suggestions (1 question). In order to standardize the understanding of what was being requested, as well as to facilitate the completion of the questionnaire, a set of instructions recommended by the experts were given to the respondents at the beginning of the survey.

The answers were collected following the same pattern used in the original scales, both using a 7-point scale, ranging from 1 - Strongly Disagree to 7 - Strongly Agree. Once the questionnaire was completed, a text field was made available for the respondents to express their impressions regarding the procedure, as well as doubts and suggestions.

In addition, two check questions were included in the questionnaire completion process, one requesting that only option 6 be marked on the Likert-type scale, approximately in the middle of the questionnaire, and the other requesting that option 2 be marked, located at the end of the questionnaire. These two questions served as a basis for eliminating any respondents who did not fill them correctly. Four hundred and eleven (411) respondents started the pre-test, 95 gave up and 7 missed the check questions. The valid sample was 309 respondents.

Once the validity of the scales and scenarios considered adequate was checked, both by the researchers and the consulted experts (see appendix), the preparatory stage for the experiment was concluded. The next section deals with data collection for evaluating the proposed model considering the above mentioned procedures.

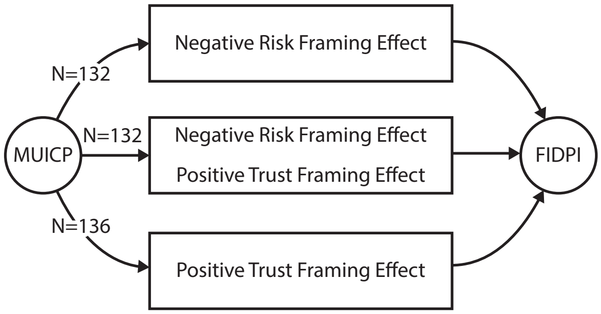
25 EXPERIMENTAL PROCEDURES AND RESULTS

Data was collected from undergraduate students taking Management courses at four Brazilian higher education institutions and the test units were selected by convenience. The respondents went to a laboratory and individually answered the questions. In terms of the security and validation criteria, the pre-test software followed the criteria described in the pre-test. The results were as follows: 514 started the questionnaire; 65 did not complete the questionnaire 34 completed questionnaires were rejected due to checking errors; and the valid sample was 412. All the statistical techniques used in this section were obtained through the SPSS Statistics 20 software package. As previously mentioned, the scale validation procedures were the same as those adopted in the previous section and the data are available in the appendix.

25.1Results of the experiment

Regarding research design in general, the adopted approach must connect the data to the research question (Punch, 2005). Accordingly, among the hypotheses defined in this study, it was necessary to check effects and measure both the relationships and the levels of the variables in determined situations to enable those hypotheses to be tested. Therefore, the beliefs of individuals were manipulated as a factor, with two treatments (positive framing of risk beliefs and negative framing of trust beliefs), while the absence of framing constituted a control group. All of these situations occurred between the MUIPC and Future Intention to Disclose Personal Information (FIDPI) constructs (Figure 1).

Figure 1 Experimental design


MUICP
N=132
N=132
N=136
Negative Risk Framing Effect
Negative Risk Framing Effect
Positive Trust Framing Effect
Positive Trust Framing Effect
FIDPI

For the purposes of clarification, it is should be remembered that the absence of framing is the standard condition in research into concern with information privacy, whereby risk beliefs are invariably described with negative connotations and trust beliefs are described with positive connotations. By means of the experimental design, it was possible to test hypotheses H2 and H3 specifically, observing the main effect of each type of framing. The other hypotheses considered in this study (H1 and H4), although unrelated to the experiment itself, will also be analyzed in this section. After responding to the eight MUIPC questions, the users were allocated to the framing groups, with two experimental groups (positive framing of risk beliefs and negative framing of trust beliefs) and a standard-control group used in previous research on scales addressed in this study.

