Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 6 (2022) 1014-1020 ISSN Media Electronic: 2580-0760

Measuring the effect of Users' Privacy Concerns on the Use of Jakarta Smart City Mobile Application (JAKI)

[1]Arif Wahyudi, [2]Mirza Triyuna Putra, [3]Dana Indra Sensuse, [4]Sofian Lusa, [5]Prasetyo Adi, [6]Assaf Arief
[1,2,3,4,5,6]Magister of Technology Information, Faculty of Computer Science, Universitas Indonesia
[1]arif.wahyudi11@ui.ac.id, [2]mirza.triyuna@ui.ac.id, [3]dana@cs.ui.ac.id, [4]sofian.lusa@cs.ui.ac.id, [5]prasetyo.adi01@cs.ui.ac.id, [6]assaf.arief@cs.ui.ac.id

Abstract

Jakarta Kini (JAKI) is a super-app developed by Jakarta Smart City that offers a one-stop service to help citizens connect and communicate with the Government. It is undeniable that the use of mobile applications can indeed facilitate people's activities, but on the other hand, it also poses risks and raises concerns in terms of privacy. The purpose of this study is to assess the impact of users' privacy concerns on their tendency to use the JAKI mobile application. To measure the privacy concern, we conduct an online survey of the users of JAKI. The hypothesis and research model were formulated to assess the users' privacy concerns based on the Mobile Users' Information Privacy Concerns (MUIPC) theory, with additional factors, namely prior privacy experience and awareness, as the antecedents. As a result, we found that MUIPC had a significant effect on negatively influencing the intention to use the JAKI application. Our study contributes as a starting point in exploring privacy research in the context of a smart city in Indonesia. Additionally, this study proved that the IPC scales that were originally designed for English-based countries could also be adapted to Bahasa Indonesia and utilized in the Indonesian context.

Keywords: smart city, Jakarta, mobile application, privacy concern

1. Introduction

Jakarta Smart City (JSC) is a Regional Public Service Agency serving the Office of Communication, Information, and Statistics of the Special Capital Region of Jakarta. JSC was formed and inaugurated on December 26, 2014. Following the current Smart City 4.0 development, JSC is trying to transform Jakarta into a smart city by implementing the Smart City 4.0 ecosystem. One of the initiatives is the mobile app named Jakarta Kini. Jakarta Kini, or JAKI, is a super-app developed by Jakarta Smart City and launched on September 27, 2019, and is intended to help residents find their daily needs in Jakarta. JAKI is also a hub for the integration of all services from the Government and the community. Currently, JAKI is integrated with 32 applications by the Jakarta Provincial Government and 11 service applications by external parties, and as of October 2020, JAKI has been used by 849,214 users. Some of JAKI's main features are JakWarta, JakRespons, JakPangan, JakPantau, JakCLM, JakSiaga, and JakAman [1]. In the principle of smart collaboration, JAKI as a one-stop service platform, provides a collaborative ecosystem that fosters a digital ecosystem that collaborates with the Government, the start-up industry, and the community. The system and data-driven principle of JAKI are applied through personalized service to the public through the user's omnichannel experience, which generates a variety of data to be used in making data-based policies.

The implementation of a smart city, which involves various aspects of life and is closely related to data exchange, is certainly inseparable from problems and privacy issues. Based on the results of previous research, problems and privacy issues that tend to occur, are discussed, and feared in smart cities, including those related to mobile applications, include Unsecured data sharing [2][3][4], Massive data collection [2][5][6], Unauthorized access [2][7][8][9][10], and Lack of data protection mechanism [2][9][10][11]. In addition, privacy issues and problems also affect trust and social aspects, including lack of trust from citizens [7][8][11][12], concern about privacy surveillance [11][12], social inequality, and social bias [10][12].

Those various issues related to privacy in a smart city might potentially occur in the operationalization of JAKI, since JAKI needs to collect a number of personal information from users, which some data like personal identification number (NIK), phone number,

Accepted: 28-09-2022 | Received in revised: 13-12-2022 | Published: 29-12-2022

geolocation, and user activity which are considered sensitive. Moreover, JAKI has also requested location permission that could potentially be misused to track the users' behavior. Though the protection of personal data has been guaranteed in their privacy policy, the violation of users' privacy might still occur. One of the cases that ever happened was the identity leak of citizens' data who used JakLapor in JAKI to report the health protocol violation in their neighborhood [13]. The case got massive attention and responses from the public, and some of them claimed to have experienced a similar incident [13].

