VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v9i1.4316

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

ANALYSIS OF EFFECTS OF APP PERMISSION CONCERNS ON INTENTIONS TO DISCLOSE PERSONAL INFORMATION: A CASE STUDY OF MONEY TRANSFER SERVICE APP

Azis Amirulbahar[1*]; Yova Ruldeviyani[2]

Faculty of Computer Science[1,2]
Universitas Indonesia
http://ui.ac.id
azis.amirulbahar@ui.ac.id[1*]; yova@cs.ui.ac.id[2]

(*) Corresponding Author

Abstract— *Data growth increased alongside the rise of mobile app users in financial services. In Indonesia, the number of financial services application downloads reached 24 million by the end of 2022, with a 28.72 percent increase in transactions. However, this growth also brings issues regarding the potential misuse of personal information, although according to the Personal Data Protection Act (UU PDP) in Indonesia, personal data is protected and kept confidential when accessed by another party. This prompts users to be more cautious in disclosing personal information. On the other hand, users are faced with risks to personal data that can be accessed by service providers, one of which is through app permissions. This research focuses on the influence of App Permission Concerns on users' intentions to disclose their personal information, with a case study of a money transfer services app in Indonesia, namely Flip, that received numerous negative reviews about users' data privacy concerns, especially when verifying using an identity card. The study uses a quantitative approach with PLS-SEM for data analysis. Convenience sampling was used, and data were collected via a questionnaire distributed through Google Forms on social media from May 9 to May 21, 2023 and a total of 224 respondents were obtained. The results of this study indicate that App Permission Concerns have a significant influence on Privacy Fatigue, Privacy Awareness, Privacy Concern and Trust. Trust significantly influences Intention to Disclose. This research is expected to contribute to future studies on app permissions and mobile app feature development.*

Keywords: *app permission concerns; application; personal data; mobile; intention to disclose;*

Intisari— *Pertumbuhan data mengalami peningkatan seiring dengan pertumbuhan pengguna aplikasi mobile layanan keuangan. Jumlah unduhan aplikasi layanan keuangan di Indonesia pada tahun 2022 mencapai 24 juta dengan peningkatan jumlah transaksi sebesar 28,72 persen. Namun pertumbuhan tersebut menimbulkan permasalahan terkait informasi pribadi yang berpotensi disalahgunakan, sedangkan berdasarkan Undang - Undang Perlindungan Data Pribadi (UU PDP), pihak lain wajib menjaga kerahasiaan data pribadi serta mencegah akses yang tidak sah. Hal tersebut memicu pengguna untuk lebih waspada dalam mengungkapkan informasi pribadinya. Di sisi lain, pengguna dihadapkan dengan risiko data pribadi yang dapat diakses penyedia layanan, salah satunya melalui app permissions. Penelitian ini berfokus pada pengaruh App Permission Concerns terhadap niat pengguna untuk mengungkapkan informasi pribadinya, dengan studi kasus aplikasi mobile layanan transfer uang di Indonesia yaitu Flip, yang terdapat banyak ulasan negatif pengguna mengenai kekhawatiran terhadap data pribadi, khususnya saat verifikasi kartu identitas. Penelitian ini menggunakan metode kuantitatif dengan teknik analisis data menggunakan PLS-SEM (Partial Least Square – Structural Equation Modelling). Teknik pengambilan sampel menggunakan convenience sampling dengan kriteria responden pengguna aplikasi Flip. Proses penghimpunan data melalui kuesioner yang disebarkan dengan Google Form melalui media sosial sejak 9 Mei 2023 hingga 21 Mei 2023 dan diperoleh 224 responden. Hasil penelitian menunjukkan bahwa App Permission Concerns memiliki pengaruh yang signifikan terhadap Privacy Fatigue, Privacy Awareness, Privacy Concern, serta Trust. Trust memiliki pengaruh signifikan terhadap Intention to Disclose. Penelitian ini diharapkan dapat berkontribusi mengenai konsep app permission terkait akses data pengguna di perangkat pada penelitian selanjutnya maupun dalam rangka pengembangan fitur aplikasi mobile bagi para pengembang aplikasi.*

Kata Kunci: *aplikasi; app permission concerns; data pribadi; mobile; pengungkapan informasi pribadi;*

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4316

INTRODUCTION

Data owned by companies and governments continue to increase. Likewise, access to user data is directly proportional to this growth. On the other hand, the designation of data management must be transparent. The larger an organization in terms of data ownership, the greater the potential for data-related risks. Not all organizations have consumer data protection procedures in place or how to prevent them in the event of a data leak. So that the existence of rules/policies related to data management is a competitive advantage of a company. Users will prefer service providers who prioritize personal data protection and who manage it well [1]. Because competitive advantage is not only related to achieving high product sales or market share, but also related to the protection of personal data [2].