Next came the first attention check, in which the respondents were asked to select option 6 on the scale. That was followed by the questions regarding the future intention to disclose personal information. In addition to the questions, the original versions of the respective scales were used, measured using a seven-point scale with anchors ranging from “Strongly Disagree” to “Strongly Agree” were also presented. Towards the end of the questionnaire, socio-demographic issues and those related to the control variables were presented, as well as the second attention check, requesting the respondent to select option 2.

25.2 Data analysis

Regarding the study hypotheses, for H1 a correlation was made between the MUIPC variable and the future intention to disclose personal information. In relation to H2 and H3 Analysis of Variance (ANOVA) and Analysis of Covariance (ANCOVA) were used. The ANOVA, widely used in experimental studies (Ferrin *et al*., 2007; Laer and Ruyter, 2010), requires the presence of factors - independent categorical variables - which in this study was the manipulated or treated variable (risk/trust beliefs). Regarding ANOVA, the influence of the covariables can be adjusted in the analysis model prior to initiating the ANOVA procedures (Hair *et al*., 2009). Thus, this research used ANCOVA to control the effects of the control variables.

In addition to these techniques, Cohen’s *d* (1988) was calculated as well as of η^2_p, to check the effect size of the independent variable on the dependent variable, since both measures indicate the power that a manipulated independent variable has in experimental conditions. In terms of interpretation, the size of the effect is a quantitative reflection of the magnitude of some phenomenon, and follows certain conventions regarding size (Cohen, 1988): values up to 0.20 are considered small; of 0.20 to 0.80, with 0.5 being reference, are considered average; and above 0.80 are considered large. The η^2_p was interpreted as follows: values around 0.01 can be considered a small effect; values around 0.06 are considered average effect; and values around 0.13 can be considered large effect.

The moderating effect of the negative framing of trust beliefs and positive framing of risk belief on the relationship between concern for privacy and the future intention to disclose personal information (H4), was checked by performing regressions for each type of framing using future intention to disclose personal information as the dependent variable and the MUIPC as the independent variable. Afterwards, the results of the two regressions (Betas) were compared. The two results were both found to be different and significant, thus characterizing a moderating effect. Otherwise, there is no moderation.

In socio-demographic terms, the mean age of the respondents was 31.48 years (σ=10.45 years), with a minimum of 17 years and a maximum of 61 years, while the majority were female (60.2 %). In terms of app use, measured in terms of the average number of accesses per day, 36.8% accessed up to 15 times a day, 43.2% accessed from 16 to 59 times a day, and 13.6% accessed 60 times a day or more, while 6.4% of respondents reported that this situation was not applicable.

The dependent variable future intention to disclose personal information was measured using a new seven-point scale composed of five items and built from the combination of previous scales used in research on concern about privacy from CFIP (Smith, Milberg And Burke, 1996); (Stewart *et al*., 2002), IUIPC (Malhotra, Kim And Agarwal, 2004) and MUIPC (Xu, Gupta, *et al*., 2012). In terms of reliability, the scale was attested by the Cronbach’s alpha (α=0.869) and factorial analysis (see appendix).

As mentioned above, in the procedures section, some variables were controlled to avoid intervening effects in the study results. Therefore, in addition to the variable that measures the level of concern for information privacy with the use of mobile applications (MUIPC), other control variables were included in the analysis model (treated as covariates in the Covariance Analysis), and their control effects on the variables were identified. Thus, the results obtained (in brackets) were as follows:

a) MUIPC (M=5.31 in a scale of 1 to 7; F(1.401) = 17.100; p < 0.001);
b) If the respondent had a mobile device that allowed access to the Internet and use of apps (96.3% yes, 3.7% no; *F*(1.401) = 1.617; *p* = 0.204);
c) Age (*M* = 31.48 years; *F*(1.401) = 28.036; *p* < 0.001).

Observing the values obtained, only MUIPC (p <0.001) and age (p <0.001) had a significant controlling effect on the variations in the future intention to disclose personal information. Thus, the variable referring to the respondent having a mobile device that allowed access to the Internet and use of apps was excluded from the subsequent analyzes.

