INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 12, (2025) E-ISSN: 2222-6990

The Effect of Security and Privacy Concerns towards User Adoption of Big Data in Telecommunication Services

Nur Fadzilah Othman[1], Syarulnaziah Anawar[2], Siti Rahayu Selamat[1], Zakiah Ayop[2], Norharyati Harum[2], Cik Feresa Mohd Foozy[3]

[1]Fakulti Kecerdasan Buatan dan Keselamatan Siber, Universiti Teknikal Malaysia Melaka, Malaysia, [2]Center for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malaysia, [3]Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Batu Pahat Johor, Malaysia

Corresponding Author Email: fadzilah.othman@utem.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i12/26946

Published Date: 02 December 2025

Abstract

The telecommunication industry is the leading industry in Big Data trends as the industry has the most infrastructure capability for Big Data. The adoption of Big Data in telecommunication services fosters extensive real-time data collection. However, the adoption of Big Data in telecommunication services also raises important security and privacy challenges. The perspectives of telecommunication users on issues about privacy and security, as well as the correlation with take-up and continued use of applications and services utilizing Big Data. A questionnaire survey was used to identify the effect of security and privacy concerns towards user adoption of Big Data. An empirical analysis involved a total of 400 respondents. Results indicate that perceived trust mediates the effect of collection, improper access, and error towards Big Data adoption, while perceived risk mediates the effect of collection, improper access and error towards Big Data adoption in telecommunication services. Perceived risk only mediates the effect of data privacy awareness towards user's adoption. Finally, perceived trust and risk significantly predict users' adoption of Big Data in telecommunication services. With the combined theory of Concern for Information Privacy (CFIP)) and Trust, Confidence and Cooperation (TCC) Model, this study provides the basis to direct future studies in the related field.

Keywords: Security Concern, Privacy Concern, Big Data Adoption, Telecommunication Services

Introduction

The advancements in information and communication technologies over the last decade have resulted in the generation and use of an unprecedented amount of data about every aspect of modern life (Acquisti, Taylor, & Wagman, 2016). As a result, Big Data has evolved as a practical method of dealing with and using the influx of information.

Having access to massive volumes of data, the telecommunication service provider is also emerging as a prominent proponent of the Big Data trend in recent years. For example, a telecommunication service provider may collect call detail data, network data, and customer information to understand better how customers use their service and interact with it. Due to the valuable insights and analytics that Big Data can offer to businesses, Big Data is becoming a necessary aspect of doing business in practically all industries as time goes on. However, the increased usage of Big Data does not come without risks. One of the most significant concerns is the compromise of personal privacy and data security of persons and their data. For the telecommunications service provider, data security and data privacy are two requirements that must be met. A relationship exists between Big Data and privacy and security-related issues, including data collection, archiving, sharing, and accessibility (Martin ,2015). Because of the increase in security and privacy issues, telecommunications service providers have difficulty dealing with security and privacy concerns. Therefore, this study aims to examine the viewpoints of telecommunications users on privacy and security concerns in telecommunication services and the correlation between adoption and continuous usage of applications and services that leverage Big Data.

This paper is structured as follows: Section 2 conducts a literature review on Big Data security and privacy implications. Section 3 introduces the theoretical basis. Section 4 discusses the details of the methodology. Finally, Sections 5 and 6 offer the results of the data analysis and a discussion of the findings. The last section concludes this paper.

Literature Review

Big Data in Telecommunication Services

Big data is a term that refers to combining massive amounts of complex data with powerful analytics to enhance security and marketing while minimising risk (Martin, 2015) . The 3V's of big data management were initially mentioned by Laney (2001) : volume, velocity, and variety. The big data concept has been successfully applied in business by well-known internet platforms to manage real-time data in the billions of bytes (Keshavarz et al., 2021). According to Frizzo-Barker et al.,2016), there are various critical insights to be gained from the examination of big data, and it remains a topic of research that is still in its infancy in terms of theoretical grounding Sajjad & Dhary (2020). Big data presents the opportunity for researchers to investigate new scientific fields. Initially, the rise of big data was seen as a socio-technological phenomenon. However, big data also brings a slew of obstacles ranging from data collection and technology issues to processing and maintenance issues and corporate and social ramifications.