Many scholars have offered technical and design solutions to overcome the privacy issues in smart cities, yet they still lack to address the citizens' privacy concerns and actual behavior [14]. Citizens' privacy concern is a very crucial aspect to take into account to preserve citizens' support and participation in smart city development [14]. Smart city Governments need to identify which privacy concerns that arise from their technology implementation.

Information Privacy Concern (IPC) can be defined as an individual's perception of the possible loss of privacy when giving information to known or unknown entities and their concern about losing control of personal data [15]. To measure the IPC, many scholars have designed theories and measurement models for determining individual IPC; some of the most comprehensive models were developed by Smith et al. [16], Sheehan and Hoy [17], Malhotra [18], Buchanan et, al. [19], Earp et al. [20], Dinev and Hart [21], and Braunstein et al.[22]. In the modern context of mobile application, Xu et al. [23] developed a model to measure IPC, which focus on measuring the privacy concern of mobile internet users, which is called Mobile Users' Information Privacy Concerns (MUIPC).

MUIPC has been used or adopted to investigate the privacy issues in new technology e.g., mobile applications, the Internet of Things, and wearable technologies. Gu et al. [24] and Geovanny et al. [25] used MUIPC to examine the privacy concern in the case of mobile application download. Degirmenci [26] examined the correlation between mobile app permission requests with privacy concerns and the impact on the users. Foltz et al. [27] and Lopes et al. [28] adopted MUIPC as an instrument to measure privacy concerns in the Internet of Things (IoT) environment. Wiegard et al. [29] combined the UTAUT2, PCT, and MUIPC models to investigate critical success factors of wearable technologies' usage. Guhr et al. [30] adopted MUIPC to examine the privacy concern in the smart home context.

In our study, we utilized MUIPC to assess the impact of users' privacy concerns on their tendency to use the JAKI mobile application. The hypothesis and research model were formulated to assess the users' privacy concerns based on the Mobile Users' Information Privacy Concerns (MUIPC) theory. Different from prior studies, we extend the MUIPC with additional factors, namely prior privacy experience and awareness as the antecedents. The context of this study is also different, in which we focus on measuring the effect of users' privacy concerns on the willingness to use the JAKI mobile application by conducting a survey of the users. This study was motivated to answer the question: "what are the relative impacts of users' privacy concerns on the intention to use JAKI?"

2. Research Methods

The process of our research consists of 8 steps, as illustrated in Figure 1: identification of the research problem, review of relevant literature, develop a research model and hypothesis, design of the research instrument, collecting data, data processing and analysis, results and discussion, and conclusion.

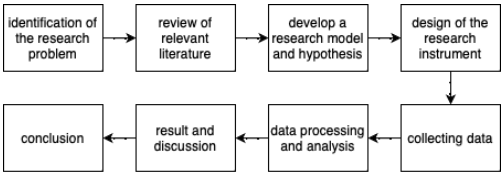

Figure 1. Research process.

2.1 Research Model

To measure the IPC on the use of the JAKI mobile app, we designed the research model based on the MUIPC construct, which is designed as a second-order model that focuses on measuring IPC in the context of mobile users which consists of a 9-item scale and three dimensions, namely perceived surveillance, perceived intrusion, and secondary use of personal information [23]. Furthermore, we also proposed two additional constructs to be the antecedents of MUIPC, namely prior privacy experience and awareness, based on the systematic literature review study from Bartol et al. [15]. From the proposed research model, we examined the impact of MUIPC on the intention to use the JAKI mobile application. Figure 2 depicts the research model for our study.

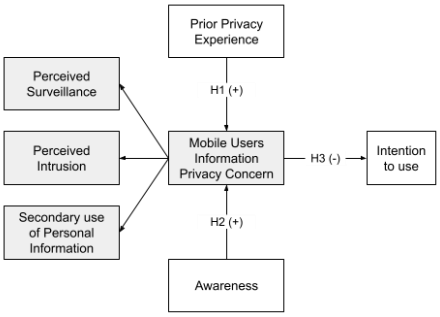

Figure 2. MUIPC (shaded gray) and the proposed research model.