Since the covariates should have some correlation with the dependent variable (HAIR *et al.*, 2009), despite the evidence presented in the analyzes of covariance reported above, it was also decided to use the correlation analysis technique. As a result, the two variables presented significant correlations at the p<0.001 level with the dependent variable future intention to disclose personal information, with MUIPC (r=-0.245) and age (r=-0.250).

Following this initial verification, the variables were tested for differences in the means between the experimental groups, with the following results being obtained: Negative Framing: n= 137 M = 5.6 (MUIPC) M= 31.96 (age); Control group: n= 132 M = 5.22 (MUIPC) M= 31.21 (age); Positive Framing: n= 136 M = 5.1 (MUIPC) M= 31.26 (age). When observing the data, it can be seen that, in proportion to the magnitudes of each variable, neither one presents significant differences.

Before performing ANOVA and/or ANCOVA, some checks were conducted for: missing values, outliers, normality and homoscedasticity (Hair *et al.*, 2009). The missing data were checked using a simple frequency distribution of the missing data for each variable, in which no missing data were found for the observed variables. This had been expected, since the absence of missing data was guaranteed when exporting the data to the software.

As for atypical observations, they were evaluated by means of box-type graphs. As a result, seven cases were withdrawn, reducing the initial database from 412 to 405 cases. The normal distribution of the data, which compares their distribution to a normal distribution, was confirmed by calculating the asymmetry (a simple arc) and kurtosis (flattened or elevated distribution). In terms of interpretation, the most commonly used critical values are as follows: plus, or minus 2.58 for a significance level of 0.01 and plus or minus 1.96 for a significance/error level of 0.05. Hence, if the values exceed these parameters the distribution is not normal (HAIR *et al.*, 2009).

Considering the variables to be used in the subsequent analyzes herein, according to the most conservative parameters (Hair *et al.*, 2009), they all met the requirements for univariate normality. The study's dependent variable, the future intention of disclosing personal information, presented absolute values for kurtosis (0.841) and asymmetry (0.114). MUIPC presented absolute values for kurtosis (0.362) and asymmetry (0.784), while age presented kurtosis (0.187) and asymmetry (0.816).

Following the statistical assumptions for ANOVA and/or ANCOVA, we checked the homoscedasticity of the data using the Levene test, with the manipulation of the risk and confidence beliefs as a predictive variable and the future intention to disclose personal information (Levene= 0.092; p= 0.912), the MUIPC (Levene= 1.380, p= 0.253) and age (Levene= 2.559, p= 0.079) as dependent variables. Analyzing the results, all with p> 0.05, it can be stated that no variable presents different variances between the groups of the predictive variable.

Finally, the multicollinearity of the data (HAIR *et al.*, 2009) was checked by calculating the tolerance values and the variance inflation factor (VIF). For the purpose of interpreting the results, tolerance values lower than 0.19 and VIF values above 5.3 indicate a multiple correlation above 0.9, which characterizes multicollinearity (HAIR *et al.*, 2009). When analyzing the variables of this study regarding multicollinearity, based on the tolerance values and VIF, it was found that none presented values outside the specified limits, since the lowest tolerance value and the highest VIF value observed were those of the variable, the future intention to disclose personal information (0.887 and 1.127, respectively). In the bivariate correlation analysis, the highest correlation was found in the relationship between future intention and age (r= 0.253), and the value found did not indicate multicollinearity among the variables.

25.3 Testing the hypotheses

In relation to Hypothesis 1, this was previously validated when the MUIPC was found to have a negative and significant correlation with the future intention to disclose personal information (r= -0.245), with a significance at level $p<0.001$. Therefore, Hypothesis 1 of this study was accepted (H1), since concern with the privacy of personal information with the use of mobile applications (MUIPC) was shown to be related to the future intention to disclose personal information.