The telecommunication industry is one of the industries which has benefited from big data. Telecommunication service providers have access to vast volumes of data and a sizable customer base that regularly connects to their services and networks. By expanding voice business into broadband, telecommunication service providers are now generating large

amounts of data (subscribers make more calls and connect to the internet in greater numbers), and benefiting from a diverse set of sources (heavy usage of multiple internet broadband applications) and also from high data velocity levels (for instance, Malaysians spend around 7.5 hours on the internet and 2.45 hours on social media daily in the opposite to just short messages and few calls (Keshavarz et al., 2021). As the number of smartphone users continues to grow, service providers can monitor regular customer profiles, device data, network data, customer usage patterns, location data, apps downloaded, call durations, and other data. Such data can be highly informative for telecommunication service providers to make informed decisions and execute appropriate customer experience, network optimization, operational analysis, and data monetization strategies.

Security and Data Privacy Concern in Big Data

Security is the practice of defending information and information assets through technology, processes, and training from unauthorized access, disclosure, disruption, modification, inspection, recording, and destruction (Jain et al., 2016).Data privacy refers to a person's or a group's ability to keep personal information from being shared with persons other than those to whom they disclose it (Westin, 2015). The challenge from a security and data privacy standpoint is to ensure that customers have long-term control over their data, preventing misuse and abuse by data controllers while preserving data utility.

Security and data privacy are crucial challenges in big data adoption among data subjects since it includes personal and sensitive information for customers. The flow of data and content that contributes to big data includes material created, kept, and processed for a specific purpose. Crawford & Schultz (2014) argue that the extensive use of existing data and analysis in big data will result in detailed individual profiles.

The risk of data breaches grows as more data becomes available and stored in online databases and is increasingly shared with third parties. As a result, big data raises security and data privacy concerns about who has access to, stores, and uses customer data. Other than that, as data collection, processing, and sharing in the context of big data is becoming more ubiquitous than in traditional online environments, control over personal information flows becomes harder to maintain (Sajjad & Dhary, 2020). These concerns cast questions on whether customers' right to preserve control over data they explicitly and implicitly disclose can be effectively enforced. Additionally, it raised a concern whether individual control of personal data throughout the entire data life cycle is a feasible or achievable goal in the context of big data.

Another security and data privacy concern in big data is regarding the accuracy of data. Telecommunication providers need to adequately design data collection methods and extra measures to reduce and avoid the risk of making incorrect decisions and misinterpretations resulting from inaccuracies in the data collection process. Acting based on insights gained from either inaccurate data or imprecise big data, data subjects may suffer serious and negative consequences including being sorted into categories, which often reinforce existing social stereotypes, subsequently being subjected to unfair or unlawful discrimination, denied access to services, or otherwise subjected to unpleasant experiments (Smith, 2011).

Theoretical Framework

Concern for Information Privacy (CFIP) Model

The Concern for Information Privacy (CFIP) model was first developed by Smith, Milberg, & Burke (1996) to measure individuals' concerns regarding organisational practices. Subsequent research, Stewart & Segars (2002) stated that the CFIP needs to be revaluated and modified in light of technology, research, and practice developments. CFIP consists of four dimensions of information privacy concerns: collection, errors, secondary use, and unauthorised access to information.

The collection is best described as the concern that extensive amounts of personally identifiable data are collected and stored in databases (Smith, Milberg, & Burke, 1996). When collecting personal information from users, the telecommunication service provider may request a great deal of information that is not necessary, such as the user's credit card details, ethnicity, and others. This may increase users' concerns about excessive data collecting. Improper access can be defined as the degree to which a person is concerned that personal information is readily available to people not properly authorised to view or work with the data (Stewart & Segars, 2002). Improper access usually reflects on the security of information storage. Errors entail the concern that inadequate procedures are used to protect against accidental or deliberate errors in storing personal data (Hsu & Lin, 2016). Errors are indicative of the accuracy of personal data stored in databases. According to Smith, Milberg, & Burke (1996), secondary use of personal data is when data is collected from individuals for one purpose but is used for another (e.g., profiling individuals and sending marketing messages) without authorisation from the individuals. Secondary use of personal data can jeopardise the organisation's legitimacy in its interactions with consumers, shareholders, and regulators (Culnan & Armstrong, 1999) .