In the field of financial services, data is also a concern for users when using mobile-based services, due to financial activities carried out on mobile applications being related to sensitive personal data as well as financial data [3]. Indonesia in 2020, has the highest ranking on Association of Southeast Asian Nation (ASEAN) on the number of mobile based banking services users', it has growth 44% than previous year [4]. The number of downloads for financial services applications reached 24 million by the end of 2022 [5]. When viewed from the transaction figures, the transaction value in 2022 reached Rp52.545.8 trillion or increased by 28.72 percent [6]. The increase in the number is influenced by the presence of a pandemic that has caused a shift from offline to online to fulfill financial service needs [7]. The use of financial service applications through mobile apps will ease customers in fulfilling all of their transactional needs rather than having to go to ATMs or physical branches [8].

Increasing features in mobile apps is inseparable from requests regarding user information which is sometimes irrelevant to app functions or unofficial (illegal) which makes it difficult for users to protect their personal data and will undermine consumer trust. An app will usually ask the user to allow access to personal information and will potentially pose risks related to personal data [9]. Users are also reluctant to install or immediately uninstall the app if there are issues related to data privacy [10]. According to the Information and Electronic Transactions Law of 2008 (ITE Law), protected personal data from various forms of disturbance, such as unauthorized usage or interventions, is an individual's right [11].

The personal data required by service providers in the digital era demands users to surrender their personal information, making it challenging for users to easily maintain control over their personal data stored with the service providers [12]. Cases of misuse of personal data such as fraud and the like will also lead to a decline in users' trust in online-based services. If such data is disclosed to unauthorized parties, it can be exploited and result in financial losses, and even jeopardize the safety and security of the data owners. Common forms of data misuse include telemarketing activities that leverage data stored by service providers without prior user consent. Users are offered insurance products or unsecured loans, sometimes even requesting data from other family members. However, every piece of information conveyed through electronic media related to personal data must be done with the concerned individual's consent [12].

Sirait (2019) in [13] explains that personal data is any form of information that can define an individual, such as identification numbers, telephone numbers, names, physical conditions, economic status, and so on. Personal data is information that must be kept confidential and accurate [13]. In Indonesia, the protection of personal data is currently regulated by the Personal Data Protection Act (UU PDP), which was enacted in 2022. One of the regulations within it pertains to the collection, storage, and use of personal data conducted by companies or service providers. Personal data is information that must be kept confidential and protected for purposes that are legitimate [14].

However, with the existence of the Personal Data Protection Act (PDP) [in Indonesia], it has not been able to address cases of personal data leaks and misuse. Such as the case experienced by Tokopedia in 2021, which is estimated to have affected 91 user accounts and 7 million merchant accounts, being sold illegally for $5,000 and resulting in lawsuits amounting to 100 billion rupiah. Another significant case is the leakage incident that befell the Social Security Agency on Health (BPJS), causing losses to the country of up to 600 trillion rupiah [15]. Data leaks have also occurred in banking services, namely at Bank Rakyat Indonesia (BRI) regarding the "BRI Life" product [11].

Until early 2022, Indonesia is among the top 10 countries with the highest number of data breaches [11]. Cases related to data leaks or data misuse can occur due to factors from both the security of the service provider and human factors, namely the users who lack awareness about the security of personal data. The forms of abuse occurring in financial services are the theft of customers' personal data, PIN, payment card number, and password [16].

One of the most popular mobile apps in the financial services sector is Flip. Flip is a financial

services app whose main feature is free transfers to other banks managed by PT Fliptech Lentera Inspirasi Pertiwi [17]. Customers who send account balances to other banks will first be accommodated in Flip accounts, then the system will forward them to the destination account [18]. The current number of Flip app users has reached more than 12 million [19]. Flip cooperates with various parties in doing business. These parties include banks, payment gateways and other third parties who have roles for operations and product development [20]. The collaboration also carries out the process of sharing personal data with third parties [21]. Flip has uncovered several criminal cases through its mobile app. One of them is the case of online loan offer fraud, in which the perpetrator pretends to be Flip's customer service by contacting the user and then being asked to send an identity in the form of a photo ID card, savings book, and other identities. Then the perpetrator asked to send some money through the Flip app [22].

