
MCMC
DSRG
DIGITAL SOCIETY RESEARCH GRANT
MEDIA MATTERS
DIGITAL SOCIETY RESEARCH REPORT VOL. 5

RESEARCH REPORTS

CONTACT US

SECURITY AND PRIVACY CHALLENGES OF BIG DATA ADOPTION: A CASE STUDY IN THE TELECOMMUNICATIONS INDUSTRY

Syarulnaziah Anawar,
Siti Rahayu Selamat,
Nur Fadzilah Othman,
Norharyati Harum &
Zakiah Ayop

Universiti Teknikal Malaysia Melaka

ABSTRACT

The telecommunications industry is the most appropriate industry to observe big data trends as this industry not only has the most capable infrastructure for big data collection, but also needs to utilise it extensively in the context of location services it provides to individuals. However, the adoption of big data in telecommunications services also raises important security and privacy challenges. This study focuses on investigating the security and privacy challenges for both data users and data subjects in telecommunications services and examines codes of practices and standards to address the privacy and security challenges. The proposed study is conducted using mixed-methodology, qualitative and quantitative methodology, where each phase is conducted concurrently and independently of each other. From the perspectives of data users, it could be concluded that data management, data privacy, data compliance, and regulatory orchestration challenges are the most pressing concerns in big data adoption. From the perspectives of the data subject, the findings indicate that only the error variable has a direct effect on big data adoption, which is partially mediated by perceived trust and perceived risk. Among the four variables of security and privacy concerns, the improper access variable has a significantly higher effect on perceived trust. Similarly, the collection variable has a significantly higher effect on perceived risk among the four variables. Finally, the findings show that telecommunications users' awareness of data privacy regulations greatly impacts big data adoption. The contributions of the proposed study are two-fold: (1) to help identify the perceived risk implications of the information collected, stored, shared, and managed in big data, and assess reasonable mitigation strategies in the context of data sharing for big data purposes; and (2) to serve as recommendations for the developers and decision-makers to design a secure and fully ethically compliant big data solution in the telecommunications industry.

Keywords: Big Data, Security, Privacy, Telecommunications

INTRODUCTION

Big data analytics has the capacity to extrapolate trends and patterns to predict the behaviour of a given population or even of individuals (Hardy, 2017).

The telecommunications industry is the leading industry in big data trends as the industry has the most capable infrastructure for big data (Chua et al., 2015). With the rollout of 5G technology, numerous emerging big data technologies have emerged as they are able to capitalise from the improved connectivity. The collection of geolocation data of telecommunications subscribers has opened up many opportunities in collecting continuous and real-time data (Wang et al., 2017) as the service provider is able to obtain geolocation data without internet services through the cellular network protocol once the subscriber turns on their mobile device. This capability may greatly benefit most areas of government services by enabling surveillance systems, cybersecurity, and public safety and defence.

Despite the potential advantages of big data, automated data collection by telecommunications service providers is not without scrutiny as it may pose privacy and security challenges. Privacy and security risks may vary depending on the purpose and types of collected data in the big data application, and the type of framework used in developing the application. Many big data applications in Malaysia are considered privacy-invasive because these applications adopt a centralised architecture, where all collected data is stored on a central server. Data breaches are the main threat in big data applications. Therefore, the telecommunications service application must adopt an open-source framework that allows system transparency for the public to test and suggest measures to correct vulnerabilities in the big data application. However, the lack of an open framework is to be expected as the requirement for the telecommunications service provider to protect personal information becomes complicated due to the uncertain reliability of data de-identification. The data user's best efforts in de-identifying personal identifiable information (PII) may not prevent the re-identifying of an individual because data could be combined with other sources (Narayanan, 2008).

Problem Statement

Pursuant to the Personal Data Protection Act, 2015 (PDPA), commercial entities are under an obligation to comply with certain obligations and rights afforded to persons providing information. These obligations and rights were further clarified

under the Personal Data Protection Standard (2015). This standard encompasses security, retention, and data integrity standards, which apply to personal data that is processed electronically and non-electronically.

However, despite the introduction of the PDPA and its various subsidiary legislation, there have been incidents where unauthorised sharing of information of data subjects has occurred. Additionally, the level of awareness and understanding of consumers of their rights and protection mechanisms is also unclear and whether there is a correlation between awareness and understanding and the take-up of various digital services. The telecommunications sector is an identified sector that the Personal Data Protection Commissioner has directed to set up a data user forum to develop its own codes of practice for adherence by data users. To date, the codes of practice for the telecommunications sector have yet to be finalised and registered with the Personal Data Protection Commissioner.

Research Objectives

1. To investigate the perspectives of telecommunications data users in addressing privacy and security issues. Perspectives sought shall include perceived risks and mitigation, industry and/or internal standards being applied, process and modes of redress for data subjects, and compliance requirements.

2. To investigate the perspectives of data subjects (telecommunications users and subscribers) on issues pertaining to privacy and security issues and the correlation with take-up and continued use of applications and services utilising data analytics.

3. To conduct a comparative review of codes of practices and standards being used by local and international telecommunications providers and recommend potential areas for improvement and/ or adoption.

LITERATURE REVIEW

Big Data Adoption Challenges in Telecommunications Services: Data Users' Perspectives

Privacy and security challenges in big data adoption have been discussed in many pieces of literature. However, apart from Chua (2015), there is a general lack of research that empirically investigates the security and privacy challenges for data subjects or subscribers and how they are related to big data adoption in telecommunications services. Figure 2.1 illustrates the classification of related security and privacy challenges of big data adoption found in the literature. The classification of the challenges is done from the context of the Technological, Organisational and Environmental (TOE) framework (Tornatzky et al., 1990). The mapping of studies in privacy and security challenges in big data adoption is shown in Figure 1.