Individuals' concerns about data collection, errors, unauthorised access, and secondary use will increase perceived risk (Meyliana et al., 2019). They may be concerned about collecting, storing, and using their data. Additionally, according to Zhou (2011) , perceived trust plays an important factor in mediating privacy concerns and user attention. Users with a high level of privacy concern will doubt the trustworthiness of the telecommunication service provider. For instance, they may have doubts about telecommunication service providers' ability to prevent unwanted access to their personal information. They are undoubtedly concerned about whether telecommunication service providers are looking out for their best interests and do not share their data with third parties.

Trust, Confidence and Cooperation (TCC) Model

The Trust, Confidence, and Cooperation (TCC) Model was introduced by Earle et al. (2012) and describes the dual concepts of social trust and confidence. Trust is an idea related to the self-confidence, hope, reliability, dependence, integrity, and capacity of an entity Meyliana et al. (2019), while risk is an act of a person who produces a decision that gives hope and detrimental effect (Peter & Ryan, 1976). Perceived risk has been investigated since the 1990s theory to describe individuals' behaviour, and numerous works have studied the impact of perceived risk on the individual's decision and adoption (Lin, 2006).

A growing number of empirical studies have explored the nature of trust in risk management and the relations between trust, risk, and cooperation. The relation between trust and risk

was stronger (Larson et al., 2018). The study by Lu et al. (2015) presents that risk perception depends on the trust in the situation of the matter. Furthermore Lu et al. (2015) in his study, also found that trust significantly affects perceived risk, and both factors further determine user behaviour. In using technology, trust and perceived risk are related to adopting such technology (Meyliana et al., 2019). Trust ensures that users will have excellent outcomes in the future. To gain customers' trust, telecommunication service providers might rely on their reputation, brand, and connections to other well-known telecommunication service providers. Telecommunication service providers who have successfully developed traditional or online channels will have an edge in gaining user trust.

Security and Data Privacy Awareness

Awareness is a critical component of any information security approach. Security awareness is a state where individuals are aware of and ideally committed to their security mission (Al-Daeef, Basir, & Saudi, 2017) . In contrast, data privacy awareness reflects how clearly users understand how their data are handled and processed by used applications (Chrysakis et al., 2021). Individuals' lack of security awareness can manifest itself in various ways, including browsing and thereby giving personal information to untrustworthy websites, installing harmful applications, and sharing personal information with others. Lack of awareness and knowledge about security measures raises concerns and worries they will be exposed to security risks and breaches (Smit et al., 2014). Additionally, Castañeda & Montoro (2007) argued that individuals feel they are likely to face risks if they are unaware that the data is collected and registered.

Based on the above discussions, this paper proposes the theoretical framework as shown in Figure 1.

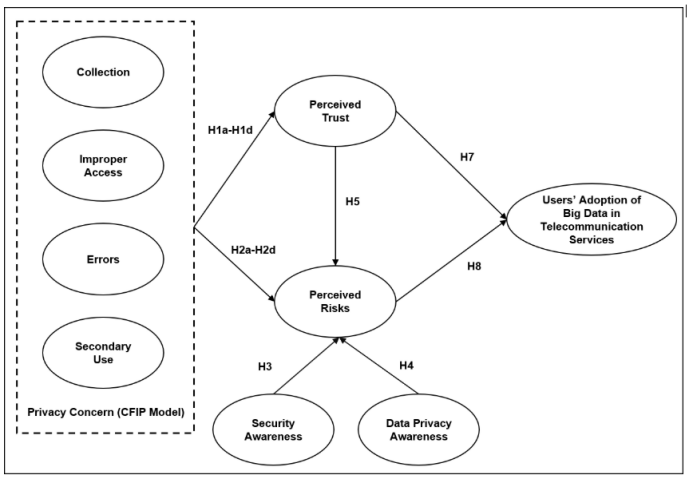

Fig. 1. Proposed Framework

The important aspect of the proposed research model is the assumption that there are two pathways to the adoption of Big Data in telecommunication services, which is via a perceived trust or perceived risks in the services. From the related work previous studies, a list of variables is identified which suited the study on security and privacy risk for technology use. The variables are then examined, and the variables that fit the context of Big Data in telecommunication services are identified. The hypotheses that we can get as the following:

Hypothesis 1(a-d): The effect of CFIP antecedent towards user's adoption would be mediated by Perceived Trust.