The researcher also observed user reviews on "Google Play Store" for Flip apps, which contained comments expressing concerns about the identity verification process using an identity card (KTP). Despite being downloaded more than 10 million times and installed by most Flip users, the Flip apps received an overall rating of 4.4 from approximately 461 thousand reviews. Many 1-2 star reviews on Google Play Store express concern about potential misuse of personal data when users are asked to disclose their identity through the camera and gallery for verification. In comparison, the iOS version of the app has a higher rating of 4.8 from approximately 61.5 thousand reviews during the research, but the researchers couldn't view the number of downloaders and the overall number of reviews, so in this research, we conducted that we would use reviews on Google Play only [23].

Gu et al. (2017) in [9] stated that considerations related to data privacy are an important factor for potential users to download apps on the applications store. If the privacy data is sensitive, then the user will consider it more than the popularity of the app. However, When users have control over the data shared with the application provider, they will have the confidence or trust to share their data through app permissions [24] .

The mobile app has an app access permission facility for user data and is one of the facilities for controlling the disclosure of user personal information via a smartphone. These access permissions can be in the form of location, gallery, or user contacts [10]. Permission to access this data can affect a person's intention to disclose his personal data and affect the use of the app, because the app will ask the user to allow access or modification of data on the user's device so that there are risks related to personal data [9]. The access permission also plays a role in protecting users to prevent the process of transferring sensitive data that is unknown or unnoticed [25].

Based on these descriptions, this research will analyze the app permission concern factors that can influence a user's intention to disclose personal information by conducting a case study of the Flip money transfer service app. This research contributes to the theory regarding app permission concerns in an awareness perspective regarding the disclosure of one's personal information, especially in the field of banking/finance apps. As well as on the app development aspect, so that the development team can release its product features by considering the presentation of provisions regarding the use of personal information that are more attractive and understandable to users.

MATERIALS AND METHODS

The materials and methods section will explain the research planning process in the form of research design, the instruments used, as well as data collection and processing techniques.

A. Research Design

This research is exploratory research. According to [26] exploratory research involves conducting studies or testing cases that have not been extensively explored in previous research or are still under theoretical development. Exploratory research is suitable for using analytical techniques with Partial Least Square – Structural Equation Modeling (PLS-SEM). Therefore, this study uses PLS-SEM in carrying out the analysis process, with the help of SMARTPLS version 4 software. This research will use 6 construct variables. The selection of these variables is based on previous studies on personal data that are related to user control. User control in this research is defined as app permission. Table 1 is a list of variables along with their sources from previous research that will form the basis for the hypotheses in this study.

Table 1. Variables that were adopted for this research

No	Variable	References
1	App Permission Concern (APC)	[10]
2	Privacy Awareness (PA)	[27]
3	Privacy Fatigue (PF)	[9], [28]
4	Privacy Concern (PC)	[9]
5	Trust (TR)	[27]
6	Intention to Disclose (ID)	[9], [10]

Here are the definitions of the research variables:

1. App Permission Concerns (APC): The user's concerns when faced with granting access to personal data in an application [10].

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4316

2. Privacy Awareness (PA): the awareness of a user regarding a privacy statement on a service provider [27].
3. Privacy Fatigue (PF): The feeling of losing control or being tired/bored when the user cannot control their personal data [9], [28].
4. Privacy Concern (PC): The feeling of worry or concern that arises in users when they are faced with issues related to their personal data that could potentially be misused [28].
5. Trust (TR): Moorman, Zaltman & Deshpande (1992) in [2] described trust as the willingness to rely on a party to perform a particular action due to the belief that the party can be trusted.
6. Intention to Disclose (ID): User's willingness to reveal their personal data [9], [10].

In light of these studies, the researcher then formulates the following hypotheses:

1. H1. App Permissions Concerns (APC) affects Privacy Fatigue (PF).
2. H2. App Permissions Concerns (APC) affects Privacy Awareness (PA).
3. H3. App Permission Concerns (APC) affects Trust (TR).
4. H4. App Permission Concerns (APC) affects Privacy Concern (PC).
5. H5. Privacy Fatigue (PF) affects Intention to Disclose (ID).
6. H6. Privacy Awareness (PA) affects Trust (TR).
7. H7. Privacy Awareness (PA) affects Intention to Disclose (ID).
8. H8. Privacy Concern (PC) affects Intention to Disclose (ID).
9. H9. Trust (TR) affects Privacy Concern (PC).
10. H10. Trust (TR) affects Intention to Disclose (ID).

The relationship between variables is shown in figure 1.