DOI: https://doi.org/10.29207/resti.v6i6.4544

Perceived surveillance refers to the users' concern about being profiled and monitored by the surveillance capabilities of smartphone technology through its various sensors [23]. Perceived intrusion refers to the unwanted invasion of individual activities or routines that can create discomfort and harm to mobile users, both in the real and virtual realms [23]. Secondary use of personal information refers to the situation where the mobile user's data are being used for an unrelatedly different purpose by another entity without authorization or consent from the individual [23]. Awareness refers to the level to which a user is worried about their understanding of organizational data privacy practices and management [18][19]. Prior privacy experience refers to the condition where Individuals who have had prior experience with personal data mishandling would be more concerned about information privacy [16]. Based on our research question and the previously explained background, we set our research hypotheses as follows:

- Hypothesis 1 (H1): prior privacy experience positively influences MUIPC.
- Hypothesis 2 (H2): user awareness positively influences MUIPC.
- Hypothesis 3 (H3): MUIPC negatively influences the intention to use JAKI.

2.3 Research Design

In conducting the research, we used a quantitative approach by distributing an online questionnaire. To develop the questionnaire items, we used existing scale items from MUIPC and other studies that had repeatedly demonstrated a satisfactory degree of reliability, and we adjusted some of these measurements to match the setting of our research. The instruments were then translated into Bahasa Indonesia. For each question item, we used a 5-point Likert scale ranging from never to very often (for the prior privacy experience variable) and strong disagreement to the strong agreement (for all other variables). Table 1 describes the detail of the variables and questionnaire items.

Table 1. Research Instruments

Variable	Measurement Items	Ref
Prior privacy experience (PP)	PP1: How frequently have you personally witnessed incidents in which your personal information was used by a company or website without your permission? PP2: How many times have you read or heard about the utilization and potential misuse of data obtained from the Internet in the last year? PP3: How frequently have you been the victim of what you perceived to be an unwarranted invasion of privacy?	[16] [23]
Awareness (AW)	AW1: DKI Jakarta Government should disclose how data is gathered, processed, and used when seeking information online. AW2: A proper consumer online privacy policy should include a clear and visible disclosure. AW3: It is critical to me that I am conscious of and comprehend how my private information will be utilized.	[18]
Perceived Surveillance (PS)	PS1: I believe my mobile device's location is tracked at least some of the time. PS2: I'm particularly worried that JAKI apps are gathering too much personal information about me. PS3: I am particularly worried that JAKI apps may track my mobile device activities.	[23]
Perceived Intrusion (PI)	PI1: I believe that because I use JAKI apps, somebody else knows more about me than I am pleased with. PI2: I believe that because I use JAKI apps, my private information is now more easily accessible to others than I would prefer. PI3: I believe that as a result of my use of JAKI apps, personal data about me is available that, if used, will infringe on my privacy.	[23]
Secondary use of personal information (SU)	SU1: I am particularly worried that JAKI apps may be using my personal data to accomplish purposes other than those for which I have given permission. SU2: I am concerned that if I provide personal information to use JAKI apps, JAKI apps may use my personal data for other purposes. SU3: I am particularly worried that JAKI apps may exchange my personal data with third parties without my permission.	[16] [23]
Intention to Use (IU)	IU1: In the next 12 months, I am inclined to share my personal information in order to use the JAKI apps. IU2: In the next 12 months, I expect to use JAKI apps. IU3: In the next 12 months, I plan to use JAKI apps.	[23]

DOI: https://doi.org/10.29207/resti.v6i6.4544

2.3 Data Collection

We used Google Forms to conduct an online survey to test the hypothesis based on our proposed research model. Since the questions provided were adopted from English, before conducting the survey, we conducted a readability test on some candidate respondents. Based on their feedback, several questions' wordings have been corrected so that the question will be easier to understand and not cause ambiguity and multiple interpretations. The survey is being distributed via WhatsApp groups and social media. Data were collected between November 16 to December 27, 2021. The main target respondents were the citizen of Jakarta and its surrounding cities who have used the JAKI application.