Hypothesis 2(a-d): The effect of CFIP antecedent towards user's adoption would be mediated by perceived Risk.

Hypothesis 3: The effect of Security awareness towards user's adoption would be mediated by Perceived Risk.

Hypothesis 4: The effect of Data Privacy awareness towards user's adoption would be mediated by Perceived Risk.

Hypothesis 5: Perceived Trust would be significantly associated with Perceived Risk.

Hypothesis 7: Perceived Trust would significantly predict Users' adoption.

Hypothesis 8: Perceived Risk would significantly predict Users' adoption.

Methodology

Instrument Design

This study used a structured questionnaire for data collection. The operational definition of the dependent variables, independent variables, and modifying variables is first developed as shown in Table 1.

Table 1
Operational definitions and source of items

Variables	Operational Definition	Source of Items
Collection (C)	Users' concerned whether their personal information is overly collected by the telecommunication service provider.	[11]. [12]
Improper Access (IA)	Users' concern about whether telecommunication providers fail to protect access to their personal information from unauthorised entities	[11]. [12]
Error (E)	User's concerned as to whether their personal information is appropriately protected from errors.	[11]. [12]
Secondary Use (SU)	Users' concerned about whether telecommunication providers use personal information for illegal or unauthorised purposes.	[11]. [12]
Perceived Trust (PT)	User's belief or confidence about telecommunication provider's trustworthiness.	[16], [26]
Perceived Risks (PR)	User's expectation of losses associated with the release of personal information to the telecommunication service provider.	[16], [27]
Security Awareness (SA)	Level of knowledge and understanding regarding information security and the relevant protection mechanisms.	[28]
Privacy Awareness (PA)	Level of knowledge and understanding regarding the options for privacy available to them and the privacy practices of the telecommunication provider.	[29]
User Adoption (UA)	The acceptance, integration, and use of telecommunication services.	[30]

The questionnaire is divided into four sections, namely section A, B, C, and D. In section A, a participant is required to provide their demographic information. Section B is to indicate the telecommunication user's concern for information security and data privacy. Section C

includes questions to evaluate telecommunication users' awareness of information security and data privacy, whereas Section D evaluates telecommunication users' adoption of big data. Most of the items in section B are adapted from the CFIP scale and are then modified to fit the context of the present study. Other item s in Sections C and D were self-developed from a critical review of literature in information security. There is a total of 46 items in the survey instrument. The sources of the items are shown in Table 1.

Instrument Validity and Reliability

Content validity was carried out to verify the representation and relevance of the items in measuring the variables. The questionnaire is validated by six experts with a minimum experience of 10 years. The experts are selected based on their expertise in the field of information security and usable security. The experts are given the variable and the items that represent the variable in the content validation form. The experts are requested to critically review the variable and its items before scoring on each item using a 4-point degree of relevance. There are two forms of Content Validation Index (CVI) namely, item-level content validity index (I-CVI) and scale-level content validity index (S-CVI). This study will measure I-CVI and S-CVI based on the average method (S-CVI/Ave) (Crawford & Schultz, 2014); Smith, 2011). To calculate CVI, scores 3 and 4 were re-categorised into 1 (relevant) and others into 0 (not relevant). I-CVI was calculated, and the item with the value of I-CVI below 0.83 was dropped. This is in accordance with the study by [31], who stated that the acceptable CVI values for six to eight experts should be at least 0.83. Some of the items are revised based on the comments of the experts. Before the revision, the value of S-CVI/Ave was 0.8789, while the value after revision was 0.9211. The total number of items after revision is 38. The I-CVI and S-CVI/Ave meet satisfactory levels, indicating that the questionnaire scale has a satisfactory level of content validity.