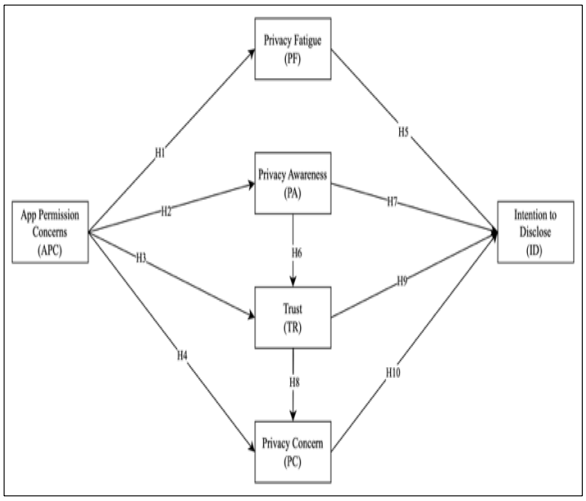

Figure 1. Research Hypothesis

B. Research Instruments

The research instrument that will be used is a questionnaire containing statements from each indicator using a 1-5 Likert scale, ranging from "strongly disagree" to "strongly agree". In addition to these responses, there are questions about the demographic data of the users. The user demographic data includes age range, occupation, gender, province, city of residence, and education level. Besides personal data, there are also questions related to the usage of the Flip application, such as frequency of usage, features used, and knowledge about the personal data that sent to the Flip application, which can be used as a synthesis for recommendations in the conclusion section. The questionnaire will be distributed online through Google Forms on social media platforms such as WhatsApp groups, Instagram, Twitter, and Facebook, targeting active Flip application users as respondents.

In this study, the number of indicators for each construct variable is 4 indicators, except for the Privacy Fatigue (PF) variable, which has 3 indicators. Table 2 is a list of variables and indicators used in the research questionnaire.

Table 2. Variable and Indicators

Variable	Indicators	Sources
App Permission Concern (APC)	APC1: I'm worried that the app provider will collect my personal data without my consent. APC2: I'm concerned that the data stored in the app will be misused for other purposes. APC3: I'm worried that the data I store in the app may be leaked. APC4: I am concerned that the app provider will not be held responsible if my data is misused.	[10]
Privacy Awareness (PA)	PA1: I am aware that the app provider will store my personal data PA2: I am aware that the app provider will access my personal data. PA3: I am aware of the purposes for which the app provider collects my personal data. PA4: I am aware of the app provider's limitations on accessing my personal data.	[27]
***Privacy Fatigue* (PF)**	PF1: I feel uncomfortable when dealing with requests for personal information or when providing personal information. PF2: Giving consent to personal data access in apps is frustrating for me.	[9], [28]

***Privacy Concern* (PC)**	PF3: I'm bored/tired by the issue of personal data on apps. PC1: I'm worried that the app provider will collect my personal data without my consent. PC2: I'm worried that the data stored in the app will be misused for other purposes. PC3: I'm worried that the data I save in the app may be leaked. PC4: I'm worried that the app provider won't be held responsible if my data is misused.	[9]
Trust (TR)	TR1: I trust that Flip will protect my personal data. TR2: I trust that Flip will not misuse my personal data. TR3: I trust that Flip will be transparent in the event of an incident/case involving personal data. TR4: I believe that Flip has a robust security system to protect personal data.	[27]
Intention to Disclose (DI)	ID1: At this time, I will still disclose my personal data on the app. ID2: If there is a change in my identity, I will immediately make changes to the data in the application. ID3: In the future, I will still disclose my personal data on the app. ID4: I will always agree to all privacy policies.	[9], [10]

C. Data collection Technique

The data collection technique used was a questionnaire that was shared online through social media, namely WhatsApp, Instagram, Twitter, and Facebook groups with the target respondents being active users of the Flip app, with convenience sampling. The respondent data that has been collected was analyzed using PLS-SEM (Partial Least Square – Structural Equational Modeling) through SMARTPLS 4 software.

RESULTS AND DISCUSSION

A. Demographic Analysis

The distribution of the questionnaire that was carried out from May 9, 2023 to May 21, 2023, obtained 224 respondents who used Flip, of which 77 were male and 147 were female. In terms of the age group of the respondents, it was found that the majority of respondents were in the age group of 26-35 years with the majority of jobs being private employees. The majority of respondents live in the West Java region. The education level of the respondents was dominated by high school and bachelor graduates. The demographic characteristics of the respondents are shown in table 3.