In a short period of time, we successfully collected responses from 168 respondents. Out of these 168 respondents, 16 participants stated that they had never used JAKI, and thus, the results were not eligible and needed to be removed from the data set. In the end, we used 152 respondents' data for the analysis. The gender distribution of 152 samples was 92 male and 60 female. The majority of the respondents were millennials (68.4%), held a bachelor's degree (52.6%), and worked in the private sector (46.7%). The demography of participants lived in South Jakarta (28.9%), East Jakarta (18.4%), West Jakarta (17.8%), Central Jakarta (12.5%), North Jakarta (11.8%), Greater Jakarta (9.9%), and Kepulauan Seribu (0.7%). On the frequency of using JAKI, 60.6% of respondents were using JAKI weekly, 25% were using JAKI once a month, 7.2% were irregularly used, and only 7.2% of respondents were open JAKI every day.

2.4 Data Analysis

To process the collected data, we conducted partial least squares structural equation modeling (PLS-SEM) analysis using SmartPLS 3. Because of its broad adaptability and applicability for theory and practice, the use of PLS-SEM is rapidly increasing in a variety of research areas. Furthermore, PLS-SEM is appropriate for unproven models or exploratory model building, and it can be used even when sample sizes are small, data are less normalized, or models are difficult and complicated with many elements and relationships [30]. There was two steps approach involved in conducting the PLS-SEM analysis, i.e., the evaluation of the outer model (measurement model) and the evaluation of the inner model (structural model). In the outer model evaluation, we conducted the reliability test followed by a validity test for the construct measures. To validate indicator reliability, we examined each indicator's loadings relative to its underlying construct. Furthermore, we validated the reflective-reflective second-order construct of our model using the repeated indicator approach. For the inner model, we tested the direct significance effect between latent variables. Finally, we assessed the hypothesis based on the result of the inner model evaluation.

3. Results and Discussions

3.1 Measurement Model Evaluation

There are two steps to evaluate the measurement model, namely the validity test and the reliability test. To evaluate the validity of indicators, we must examine the convergent validity from the loading factor and average variance extracted (AVE) and discriminant validity from cross-loading or Fornell Larcker Criterion. In addition, to check the reliability of the research instruments, we evaluated composite reliability (CR) or Cronbach's Alpha. Using SmartPLS 3, we processed the collected data with a parameter of maximum iterations of 300 and a stop criterion of 10^{-7}. Tables 2 and 3 show the outcome of the process.

Table 2. Reliability Test Result

Indicator	Loading	AVE	CR
AW1	0.941		
AW2	0.932	0.845	0.942
AW3	0.882		
PP1	0.927		
PP2	0.836	0.801	0.923
PP3	0.919		
PS1	0.811		
PS2	0.866	0.729	0.889
PS3	0.882		
PI1	0.917		
PI2	0.939	0.867	0.951
PI3	0.937		
SU1	0.916		
SU2	0.920	0.834	0.938
SU3	0.904		
IU1	0.836		
IU2	0.896	0.786	0.917
IU3	0.925		

Table 2 shows the data for the loading factor, AVE, and CR. As commonly known, the indicators were considered good if the loading value > 0.7, AVE > 0.5, and CR > 0.7.

Based on the data from Table II, the loading factor ranges from 0.811 to 0.941, and AVE ranges from 0.729 to 0.867, which is above the minimum criteria. This indicates that the convergent validity size is adequate or that it fulfills the convergent validity thresholds. Additionally, the CR value shown in Table II ranged from 0.889 to 0.951, meaning that all CR values were above the minimum criteria. This implies that all measurement indicators were reliable.

Table 3. Discriminant Validity Result

	AW	IU	PI	PP	PS	SU
AW	**0.919**					
IU	-0.458	**0.887**				
PI	0.588	-0.584	**0.931**			
PP	0,282	-0.430	0.701	**0.895**		
PS	0.708	-0,562	0.814	0.590	**0.854**	
SU	0.650	-0,569	0.811	0.624	0.802	**0.913**

DOI: https://doi.org/10.29207/resti.v6i6.4544

Discriminant validity examines the extent to which a construct is completely different from another construct. We used the Fornell-Larcker approach with SmartPLS 3, which compares the result of a latent variable's square root to the correlation value among other latent variables. In this approach, the square root of a latent variable result must be greater than the result of the correlation value among the latent variable and other latent variables. Based on table 3. we can see that the square root value of AVE for each latent variable has met the criteria, which infers that the research instruments have good discriminant validity based on the Fornell-Larcker approach.