To test H2 and H3, covariance analysis (ANCOVA) was used to compare the effects of positive and negative belief constructs with the standard situation used in the research (a negative connotation for risk beliefs and a positive connotation for trust beliefs) regarding variations in the future intention to disclose personal information. Thus, ANCOVA was carried out with the manipulation of the framing risk and trust beliefs as an independent variable, the future intention to disclose personal information as a dependent variable, and MUIPC and age as covariables. The results of this analysis are shown in Table 4:

Table 4 Effects of Framing the risk and trust beliefs

Dependent Variable: Future intention to disclose personal information

Source	Type III Sum of Squares	Degree of freedom	Mean Squared	F	Sig.	Partial eta squared
Corrected model	214.603a	4	53.651	25.797	.000	.205
Interception	1.504	1	1.204	.723	.396	.002
MUIPC	28.927	1	28.927	13.909	.000	.034
Age	54.268	1	54.268	26.094	.000	.061
Belief Framing	96.860	2	48.430	23.287	.000	.104
Error	831.891	400	2.080			
Total	7711.800	405				
Corrected Total	1046.494	404				

■ R^2 = .205 (R^2 adjusted = .197)

When assessing the power of an analysis, the sample size has an impact not only on the assessment, but also on the anticipation of its statistical power (Hair *et al.*, 2009). As a parameter to detect a significant coefficient of determination (R^2), in relation to the reciprocal effect between the sample size of this research (N=405), a level of significance (α)=0.01 and three independent variables, which also is the case in this study, (Hair *et al.*, 2009) suggests a minimum value of 5% (0.05), considering a power (probability) of 0.80. As can be observed, the R^2 obtained in this study is higher than the suggested minimum. Moreover, it is important to note that the quantity of three independent variables was adopted to obtain the reference coefficient of determination since, in ANOVA/ANCOVA, the covariates represent independent metric variables (Malhotra, 2006).

The framing of the risk and trust beliefs can be seen to have had a significant effect on the future intention to disclose personal information (F (2, 400) = 23,287; $p<0.001$; η^2_p= 0,104). By means of the partial square (η^2_p) of the effect, it can be seen that the framing of the risk and trust beliefs explains 10.4% of the global variations in the future intention to disclose personal information, which characterizes a medium to large effect (values around 0.06 are considered average effects and values around 0.13 can be considered a large effect).

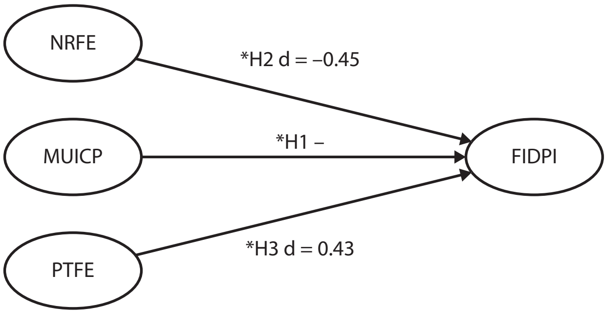
Specifically, the negative framing of trust beliefs (*M*= 3.38) presented a lower mean for future intention to disclose personal information than that found for the control group condition (positive framing of trust beliefs) (*M* = 4.07, *p* <0.001, *d* = -0.45). Thus, the effect size of the negative framing of trust beliefs has on the future intention to disclose personal information can be considered medium, thus supporting H2, that framing trust beliefs negatively has a negative effect on the future intention to disclose personal information.

Positively framing risk beliefs (*M*= 4.72), in turn, generated a future intention to disclose personal information higher than that found for the control group condition (negative framing of risk beliefs) (*M*= 4.07, *p*<0.001, *d*= 0.43). Hence, the effect size of the positive framing of risk beliefs on the future intention to disclose personal information may also be considered medium, thus supporting H3, that positively framing risk beliefs has a positive effect on the future intention to disclose personal information. Moreover, the variables MUIPC (F (1, 400) = 13,909, p <0.001; η^2_p = 0.034) and age (F (1, 400) = 26,094, p <0.001, η2p = 0.061) controlled the variations in the future intention to disclose personal information in the analysis model.