Table 3. Demographic of Respondents

Variable	Demographic Analysis		
	Answer Group	Total	%
Gender	Male	147	65.6%
	Female	77	34.4%
Age Group	17-25 years old	87	38.8%
	26-35 years old	109	48.7%
	36-45 years old	26	11.6%
Occupation	46-55 years old	2	0.9%
	Private Sector employee	56	25%
	Student/College Student	46	20.5%
	Housewife	36	16.1%
	Civil Servant	13	5.8%
	Entrepreneur	13	5.8%
	Others	60	26.8%
Province of Domicile	West Java	61	27.2%
	Central Java	40	17.9%
	Special Capital Region of Jakarta	31	13.8%
	East Java	29	12.9%
	Special Region of Yogyakarta	20	8.9%
	Others	43	19.3%
Latest Education	Undergraduates	103	46%
	Senior High School	104	46.4%
	Magister	14	6.3%
	Junior High School	3	1.3%

B. App Usage Analysis

The data obtained indicates that the majority of respondents know that personal data input into the application can be accessed by application providers by 79.9% or as many as 179 respondents. Respondents who know that their data is accessed by third parties is 50.9% or as many as 114 respondents. The majority of respondents use the Android OS. The most frequent use of the Flip app is once every 2-3 days with the most used feature being the money transfer feature, which is the app's primary feature.

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4316

With regard to data sent by users on the app, 79.9% or as many as 179 respondents knew that the data they sent could be accessed by the application provider. When users answered questions regarding their knowledge that their data could be accessed by third parties, almost half of the respondents stated that they do not know if their data can be accessed by third parties, namely 50.9% of the total respondents.

During the registration process, 65.2% of respondents or 146 respondents stated that they had read the contents of the privacy policy first. There were 34.8% or 78 respondents who stated that they had not studied the content of the privacy policy beforehand, therefore the researchers confirmed it by sampling 32 users who stated they had not read it first.

Most of them stated that they were reluctant to read the privacy policy content because they felt the privacy policy text was too long and felt that reading the privacy policy content was not important. This is of course contrary to the content of the privacy policy which encourages users to understand the content of the privacy policy to avoid losses in the future. The usage statistic at Flip features is shown at table 4.

Table 4 . Usage Statistics of the Flip Application

Question	*Answer Group*	*Total*	*%*
Operating system used	Android	197	87.9%
	iOS	15	6.7%
	Both	12	5.4%
Frequency of Using the Flip app	2-3 times a day	65	29%
	Once a few weeks	54	24.1%
	Once a week	37	16.5%
	Daily	34	15.2%
	Once a few months	20	8.9%
	Once a month	14	6.3%
Frequently used features	Transfer	160	71.4%
	E-wallet	43	19.2%
	Top-Up & Billing	20	8.9%
	Flip Globe	1	0.4%
User's knowledge that user-submitted data is accessible by the app provider	Yes	179	79.9%
	No	23	10.3%
	Uncertain	22	9.8%
User's knowledge that personal data may be accessed by third parties	Yes	114	50.9%
	No	77	34.4%
	Uncertain	33	14.7%
Do users first read the contents of the privacy policy	Yes	146	65.2%
	No	78	34.8%

C. Model Analysis

The first step in PLS-SEM analysis is the evaluation of the outer model [29]. In the SMART-PLS app, this process is carried out by selecting the calculate PLS algorithm menu. The PLS algorithm is a process for measuring the structural model [26]. From the results of the PLS algorithm, results are obtained as shown in figure 2.

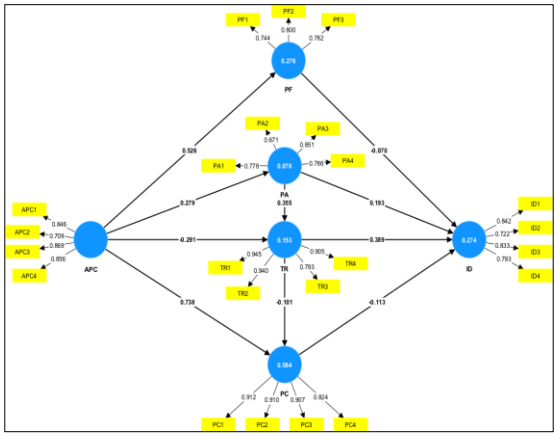

Figure 2. Structural model calculation results

Figure 2 shows the results of the outer loading values for each indicator (in yellow) and the value of Composite Reliability (CR) in blue. According to [26] the Outer Loading value for exploratory research is >0.60.

The next process for evaluating the outer model is observing the Composite Reliability (CR) and Average Variance Extracted (AVE). The CR value in exploratory research is in the range of 0.60 to 0.70. CR values > 0.70 are recommended values, while AVE values are > 0.50 [26]. Table 5 shows the results related to Outer Loading, CR, and AVE measurements. In table 5, the results show that each construct has a value of Outer Loading>60, CR> 0.70, and AVE> 0.50, so in this study all variables meet the criteria.