A pilot study was carried out by collecting data from 50 respondents to determine the reliability of the questionnaire. The questionnaire's reliability is tested using the Cronbach alpha value for each variable. A total of nine variables (38 items) have been tested. The initial reliability test shows that seven variables are considered highly reliable where the Cronbach alpha value is above 0.7. The variables are collection (COL), improper access (IA), error (ERR), perceived trust (PT), perceived risk (PR), security awareness (SA), privacy awareness (PA), and user adoption (UA) with Cronbach alpha values of 0.911, 0.92, 0.928,0.938,0.819,0.953, and 0.923, respectively. Error (ERR) and secondary use (SU) show lower Cronbach alpha value; thus, item ERR4 was removed from the error variable and item SU3 and SU4 were deleted from the secondary use variable. The reliability analysis was carried out again to meet the requirement of a Cronbach Alpha value of 0.7 and higher.

Data Collection

A total of 400 respondents were included in this study. In order to improve the quality of survey response, the criteria for selecting the participants for the quantitative study included: (1) familiarity with smartphones and (2) experience in the use of the MySejahtera application. This study utilised non-proportional quota sampling. The abovementioned target sample will be subdivided into unequal proportions of respondents to represent the age demographic segments in the study. The proportion of each quota of respondents is based on the percentage distribution of smartphone owners by age group in the Hand Phone User Survey conducted by Malaysian Communications and Multimedia Commission (MCMC) in 2017. This

strategy is selected to further investigate the association of age with the security and privacy awareness variables. This study argues that the use of quota sampling is sufficient to draw a conclusion as the purpose of this study is to generalise to theoretical propositions, not to wider populations.

The questionnaire will be distributed in two ways. First, the respondent will be given a printed questionnaire, particularly for elderly respondents. Second, the same question is created in Google forms and will be distributed online. The sampling process will be advertised to everyone on Facebook, Messenger, WhatsApp, and email. All the respondents voluntarily answer the question. For elderly respondents who are not familiar with Google forms, the questions will be given in printed copy. All responses are then collected and transferred to an excel file before the data is analysed in SmartPLS software. The data collection process is done within one month

Results

Respondent Profile

Three demographic criteria are collected in the survey, namely age, gender and telecommunication provider. Table 2 displays the summary of respondent profiles.

Table 2
Respondent profiles

Categories	Description	Frequency	Percentage (%)
Gender	Male	148	37.0
	Female	252	63.0
Age	<20	50	12.5
	20-34	191	47.8
	35-49	102	25.5
	50-64	48	12.0
	>65	9	2.3
Tele-communication Provider	Maxis	60	15.0
	Celcom	123	30.8
	Digi	52	13.0
	U Mobile	79	19.8
	Unifi Mobile	40	10.0
	redONE	18	4.5
	TuneTalk	19	4.8
	Other	9	2.3

Factor Analysis

Exploratory Factor Analysis (EFA) is performed to explore the relationship between observed variables, and to group them according to their factor loading. In this study, direct oblimin rotation is used, as it is an oblique rotation method to allow correlation between factors. There is a total of 33 items in independent variables after EFA was carried out. Two items were removed from the survey instrument. All items were grouped into eight factors based on their highest factor loadings. The extracted factor's structure explained 74.1%, of the variance, which is sufficient for social science research. A minimum of two items should be loaded in each factor (Henseler et al., 2009); otherwise, the factor will be eliminated. None of the factors were dropped.

Hypothesis Testing

In order to test hypotheses, path coefficients (results of PLS), in addition to p-values (results of bootstrapping), were examined. In addition, the strength of the mediator variable's relationships with the other independent variables is analysed. To test the hypothesised model, the condition of mediation is evaluated based on the guideline given by Hair et al. (2021) and Zhao et al. (2010) . From the results, four hypotheses were rejected, namely H1d, H2b, H3, and H5, whereby the p-value of the path coefficient is under a significant value of 0.05; $p < 0.05$. In addition, PLS-SEM was used to determine the effects of eight independent variables on the user adoption of big data. The results show this model to be structurally good (R2 0.657), and able to predict user adoption of big data in telecommunication services. Table 3 summarises the results for hypothesis testing.