To test the hypothesis 4, which addresses the moderating role of negatively framing trust beliefs and positively framing risk beliefs in the relationship between concern about information privacy with the use of apps and the future intention to disclose personal information, linear regression was used (Baron And Kenny, 1986).

As a result, the regression that included the negative framing of trust beliefs was significant (*B*= -0.030; *t*= -2.531; *p*<0.05), while the regression with the positive framing of risk beliefs as a variable selection was not significant (*B*= -0.009, *t*= -0.898, *p*= 0.371). Thus, although the two regressions presented different results, which might indicate that the form of framing causes a change in future intentions, this cannot be said to be the case, since one of the framings was not significant. Therefore, no moderating effect was characterized. Figure 2 summarizes the confirmed hypotheses and the final model.

Figure 2 Final model



Regarding H1, the confirmation was of great relevance for the following analyzes of the study, besides corroborating what had been found in previous studies. The acceptance of H2 and H3 was of great relevance in terms of the contribution of this study, since it reveals that manipulation through negative framing of trust beliefs and positive framing of risk beliefs causes medium-sized effects on the future intention to disclose information personal. Thus, a question remains regarding the use the mobile application industry would make of this effect, to the extent that they became aware of it (if they do not already know).

25.4 General discussion

While people are increasingly using apps, when doing so, they rarely pay attention to security criteria regarding access to their data (Degirmenci, *et al.*, 2013). In this context, the fact it is unknown whether users are increasing installing mobile applications due to real perceived needs or the fruit of manipulative tools that stimulate this behavior is intriguing. The fact is they can lead to the invasion of privacy of personal information under the pretext of being 'free', although they may actually be charging the user an invisible price.

The results obtained from the analysis of the moderation hypothesis (H4) show that the positive framing of the risk beliefs was not significant, in contrast to the negative framing of trust beliefs, which was significant. Thus, this result is similar to that which supports the framing effect, by which the sensation associated with the loss of a value is stronger than the sensation associated with the gain of the same value (Tversky And Kahneman, 1974), which refers to the value function in the form of 'S' (Reflex Effect), which was one of the effects identified in the seminal article by TP (Kahneman And Tversky, 1979).

Having privacy of information as a central concern, this study analyzed the effects of concern with the disclosure of personal information and the future intention to disclose personal information and the moderation of the risk of trust in the scenario of mobile applications. To do so, it was necessary to identify the best way to evaluate user decisions regarding the disclosure of personal information for the use of mobile applications. Considering the theoretical model, this study began based on the nomological network of constructs of the scales referring to the concerns of users regarding privacy (CFIP, IUIPC, IPC and MUIPC).

The CFIP, IUIPC and MUIPC scales were found to have a negative effect on the behavioral intention to disclose personal information, a construct totally in line with to the objective of this study. As a result, from the junction of the constructs used in the three scales, a new construct entitled 'future intention to disclose personal information' was suggested and validated in this study.

The next step was to investigate any possible relationship between concern about information privacy and decisions about the disclosure of personal information for the use of apps, which directly concerns Hypothesis 1 (H1), which was accepted in this study, that concern with privacy (MUIPC) would negatively relate to the future intention to disclose personal information. This procedure was essential because, based on that, it was possible to build the nomological network for this study, serving as the basis for further analysis. With this, the third specific objective of this study was achieved.

Finally, it was necessary to identify and execute a procedure capable of subjecting the users' decisions on the disclosure of personal information to the framing effect (Tversky And Kahneman, 1981). In the same way as the identification of the future intention to disclose personal information, based on the nomological network of the scales referring to users' privacy concerns (CFIP, IUIPC, IPC and MUIPC), it was found that the IUIPC scales IPC use constructs referring to risk and trust beliefs.