Table 5. Outer Loading, CR, and AVE Measurement Results

Variable	Indicator	Outer Loading	CR	AVE
APC	APC1	0.846	0.893	0.677
	APC2	0.709		

Variable	Indicator	Outer Loading	CR	AVE
ID	APC3	0.869	0.876	0.638
	APC4	0.856		
	ID1	0.842		
	ID2	0.722		
	ID3	0.833		
	ID4	0.793		
PA	PA1	0.778	0.856	0.599
	PA2	0.671		
	PA3	0.851		
	PA4	0.786		
PC	PC1	0.912	0.938	0.790
	PC2	0.910		
	PC3	0.907		
	PC4	0.824		
PF	PF1	0.744	0.819	0.602
	PF2	0.800		
	PF3	0.782		
TR	TR1	0.945	0.943	0.806
	TR2	0.940		
	TR3	0.793		
	TR4	0.905		

The next step according to [26] is to calculate discriminant validity. Discriminant validity can be measured by heterotraits-monotraits (HTMT). According to Hensler et. al (2015) in [26], the criterion value for HTMT is less than 0.90. Table 4 shows that the HTMT value does not exceed 0.90 which makes it meet the validity criteria. The result of discriminant validity is shown at table 6.

Table 6. Discriminants Validity Results

	APC	ID	PA	APC	PF	TR
APC						
ID	0.201					
PA	0.356	0.332				
PC	0.846	0.231	0.319			
PF	0.676	0.255	0.265	0.881		
TR	0.218	0.537	0.344	0.259	0.249	

After evaluating discriminant validity, according to [26] is to evaluate the structural model by looking at the value of R^2, R^2 is used to measure the explanatory power in each endogenous variable. This process is in the form of measurements related to the level and significance of the path. Chin (1998) in [29] argues that the criteria for R^2 values are as follows: 0.19 (weak), 0.33 (moderate), and 0.67 (strong). From the results of the calculation of R^2 contained in table 7, the PC (Privacy Concern) value is included in the moderate criteria, it is mean that PC has 57.3% to affect endogenous variables (intention to disclose). While the other constructs have weak values.

Table 7. R^2 Measurement Result

Variable	R-Square	R-Square Adjusted
ID	0.274	0.235
PA	0.078	0.066
PC	0.584	0.573
PF	0.276	0.267
TR	0.153	0.131

The last process is hypothesis testing by looking at the results of the relationship between variables, namely inner model/structural model evaluation [29]. Testing was carried out using a two-tailed test. According to [29], two-tailed testing is carried out when a hypothesis is not yet known and does not have a strong theoretical basis in previous research. The value of the relationship between variables according to [30] is 1.645 on T-values with a significance of 10%, 1.960 on T-values with a significance of 5%, or 2.576 on T-values with a significance of 1%. The results of hypothesis testing are shown in table 8.

Table 8. Hypothesis Result

Hypo-thesis	Original Sample (O)	T Statistics	P Values	Results
H1 : APC→PF	0.526	6.904	0.000	**Accepted**
H2 : APC→PA	0.279	1.717	0.086	**Accepted**
H3 : APC→TR	-0.291	3.012	0.003	**Accepted**
H4: APC→PC	0.738	15.378	0.000	**Accepted**
H5 : PF→ID	-0.070	0.410	0.682	Rejected
H6 : PA→TR	0.355	2.563	0.010	**Accepted**
H7 : PA→ID	0.193	1.405	0.160	Rejected
H8 : TR→PC	-0.101	1.658	0.097	**Accepted**
H9 : TR→ID	0.389	3.817	0.000	**Accepted**
H10 : PC→ID	-0.113	0.804	0.422	Rejected

Based on the results presented in Table 6, the construct variable App Permission Concerns (APC) and its corresponding hypotheses, namely H1 (APC → PF), H2 (APC → PA), H3 (APC → TR), and H4 (APC → PC), each show a significant effect (accepted) on the variables of privacy fatigue, privacy awareness, trust, and privacy concerns.

Worries about control can lead to privacy fatigue. When the user does not pay attention to the access permission question, there is the potential for someone's personal information to be accessed by the application, this will make someone feel

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4316

powerless over the data stored on their smartphone, that proved at H1 (APC→PF). This is relevant to previous research conducted by [28] regarding the concept of privacy fatigue which is motivated by the inability of users to control access to personal information.

H2 (APC→PA) proves that privacy awareness is driven by the user's exercise of control significantly. Users with control over access to personal information that will be sent to a service provider means that they have awareness regarding privacy. This is relevant to research conducted by [27]. User awareness also has a significant positive effect on trust, as evidenced by H6 (PA→TR). Users who have awareness of the use of personal data, they will also have confidence regarding the use and management of their data.