Table 3
Summary of Results

Hypotheses	From → To	Path Coefficient			Mediation	Result
		PT	PR	UA		
H1a	COL	-0.119*		0.006	Full	Accepted
H1b	IA	-0.604*		0.068	Full	Accepted
H1c	ERR	0.148*		0.246*	Partial	Accepted
H1d	SU	-0.014		-0.008	No	Rejected
H2a	COL		0.369*	0.006	Full	Accepted
H2b	IA		0.008	0.068	No	Rejected
H2c	ERR		0.201*	0.246*	Partial	Accepted
H2d	SU		0.220*	-0.008	Full	Accepted
H3	SA		0.072	0.024	No	Rejected
H4	PA		0.130*	0.296*	Partial	Accepted
H5	PT		0.018		NA	Rejected
H6	PT			0.136*	NA	Accepted
H7	PR			0.068*	NA	Accepted
Notes: Overall Model F= 48.334; *p<0.05; R^2 = 0.657; adjusted R^2 = 0.66						

Discussion

The adoption of Big Data technology is usually associated with the perceived quality of the services in terms of the improvement in quality of life (Chatterjee et al., 2019). However, due to the increased demand for secure Big Data implementation, the telecommunication service provider needs to understand and capture the market needs pertaining to security and privacy. This study sought to investigate the influence of security and privacy concerns towards user adoption of Big Data in telecommunication services. In addition, this study investigates the effect of security awareness and data privacy awareness on user adoption. The important aspect of this study is the assumption that the influence of the independent variables is mediated through perceived trust and perceived risk in telecommunication services. Thus, this study can produce insight and provide guidelines to the telecommunication service provider in how telecommunication users evaluate the utility and adoption of Big Data service according to their security and privacy concerns and awareness. Concerning hypotheses H1a-d and H2a-d, the findings of the PLS structural modelling indicates partial support for our initial hypotheses that perceived trust and perceived risk will mediate the relationship between security and privacy concerns and Big Data adoption in telecommunication services. The influence of users' concern on collection towards Big Data

adoption was fully mediated by perceived trust and perceived risk in telecommunication service providers. Interestingly, among all security and privacy concerns, only error (ERR) has a direct effect on Big Data adoption, which is partially mediated by perceived trust and perceived risk. This indicates that information accuracy plays an important role in users' decision to adopt Big Data services from the telecommunication service provider.

On the other hand, the effect of user's concern on secondary use towards Big Data adoption was fully mediated by perceived trust only, but not by perceived risk. Thus, H1d is rejected. In contrast, users' concern on improper access does not influence Big Data adoption and was fully mediated by perceived risk only, but not by the perceived trust. Therefore, H2b is not supported. The findings seem to suggest that when evaluating the potential damage from security and privacy breach, the telecommunication users are more concerned about the technical ability of the telecommunication service providers in mitigating the risks. A possible explanation for this might be due to the user's perception that risks, both financial and non-financial, are usually associated with the lack of competence of service providers in protecting their data, which is subject to improper access and error in the data (Dewi & Ketut, 2020).

Among four variables of security and privacy concerns, the improper access variable has a significantly higher effect on perceived trust. The higher the users' concern on unauthorized access, the higher users' distrust of the telecommunication providers. The findings indicate that the users feel that the telecommunication service provider is deemed trustworthy when the provider telecommunication provider has the technical ability to protect access to their personal information from unauthorized entities. The significant relations between service providers' technical competency and customer's trust has been reviewed extensively in other industry such as e-commerce (Connolly & Bannister, 2007), health (Leisen & Hyman, 2001) , and banking (Yousafzai et al., 2003). On the other hand, the collection variable has a significantly higher effect on perceived risk among the four variables of security and privacy concerns. The findings observed in this study mirror those of the previous studies (Zhou, 2011) , where the users feel that the telecommunication service provider is deemed trustworthy when the provider does not over-collect their personal information.