When analyzing these constructs, it was noticed that in both cases the questions regarding risk beliefs are described with negative connotation, while trust beliefs, by contrast, are given a positive connotation. With this insight, the connection with the framing effect was direct, since it argues that variations in the formulation of options (for example, in terms of gains or losses) can systematically produce distinct preferences between options of choice (Tversky and Kahneman, 1986). In other words, individuals tend to adopt the descriptions of results as they are described in the question, and then evaluate the results in a similar way, corresponding to gains or losses (Kahneman and Tversky, 1984).

Thus, the risk and trust belief scales were altered and attributed positive and negative connotations, respectively, by using the semantic differential, changing two words, at most, in each item of the scale, in order to reverse the connotation from loss to gain, in the case of risk beliefs, and from gain to loss, and in the case of the trust beliefs. Once these scales were validated with the focus group, it was possible to test the remaining study hypotheses. In theoretical terms, this research contributes towards filling two gaps in scientific publications on information privacy: one referring to concern with information privacy and another concerning behavioral beliefs.

Finally, another study carried out in Brazil (Britto-Da-Silva, 2015), showed that, of the six evaluated, the dimensions 'Secondary Use' and 'Improper Access' presented the highest levels of concern. This result may explain to some extent why the MUIPC scale was found to be better statistically adjusted in these two dimensions.

26 FINAL REMARKS

Concern with the privacy of information is an increasingly recurring theme not only in academic research, but also in people's daily lives. However, historically, the proposed measurement scales referring to the subject, as demonstrated in this study, are in their entirety in the English language and have been applied among North American respondents. This finding is intriguing, since Brazil currently ranks fifth among the countries with highest rates of downloading mobile applications, an industry responsible for handling around 25 billion dollars in the country and may well reach 90 billion dollars in 2019, according to Ministry of Science, Technology and Innovation (MCTI, 2019). Thus, these figures underscore another contribution of great relevance provided by this study, since it tests relations about concern for the privacy of information in an emerging economy.

In theoretical terms, in relation to behavioral beliefs, various types of beliefs about the privacy of personal information have been studied in the literature. Nevertheless, their distinctions, relationships and behavioral impacts have not yet been systematically analyzed (Li, 2014). The present study has sought to undertake this task, insofar as risk and trust beliefs were treated experimentally, in order to assess the impact of the treatments on the future intention to disclose personal information.

The treatments, in turn, were conducted using the Framing Effect (Tversky And Kahneman, 1981). In this regard, the best of our knowledge no previous study has attempted to use of the framing effect, derived from the Theory of Perspective, in association with the theme of privacy. As a consequence, given the confirmation of the hypotheses that the negative framing of trust beliefs and positive framing of risk beliefs have an effect on the future intention to disclose personal information, a new perspective on the decision-making among mobile application users about the privacy of their personal information has opened up.

Although all necessary methodological care was taken, this study presents some limitations that may denote important aspects for any follow up research dealing with the same phenomenon. As for validity in experimental studies, Winer (1999) suggests realism may also affect this dimension, since tasks, stimuli and treatments may have little to do with reality, and therefore hamper the translation of results into reality. In addition, the scales are subject to the level of understanding of the Brazilian respondents, which may not be the same as that of North Americans. Likewise, the validation of the focus group itself may have caused some bias in the responses, which may have gone undetected in the study.

Further research in this field might consider applying the proposed relations with new variables within concern with the privacy of information and future intentions to disclose personal information: such as the influence of culture, open data, and information governance. Lastly, it is worth highlighting the proposed new scale, which refers to the future intention to disclose personal information, built by combining previous scales used in research on concern regarding information privacy, which would benefit from further investigations into different contexts and relations with other variables.

ACKNOWLEDGMENTS

This study was financed, in part, by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brasil (CAPES) and the Fundação de Amparo à Pesquisa do Estado do RS (FAPERGS). The authors are grateful for the institutional support of PUCRS, and the Graduate Program of Business Administration.

REFERENCES

Aaker, D.A. Kumar, V. and Day, G. S. (2004) Pesquisa de marketing. 2 ed., São Paulo: Atlas, 2004.

Baron, R.M. and Kenny, D. A. (1986) The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, Vol. 51, pp. 113-118.