When someone is on guard in allowing access to sensitive data, they will tend not to fully trust a service, users have considerations related to the security aspects of their personal information so that when concern increases, the level of trust will be inversely proportional to H3 (APC→TR), which has negative influence significantly. This reinforces previous research conducted by [24] that the control aspect in terms of this research is access permission, which will affect trust in a service. H4 (APC→PC) proves that access permissions also have a significant influence on users' concerns about their personal data, when users have high concerns about access permissions, concerns about privacy will also increase.

However, when user trust is high, the user's concern for personal data will decrease as shown by H8 (TR→PC) which has significant results with a negative effect between trust and privacy concerns. With this increased trust, a person will voluntarily disclose his personal data to service providers as contained in H9 (TR→ID) which has positive significant results.

CONCLUSION

This study aims to determine the effect of the App Permission Concerns (APC) factor on mobile-based financial service applications on users' intentions to disclose their personal information. The results showed that APC has a significant effect on privacy fatigue, privacy awareness, trust and privacy concern. So that the access permission factor needs to be considered from the side of research/academicians and practitioners related to the factor of disclosing personal data, because access permission is one of the controls for disclosing personal data when using mobile applications to be able to access that provided by users. App access permissions are a factor in determining the user's level of trust in service providers and can also increase awareness about disclosing personal data, when the user has doubts when an order appears to perform access permission, the user lacks confidence in disclosing his personal information. With this lack of trust, there will be losses for app providers in the form of negative perceptions about data security so that apps become less attractive to users and can potentially move to competitors who might provide more security.

Correlated with questions about user knowledge regarding the content of privacy policies, many users do not pay attention to the content of privacy policies because they find them lengthy or unimportant, or they are aware that their data can be accessed by app provider and third parties. App developers and data protection parties need to innovate privacy policy content with attractive visuals during registration and permission requests. This will encourage users to read carefully and understand their rights and responsibilities. By doing so, users will maintain trust in using the Flip app and feel more comfortable disclosing personal data for application usage. Utilization of features such as push notifications or via official social media accounts that contain messages regarding the protection of personal data and its use also needs to be done. This is to provide an understanding to users regarding the management of personal data. This message can be conveyed briefly but easy to understand, so users will be more interested in reading it. Messages that are too long will discourage users from being as interested as when they are asked to comprehend the contents of the privacy policy.

ACKNOWLEDGEMENT

Thank you to the Ministry of Communication and Information of the Republic of Indonesia for supporting this research through the “Beasiswa Kominfo Dalam Negeri 2021”.

REFERENCE

[1] E. Janiszewska-Kiewra, J. Podlesny, and H. Soller, ‘Ethical data usage in an era of digital technology and regulation’, 2022.

[2] A. Bleier, A. Goldfarb, and C. Tucker, ‘Consumer privacy and the future of data-based innovation and marketing’, *International Journal of Research in Marketing*, vol. 37, no. 3, pp. 466–480, 2020, doi: 10.1016/j.ijresmar.2020.03.006.

[3] E. Dzidzah, K. Owusu Kwateng, and B. K. Asante, 'Security behaviour of mobile financial service users', *Information and Computer Security*, vol. 28, no. 5, pp. 719–741, 2020, doi: 10.1108/ICS-02-2020-0021.

[4] R. A. Rahmi and P. W. Handayani, 'The influence of users' perspective factors on mobile banking adoption in Indonesia', *Journal of Science and Technology Policy Management*, 2023, doi: 10.1108/JSTPM-01-2022-0008.

[5] Statista, 'Number of downloads of finance mobile apps in Indonesia from 1st quarter 2019 to 4th quarter 2022 (in millions), by category', 2023. https://www.statista.com/statistics/1333919/indonesia-finance-apps-downloads/ (accessed Aug. 03, 2023).

[6] Portal Informasi Indonesia, 'Transaksi Uang Elektronik Melejit', 2023. https://www.indonesia.go.id/kategori/indonesia-dalam-angka/6855/transaksi-uang-elektronik-melejit (accessed Aug. 03, 2023).

[7] B. Andrian, T. Simanungkalit, I. Budi, and A. F. Wicaksono, 'Sentiment Analysis on Customer Satisfaction of Digital Banking in Indonesia', *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, pp. 466–473, 2022, doi: 10.14569/IJACSA.2022.0130356.

[8] D. I. Inan *et al.*, 'Service quality and self-determination theory towards continuance usage intention of mobile banking', *Journal of Science and Technology Policy Management*, vol. 14, no. 2, pp. 303–328, 2023, doi: 10.1108/JSTPM-01-2021-0005.

[9] J. Tang, U. Akram, and W. Shi, 'Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits', *Journal of Enterprise Information Management*, vol. 34, no. 4, pp. 1097–1120, 2020, doi: 10.1108/JEIM-03-2020-0088.