Table 4. Second-Order MUIPC Reliability Result

Indicator	Loading	AVE	CR
PS	0.926		
PI	0.941	0.707	0.956
SU	0.934		

When analyzing the results of a higher construct model estimation, we not only need to evaluate the measurement models of the lower order construct but also the measurement model of the higher order construct. To validate MUIPC as a reflective-reflective second-order construct, we used the repeated indicator approach. Using SmartPLS, we analyzed the loading value of its three dimensions (PS, PI, SU) as well as the AVE and CR value of MUIPC. The indicators were considered good if the loading value > 0.7, AVE > 0.5, and CR > 0.7. As presented in Table 4. we could conclude that all of the indicators exceeded the minimum criteria, meaning that the latent variable of MUIPC was reliable and valid in representing its dimension.

3.2 Structural Model Evaluation

Table 5. Structural Model Result

	Original Sample (O)	T Statistic (|O/STDEV|)	P Values
PP → MUIPC	0.534	9.128	0.000
AW → MUIPC	0.540	8.504	0.000
MUIPC → IU	-0.613	8.430	0.000

The structural model describes the relationship between latent variables evaluated using the path coefficient, while the path coefficient represents an estimated value that indicates the strength of the relationship between latent variables. To evaluate the significance of the path coefficient can be seen from the T value and P value of each path.

To measure the path coefficient, we used bootstrapping process in SmartPLS with 5000 subsamples and a significance value of 0.5. Based on the result shown in Table V, we tested our hypothesis as follows:

- *H1: prior privacy experience positively influences MUIPC.*
  With a path coefficient value of 0.534 and a P-Value of 0.000, it is shown that PP has a positive effect on MUIPC.
- *H2: user awareness positively influences MUIPC.*
  With a path coefficient value of 0.540 and a P-Value of 0.000, it is shown that AW has a positive effect on MUIPC.
- *H3: MUIPC negatively influences the intention to use JAKI.*
  With a path coefficient value of -0.613, it is shown that MUIPC has a negative effect on IU, and the result is considered statistically significant with a P-Value of 0.000.

3.3 Discussion

This research aims to measure the effect of users' privacy concerns on their willingness to use the JAKI mobile application. Adopted from the Mobile Users' Internet Privacy Concern (MUIPC) theory, we designed the model that examines the relationship between MUIPC and the intention to use and adds prior privacy experience and awareness dimension as antecedents of MUIPC. The model was tested with data collected by an online survey from 152 JAKI users around Greater Jakarta Area. Based on the PLS-SEM analysis using SmartPLS, we concluded that all of the hypotheses are accepted. The results show that prior privacy experience and awareness positively influence the MUIPC. This validates the prior studies, which stated that individuals who have experience relating to the abuse of private information would be more concerned about information privacy. Additionally, this study shows that the higher the awareness of privacy practices, the more serious the concern of users. Finally, the results indicate that MUIPC has a negative impact on the intention to use. This finding indicates that the greater the mobile user's concern for privacy, the less likely they are to use that mobile application.

This study is expected to contribute to the literature research on privacy concerns in several aspects. First, this study contributes to the investigation and understanding of users' privacy concerns in the context of smart city mobile applications in Indonesia. While there are numerous IPC kinds of research conducted in several countries, there is little found in Indonesia. Second, this research empirically attests that the IPC scales, which were originally designed in English, could also be adapted to Bahasa Indonesia and modified for the Indonesian context. Third, the result of this study could help in identifying which privacy concerns that arise from their technology implementation and could become an input for the corresponding Government in formulating policies to protect the privacy of its citizen.

4. Conclusion

This research was motivated by the extensive development of mobile apps and their widespread utilization within smart city ecosystems. By using Jakarta citizen representative data, this study adds to a growing literature that confirms the MUIPC in mobile

DOI: https://doi.org/10.29207/resti.v6i6.4544

apps.