Bélanger, F. and Crossler, R.E. (2011) Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, Vol. 35, No. 4, pp. 1017-1041.

Boniface, D. R. (1995) Experiment Design and Statistical Methods for Behavioural and Social Research. London, UK: Chapman &and Hall.

Britto-Da-Silva, V.R. (2015) Preocupação com a privacidade na Internet: uma pesquisa exploratória no cenário brasileiro. Dissertação (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia (FACE). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.

Choi, B. C. F. Land, L. (2016) The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. Information & Management, 53(7),

Cohen, J. (1988) Statistical power analysis for the behavioral sciences (2 ed.). New Jersey: Lawrence Erlbaum.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261-272.

Degirmenci, K., Guhr, N. And Breitner, M. H. (2013) Mobile applications and access to personal information: A discussion of users' privacy concerns. Thirty Fourth International Conference on Information Systems (ICIS). Milan.

Ferrin, D. Kim, P.H. Cooper, C.D. and Dirks, K.T. (2007) Silence speaks volumes: The effectiveness of reticence in comparison to apology and denial for responding to integrity and competence-based trust violations. Journal of Applied Psychology, Vol. 92, No. 4, pp. 893-908.

Jie Gu, J. Yunjie (Calvin) Xu, Heng Xu, Cheng Zhang, Hong Ling, (2017) Privacy concerns for mobile app download: An elaboration likelihood model perspective, *Decision Support Systems*, 94, 19-28. https://doi.org/10.1016/j.dss.2016.10.002

Hair Jr. J.F. William, B. Babin, B. and Anderson, R.E. (2009) Análise multivariada de dados. 6.ed. Porto Alegre: Bookman.

Hong, W. and Thong, J.Y. (2012) Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. MIS Quarterly, Vol. 37, No. 1, pp. 275-298.

https://doi.org/10.1016/j.im.2016.02.003.

Kahneman, D.P. and Tversky, A. (1979) Prospect theory: an analysis of decision under risk. Econometrica, Vol. 47, pp. 263-292.

Kahneman, D.P. and Tversky, A. (1984) Choices, Values, and Frames. American Psychologist, Vol. 39, No. 4, pp. 341-350.

Laer, T. and Ruyter, K. (2010) In stories we trust: How narrative apologies provide cover for competitive vulnerability after integrity-violating blog posts. International Journal of Research in Marketing, Vol. 27, No. 2, pp. 164-174.

Li, Y. (2014) A multi-level model of individual information privacy beliefs. Electronic Commerce Research and Applications, Vol. 13, No. 32, pp. 32-44.

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, Vol. 15, No. 4, pp. 336–355.

Malhotra, N.K. Pesquisa de Marketing: Uma Orientação Aplicada. Porto Alegre: Bookman, 2006.

Menard, P., & Bott, G. J. (2020). Analyzing IoT Users' Mobile Device Privacy Concerns: Extracting Privacy Permissions Using a Disclosure Experiment. Computers & Security, 101856.

Ministério da Ciência, Tecnologia e Inovações. (2019) Estratégis digital. Avaliable: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf

Mitchell, S. S. D. (20189) ""Warning! You're entering a sick zone": The construction of risk and privacy implications of disease tracking apps", *Online Information Review*, October, 1468-4527. DOI 10.1108/OIR-03-2018-0075

Mylonas, A. Kastania, A. and Gritzalis, D. (2013) Delegate the smartphone user? Security awareness in smartphone platforms. Computers &and Security, Vol. 34, pp. 47-66.

Petronio, S. (2002) Boundaries of Privacy: Dialectics of Disclosure. Albany: State University of New York Press.

Punch, K. F. (2005) Introduction to Social Research: Quantitative and Qualitative Approaches. Thousand Oaks, California: Sage.

Smith, H. J. Dinev, T. and Xu, H. (2011) Information privacy research: An interdisciplinary review. MIS Quarterly, Vol. 35, No. 4, pp. 989-1015.