[10] K. Degirmenci, 'Mobile users' information privacy concerns and the role of app permission requests', *Int J Inf Manage*, vol. 50, no. April 2019, pp. 261–272, 2020, doi: 10.1016/j.ijinfomgt.2019.05.010.

[11] K. R. Ramadhan and C. Wijaya, 'The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia', *Technium Social Sciences Journal*, vol. 36, pp. 18–28, Oct. 2022, doi: 10.47577/tssj.v36i1.7442.

[12] S. Dewi Rosadi and G. Gumelar Pratama, 'URGENSI PERLINDUNGAN DATA PRIVASIDALAM ERA EKONOMI DIGITAL DI INDONESIA', *Veritas et Justitia*, vol. 4, no. 1, pp. 88–110, Jun. 2018, doi: 10.25123/vej.2916.

[13] E. S. Hasibuan and L. Salsiah, 'Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia', *Jurnal Pro Hukum: Jurnal Penelitian Bidang Hukum*, vol. 11, no. 3, pp. 63–69, 2022.

[14] A. F. Sutarli, F. Hukum, and U. K. Maranatha, 'Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia', vol. 3, pp. 4208–4221, 2023.

[15] H. B. Setiawan and F. U. Najicha, 'Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data', *Jurnal Kewarganegaraan*, vol. 6, no. 1, pp. 976–982, 2022.

[16] B. Kotkova and M. Hromada, 'Cyber Security and Social Engineering', *Proceedings - 25th International Conference on Circuits, Systems, Communications and Computers, CSCC 2021*, pp. 134–140, 2021, doi: 10.1109/CSCC53858.2021.00031.

[17] rezki dwy putra, 'analisis kepuasan pengguna aplikasi flip.id menggunakan metode TAM dan EUCS', *Journal of Emerging Information Systems and Business Intelligence (JEISBI)*, vol. 2, no. 4, p. 4, 2021.

[18] Flip.id, 'Bagaimana cara kerja Flip?', 2023. https://support.flip.id/hc/id/articles/4406771893657-Bagaimana-cara-kerja-Flip- (accessed May 05, 2023).

[19] Mediaindonesia.com, 'Pengguna Flip Tahun Ketujuh Tembus 12,8 Juta', 2023. https://mediaindonesia.com/ekonomi/549267/pengguna-flip-tahun-ketujuh-tembus-128-juta

[20] Flip.id, 'Syarat dan Ketentuan', 2023. https://flip.id/syarat-dan-ketentuan (accessed May 05, 2023).

[21] Flip.id, 'Kebijakan Privasi', 2023. https://flip.id/kebijakan-privasi (accessed May 05, 2023).

[22] Flip.id, 'Hati-hati Modus Penipuan Mengatasnamakan Flip', 2022. https://flip.id/blog/modus-penipuan-mengatasnamakan-flip (accessed May 28, 2023).

[23] Google Play, 'Flip: Transfer Tanpa Admin', 2023. https://play.google.com/store/apps/details?id=id.flip&hl=id (accessed May 06, 2023).

[24] K. Bessenyei *et al.*, 'Comfortability with the passive collection of smartphone data for monitoring of mental health: An online survey', *Computers in Human Behavior*

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4316

Reports, vol. 4, 2021, doi: 10.1016/j.chbr.2021.100134.

[25] J. Feichtner and S. Gruber, 'Understanding Privacy Awareness in Android App Descriptions Using Deep Learning', *CODASPY 2020 - Proceedings of the 10th ACM Conference on Data and Application Security and Privacy*, pp. 203–214, 2020, doi: 10.1145/3374664.3375730.

[26] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, 'When to use and how to report the results of PLS-SEM', *European Business Review*, vol. 31, no. 1, pp. 2–24, 2019, doi: 10.1108/EBR-11-2018-0203.

[27] J. Sah and S. Jun, 'The Role of Consumers' Privacy Awareness in the Privacy Calculus for IoT Services', *Int J Hum Comput Interact*, vol. 0, no. 0, pp. 1–12, 2023, doi: 10.1080/10447318.2023.2184102.

[28] H. Choi, J. Park, and Y. Jung, 'The role of privacy fatigue in online privacy behavior', *Comput Human Behav*, vol. 81, pp. 42–51, 2018, doi: 10.1016/j.chb.2017.12.001.

[29] P. W. Handayani, *Konsep CB-Sem dan Sem-Pls Disertai Dengan Contoh Kasus - Rajawali Pers*. PT. RajaGrafindo Persada, 2021. [Online]. Available: https://books.google.co.id/books?id=mkwaEAAAQBAJ

[30] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. in Classroom Companion: Business. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-80519-7.