Telecommunication users' awareness of data privacy regulations greatly impacts Big Data adoption. The data privacy awareness shows that when the users make informed choices about sharing their personal data with telecommunication providers and how their data is being processed, it will directly affect the adoption of Big Data services. Contrary to expectations, it is interesting to note that this study did not find any significant relation between perceived trust and perceived risk. TCC Model by Siegrist et al. (2012) offers a possible explanation for the results. Under the condition of the perceived importance of the issue is low, and the users' awareness (i.e. knowledge) is high, trust will be irrelevant to perceived risk.

Conclusion and Future Works

This research aims to study the effect of security and data privacy concerns on Big Data adoption in telecommunication services. A proposed framework was contributed by defining the main elements and providing a comprehensive model that will affect the Telecommunication services in adopting Big Data.

The research makes significant contributions to the literature on Big Data adoption, both theoretically and contextually. Theoretically, it extends current knowledge by integrating the Concern for Information Privacy (CFIP) framework with the Trust, Confidence, and Cooperation (TCC) model to better explain how privacy concerns influence adoption behavior in the telecommunication industry. The study empirically validates previously underexplored relationships in Big Data adoption by demonstrating the mediating roles of perceived trust and perceived risk between collection, improper access, error and secondary used towards user adoption. Contextually, this research provides new evidence from the perspective of telecommunication service users in a developing country setting, where Big Data infrastructure is rapidly expanding while privacy governance remains in its early stages. The findings offer practical implications for telecommunication operators and policymakers to design user-centric data protection strategies that strengthen trust, reduce risk perceptions, and encourage responsible Big Data adoption.

The recommendation for future study in this field could overcome the limitation of this study such as the method to collect data by using quota sampling could be overcome by using another method that could avoid bias selection on the population. The method of collecting the feedback from the respondent by using a questionnaire also could be improved in a future study to gain more variety of feedback such as interview, recording, observation, and others. A better and specific study to gain more understanding in privacy protection behavior could obtain by a qualitative and high variety of efforts to ensure the study tandem with the rising of technology. Besides, this study could be improved by adding more variables towards Big Data adoption, there could be more potential security and data privacy effect to exert more significant influence and impact on Big Data adoption. Last but not least, expanding sample size and other ages with their background of education or various experience of the respondent can be extended to better generalize the analysis and potentially strengthen it among telecommunication service provider customers in Malaysia. By expanding sample size, it may result in different intend, patterns, and behavior. Hence, the future study can overcome all the limitations in this study to gain better and specific results of Big Data adoption among in Malaysia.

Acknowledgment
This research is funded by Malaysian Communications and Multimedia Commission, Malaysia through the 2021 Digital Society Research Grant. This publication has been supported by Center of Research and Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM).

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. Lecture Notes in Engineering and Computer Science, 2229, 446–451.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1). https://doi.org/10.1016/j.heliyon.2021.e06016

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. Electronic Commerce Research, 7(2), 117–141.

Chatterjee, S., Chaudhuri, B. R., & D., D. (2019). Determinants of adoption of new technology in telecom sector: A structural equation modeling approach. Global Business Review, 20(1), 166–178.

Chiou, J. S. (2004). The antecedents of consumers' loyalty toward Internet Service Providers. Information and Management, 41(6), 685–695. https://doi.org/10.1016/j.im.2003.08.006

Chrysakis, I., Flouris, G., Makridaki, M., Patkos, T., Roussakis, Y., Samaritakis, G., Tsampanaki, N., Tzortzakakis, E., Ymeralli, E., Seymoens, T., Dimou, A., & Verborgh, R. (2021). A rewarding framework for crowdsourcing to increase privacy awareness. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12840 LNCS, 259–277. https://doi.org/10.1007/978-3-030-81242-3_15

Connolly, R., & Bannister, F. (2007). Consumer trust in Internet shopping in Ireland: Towards the development of a more effective trust measurement instrument. Journal of Information Technology, 22(2), 102–118.