The data analysis and the hypothesis testing result indicates that prior privacy experience and awareness dimension play a significant role in positively influencing MUIPC. On the opposite, MUIPC had a significant effect in negatively influencing the intention to use JAKI. These findings answered our research question in discovering the relative impacts of users' privacy concerns on the intention to use JAKI. Moreover, based on our findings, JAKI users have the high number of awareness and prior privacy experience which influence their privacy concerns in the context of mobile applications (MUIPC). The high number of MUIPC would negatively impact on the intention to use the mobile applications. Thus, we could argue that the citizens in Greater Jakarta who use JAKI were well-aware and well-concerned about their privacy in using the application, and this concern would have an impact on the decision to continue using the application in the future.

Like most similar studies, the limited time of the data collection process and the limited sample size of respondents were the limitations of this study. Despite our best efforts to include a diverse range of individuals representing various social groups of Internet users, respondents were limited to the Jakarta metropolitan area who received the link to the online questionnaire that we distributed, leading to the generalization of the data. Random respondents will statistically increase confidence in our results. Moreover, the model that we used is limited and based only on the MUIPC and two antecedents, without including other important factors which need to be considered in the analysis to provide a more comprehensive picture of this issue. Finally, the object of this study is limited to the area of smart city mobile applications, which is only a small part of implementing technology in a smart city.

We hope that our findings will pique the interest of researchers and serve as a springboard for expanding our current understanding of privacy concerns in smart cities. For the future research direction, we suggest conducting more in-depth research with a wider range of respondents in a different cultural setting. We also instigate to explore the other influencing factors of IPC from the various studies, taking into account both cultural and legal aspects, in order to determine the models and theories that are most appropriate for the Indonesian context. Furthermore, we urge to investigate the privacy issue in the more different context of technologies and application areas of smart cities, particularly in the technology that poses a high risk to privacy.

Acknowledgment

The research was made possible with the support of the E-Government and E-Business Laboratory at the Faculty of Computer Science at Universitas Indonesia, as well as the Ministry of Communication and Informatics of the Republic of Indonesia through the Domestic Master Scholarship Program.

Reference

[1] L. Widiachristy and A. S. Rachmanto, "The Effectiveness of Jakarta Smart City Application in Enhancing Community Resilience in Facing Flood Risk," J. Archit., vol. 20, no. 1, p. 45, 2021, DOI: 10.12962/j2355262x.v20i1.a9034.

[2] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," Expert Syst., no. February, pp. 1–23, 2021, DOI: 10.1111/exsy.12753.

[3] J. L. Hernandez-Ramos et al., "Security and privacy in internet of things-enabled smart cities: Challenges and future directions," IEEE Secur. Priv., vol. 19, no. 1, pp. 12–23, 2021, DOI: 10.1109/MSEC.2020.3012353.

[4] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," Sustain. Cities Soc., vol. 50, no. August 2018, p. 101660, 2019, DOI: 10.1016/j.scs.2019.101660.

[5] V. N. Hoa Hong and L. T. Anh, "Development trends of smart cities in the future - potential security risks and responsive solutions," Adv. Sci. Technol. Eng. Syst., vol. 5, no. 4, pp. 548–556, 2020, DOI: 10.25046/AJ050465.

[6] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," IEEE Access, vol. 6, pp. 46134–46145, 2018, DOI: 10.1109/ACCESS.2018.2853985.

[7] A. I. Tahirkheli et al., "A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures and challenges," Electron., vol. 10, no. 15, 2021, DOI: 10.3390/electronics10151811.

[8] N. H. Abosaq, "Impact of privacy issues on smart city services in a model smart city," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 2, pp. 177–185, 2019, DOI: 10.14569/ijacsa.2019.0100224.

[9] D. Eckhoff and I. Wagner, "Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions," IEEE Commun. Surv. Tutorials, vol. 20, no. 1, pp. 489–516, 2018, DOI: 10.1109/COMST.2017.2748998.

[10] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, 2017, DOI: 10.1109/MCOM.2017.1600267CM.