Smith, H.J. Milberg, S.J. and Burke, S. J. (1996) Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly, Vol. 20, No. 2, pp. 167-196.

Stewart, K.A. and Segars, A.H. (2002) An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research, Vol. 13, No. 1, pp. 36–49

Stone, E. F. Gardner, D. G. Gueutal, H. G. and Mcclure, S. (1983) A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. Journal of Applied Psychology, Vol. 68, No. 3, pp. 459-468.

Sutanto, J. Palme, E. Tan, C.-H. and Phang, C.W. (2013) Addressing the personalization–privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quarterly, Vol. 37, No. 4, pp. 1141-1164.

Tversky, A. and Kahneman, D. (1981) The framing of decisions and the psychology of choice. Science, Vol. 211, pp. 453-458, 1981.

Tversky, A.; Kahneman, D. (1986) Rational Choice and the Framing of Decisions. The Journal of Business, Vol. 59, No. 4, Part 2: The Behavioral Foundations of Economic Theory, pp. S251-S278.

Tversky, A.; Kahneman, D. P. (1974) Judgment under uncertainty: heuristics and biases. Science, Vol. 185, No. 4157, pp. 1124-1131.

Verena M. Wottrich, V. W. Van Reijmersdal, E. A. Smit, E. G. (2018) The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems. 106, 44-52, https://doi.org/10.1016/j.dss.2017.12.003

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. International journal of information management, 36(4), 531-542.

Westin, A.F. (1967) Privacy and Freedom. New York: Atheneum, 1967.

Westin, A.F. (2003) Social and political dimensions of privacy. Journal of Social Issues, Vol. 59, No. 2, pp. 431–453.

Winer, R.S. (1999) Experimentation in the 21st century: The importance of external validity. Journal of the Academy of Marketing Science, Vol. 27, No. 3, pp. 349-358.

Xu, H. and Teo, H.H. (2004) Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective. Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004), (pp. 793-806). Washington, D. C., United States.

Xu, H. Gupta, S. Rosson, M. B. and Carroll, J. M. (2012) Measuring Mobile Users' Concerns for Information Privacy. Thirty Third International Conference on Information Systems (ICIS). Orlando.

ANNEX – FACTORIAL ANALYSIS OF THE SCALES

MUIPC – Exploratory Factor Analysis (pre-test)

Factor	Variable	Communality	Factor load	Cronbach's Alpha	Cronbach's Alpha 8 items	.912
Perceived Surveillance	**PS 2**	.829	.659	.839	*KMO*	.917
	PS 3	.904	.857		*x^2*	1434.749
Perceived Intrusion	**PI 1**	.778	.777	.806	*Df.*	28
	PI 2	.737	.741		*Sig.*	.000
	PI 3	.720	.764		*Variance Explained*	78.252
Secondary use of Personal Information	**SU 1**	.784	.791	.852		
	SU 2	.731	.737			
	SU 3	.778	.806			

FIDPI - Exploratory Factor Analysis (pre-test and construct validation)

Factor	Variable	Communality	Factor load	Cronbach's Alpha 5 items	.869
Future Intention to Disclose Personal Information	**FI 1**	.595	.772	*KMO*	.784
	FI 2	.637	.798	*x^2*	864.562
	FI 3	.599	.774	*Df.*	10
	FI 4	.720	.848	*Sig.*	.000
	FI 5	.736	.858	*Variance Explained*	65.725

Future Intention to Disclose Personal Information	**FI 1**	From now on, I will only install apps after carefully reading all the types of permissions to access my personal information requested by the developer company
	FI 2	I will stop giving app developer companies access to my personal information, even though the apps interest me a lot
	FI 3	I will install apps only after reading the online privacy policy and know and agree about how the developer will use my personal information
	FI 4	I will no longer use apps on my mobile device if they require access to my personal information, even though the apps interest me a lot
	FI 5	I will uninstall apps from my mobile device if they require access to my personal information, even though the apps interest me a lot