Crawford, K., & Schultz, J. (2014). Big Data and due process: Toward a framework to redress predictive privacy harms recommended citation. Boston College Law Review, 55(1), 1–29. http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dewi, R. P. L., & Ketut, R. I. (2020). Role of trust in mediating the effect of perceived risk and subjective norm on continuous usage intention on Gopay users in Denpasar. Russian Journal of Agricultural and Socio-Economic Sciences, 108(12), 69–80.

Earle, T. C., Siegrist, M., & Gutscher, H. (2012). Trust in cooperative risk management: Uncertainty and scepticism in the public mind. In Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind (Issue July 2014). https://doi.org/10.4324/9781849773461

Frizzo-Barker, J., Chow-White, P. A., Mozafari, M., & H. D. (2016). An empirical study of the rise of big data in business scholarship. International Journal of Information Management, 36(3), 403–413.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publications.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In New challenges to international marketing. Emerald Group Publishing Limited.

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy

perspectives. Computers in Human Behavior, 62, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. Journal of Big Data, 3(1). https://doi.org/10.1186/s40537-016-0059-y

Keshavarz, H., Mahdzir, A. M., Talebian, H., Jalaliyoon, N., & Ohshima, N. (2021). The value of big data analytics pillars in telecommunication industry. Sustainability (Switzerland), 13(13). https://doi.org/10.3390/su13137160

Laney, D. (2001). 3D data management: Controlling data volume, velocity, and variety. Application Delivery Strategies, 6(70).

Larson, H. J., Clarke, R. M., Jarrett, C., Eckersberger, E., Levine, Z., Schulz, W. S., & Paterson, P. (2018). Measuring trust in vaccination: A systematic review. Human Vaccines and Immunotherapeutics, 14(7), 1599–1609. https://doi.org/10.1080/21645515.2018.1459252

Leisen, B., & Hyman, M. R. (2001). An improved scale for assessing patients' trust in their physician. Health Marketing Quarterly, 19(1), 23–42.

Lin, W. B. (2006). Investigation on the model of consumers' perceived risk – Integrated viewpoint. Expert Systems with Applications, 34(1), 977–988.

Lu, X., Xie, X., & Xiong, J. (2015). Social trust and risk perception of genetically modified food in urban areas of China: The role of salient value similarity. Journal of Risk Research, 18(2), 199–214. https://doi.org/10.1080/13669877.2014.889195

Lynn, M. R. (1986). Determination and quantification of content validity. Nursing Research.
Martin, K. E. (2015). Ethical issues in the big data industry. MIS Quarterly Executive, 14(2), 67–85. https://doi.org/10.4324/9780429286797-20

Meyliana, M., Fernando, E., & Surjandy, S. (2019). The influence of perceived risk and trust in adoption of FinTech services in Indonesia. CommIT (Communication and Information Technology) Journal, 13(1), 31. https://doi.org/10.21512/commit.v13i1.5708

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Peter, J. P., & Ryan, M. J. (1976). An investigation of perceived risk at the brand level. Journal of Marketing Research, 13(2), 184–188.

Sajjad, R., & Dhary, A.-R. (2020). Using big data in telecommunication companies: A case study. African Journal of Business Management, 14(7), 209–216. https://doi.org/10.5897/ajbm2019.8874

Siegrist, M., Earle, T. C., & Gutscher, H. (2012). Trust in cooperative risk management: Uncertainty and scepticism in the public mind. In Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind (Issue July 2014). https://doi.org/10.4324/9781849773461

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, June, 167–197.

Smith, T. F. (2011). Measuring the business value of data quality.

Smit, E. G., Van Noort, G., & Voorveld, H. a. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. Computers in Human Behavior, 32, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97

Westin, A. (1967). Privacy and freedom. Ig Publishing, Incorporated, 2015.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. Technovation, 23(11), 847–860.

Yusoff, Z. M. (2011). The Malaysian personal data protection act 2010: A legislation note. NZJPIL, 9(119).

Zhao, X., Lynch Jr, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. Journal of Consumer Research, 37(2), 197–206.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. Industrial Management and Data Systems, 111(2), 212–226. https://doi.org/10.1108/02635571111115146

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. Computers in Human Behavior, 26(4), 760–767. https://doi.org/10.1016/j.chb.2010.01.013