[11] K. Beck, "Smart security?: Evaluating security resiliency in the U.S. department of transportation's Smart city challenge," Transp. Res. Rec., vol. 2604, no. 1, pp. 37–43, 2017, DOI: 10.3141/2604-05.

[12] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," Inf. Syst. Front., 2020, doi: 10.1007/s10796-020-10044-1.

[13] DetikNews, "Kecewa Warga Gegara Identitas Laporan via JAKI Terbuka." https://news.detik.com/berita/d-5638817/kecewa-warga-gegara-identitas-laporan-via-jaki-terbuka (accessed Nov. 16, 2021).

[14] L. van Zoonen, "Privacy concerns in smart cities," Gov. Inf. Q., vol. 33, no. 3, pp. 472–480, 2016, doi: 10.1016/j.giq.2016.06.004.

[15] J. Bartol, V. Vehovar, and A. Petrovčič, "Should we be concerned about how information privacy concerns are measured in online contexts? A systematic review of survey scale development studies," Informatics, vol. 8, no. 2, 2021, DOI: 10.3390/informatics8020031.

[16] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," MIS Q., vol. 20, no. 2, pp. 167–196, 1996.

[17] K. Bartel Sheehan and M. Grubbs Hoy, "Concern Consumers Kim Bartel Sheehan and Mariea Grubbs," J. Public Policy Markeitng, vol. 19, no. 1, pp. 62–73, 2000.
[18] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," Inf. Syst. Res., vol. 15, no. 4, pp. 336–355, 2004, doi: 10.1287/isre.1040.0032.
[19] T. B. C. P. and A. N. ;Ul.-D. R. Joinson;, "Development of Measures of Online Privacy Concern and Protection for Use on the Internet," J. Am. Soc. Inf. Sci. Technol., vol. 58, pp. 157–165, 2007, DOI: 10.1002/asi.
[20] J. B. Earp, A. I. Antón, L. Aiman-Smith, and W. H. Stufflebeam, "Examining Internet privacy policies within the context of user privacy values," IEEE Trans. Eng. Manag., vol. 52, no. 2, pp. 227–237, 2005, doi: 10.1109/TEM.2005.844927.
[21] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents -measurement validity and a regression model," Behav. Inf. Technol., vol. 23, no. 6, pp. 413–422, 2004, DOI: 10.1080/01449290410001715723.
[22] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys," p. 1, 2011, DOI: 10.1145/2078827.2078847.
[23] J. . Xu, H.; Gupta, S.; Rosson, M.B.; Carroll, "Measuring mobile users' concerns for information privacy," 2012, [Online]. Available: https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10/.
[24] J. Gu, Y. (Calvin) Xu, H. Xu, C. Zhang, and H. Ling, "Privacy concerns for mobile app download: An elaboration likelihood model perspective," Decis. Support Syst., vol. 94, pp. 19–28, 2017, DOI: 10.1016/j.dss.2016.10.002.
[25] A. Geovanny, I. W. Tong, J. A. Yang, and V. O. Vianto, "the Effect of Privacy Concern Towards the Intention To Accept App Permission on Batam Students Mobile Users," no. 455, 2021.
[26] 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.
[27] C. B. Foltz and L. Foltz, "Mobile users' information privacy concerns instrument and IoT," Inf. Comput. Secur., vol. 28, no. 3, pp. 359–371, 2020, DOI: 10.1108/ICS-07-2019-0090.
[28] B. Lopes, D. R. G. de Pontes, and S. D. Zorzo, "An instrument for measuring privacy in IoT environments," Adv. Intell. Syst. Comput., vol. 800 Part F, no. Itng, pp. 49–55, 2019, DOI: 10.1007/978-3-030-14070-0_8.
[29] R. Wiegard, N. Guhr, S. Krylow, and M. H. Breitner, "Analysis of wearable technologies' usage for pay-as-you-live tariffs: recommendations for insurance companies," Zeitschrift fur die gesamte Versicherungswiss., vol. 108, no. 1, pp. 63–88, 2019, DOI: 10.1007/s12297-019-00431-2.
[30] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," SN Appl. Sci., vol. 2, no. 2, 2020, doi: 10.1007/s42452-020-2025-8.

DOI: https://doi.org/10.29207/resti.v6i6.4544