In the technological context, most issues revolve around the need for strong security and privacy solutions to protect the high volume of data that is collected in a distributed manner. The issue of ineffective scalable privacy-preserving mechanisms (Cuzzocrea, 2014; Salleh, 2016) is also a big challenge, particularly during data mining and data analysis, where the data could easily be exploited by malicious data users. The organisational context can be referred to as 'organisational security practice and culture, security planning, and risk mitigation strategies' (Salleh, 2016). In the organisational context, addressing organisational culture (Hardy, 2017; Salleh, 2016) is very important to shape an organisation's security practices. The skills shortage (Malaka & Brown, 2015; Hardy & Maurushat, 2016; Salleh, 2016) is another organisational-related issue that needs to be solved. In the environmental context, the most widely cited issues are the lack of relevant laws and regulations (Leonardo, 2012; Fang et al., 2016; Ardagna, 2016). The responsibility for ensuring the mitigation of security and privacy risks relating to big data requires international collaboration across governments and international organisations.

FIGURE 1: MAPPING OF STUDIES IN PRIVACY AND SECURITY CHALLENGES IN BIG DATA ADOPTION

Context	Sub-Category		Leonardo (2012)	Cuzzocrea (2014)	Malaka (2015)	Chua (2015)	Aditya (2016)	Fang (2016)	Ardagna (2016)	Hardy (2017)	Salleh (2016)
Technical Context	Infrastructure Security	Secure computing in distributed frameworks			√		√	√	√		√
		Secure scheme for non relational data storage		√			√	√	√		√
	Data Management	Secure data storage and transactions logs	√	√	√		√	√			
		Granular audits					√	√			
		Data provenance			√	√	√	√	√		√
		Data usability							√		
		Analytics accuracy			√	√			√		
	Data Privacy	Scalable and compostable privacy preserving for data mining and analysis		√			√	√			√
		Mandatory encryption for data-centric security	√				√	√		√	
		Granular access control	√	√	√	√	√	√	√	√	
	Integrity and reactive security	End-point input validation/filtering			√		√	√			
		Real-time security monitoring					√				√
Organisational Context		Organisation Culture								√	√
		Skill Shortage			√						√
		Organisation compliance						√		√	
		Demographic inequality				√		√			
Environmental Context		Relevant law & regulation	√	√		√		√	√	√	√
		Outsourcing and use of 3rd party tools			√						√
		Unethical interpretation				√					√

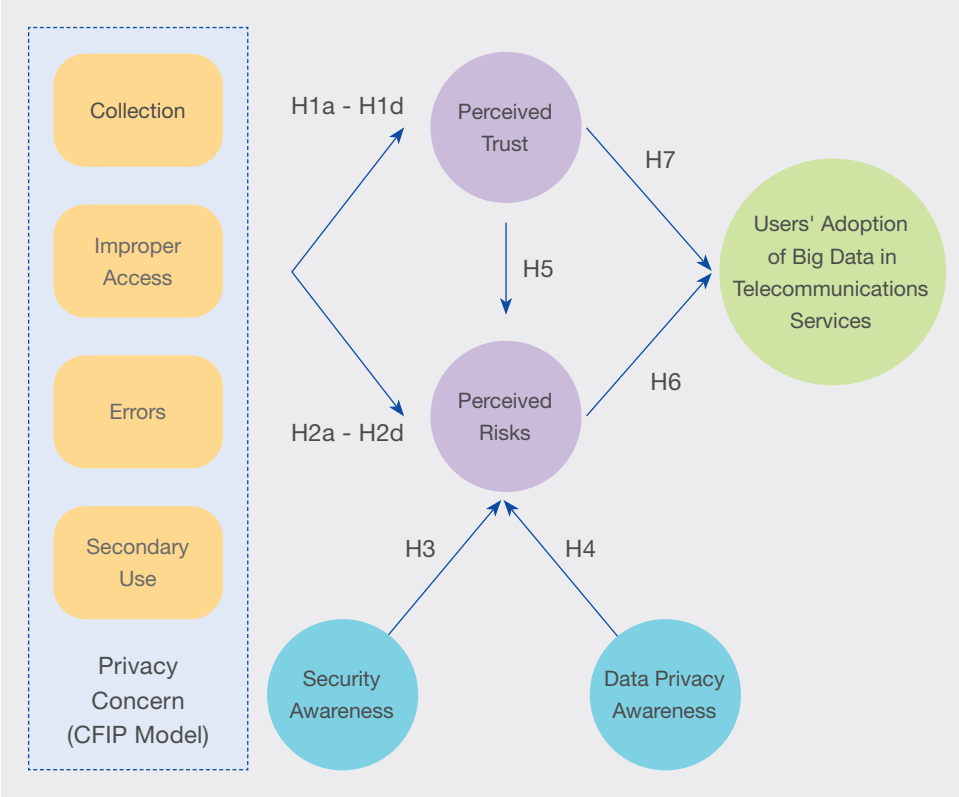
LITERATURE REVIEW

Big Data Adoption Challenges in Telecommunications Services: Data Subjects' Perspectives

Security and data privacy are crucial challenges in big data adoption among data subjects since they include personal and sensitive information about customers. Crawford and 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. Another security and data privacy concern in big data is regarding the accuracy of data. Telecommunications 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.

Figure 2 presents the theoretical framework for this study. The operational definition of each construct in the proposed model is presented in Section 5.2. The important aspect of the proposed theoretical model is the assumption that there are two (2) pathways to the adoption of big data in telecommunications services, which is via perceived trust or perceived risks in the services. From the related work and previous studies, a list of variables is identified which suits 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 telecommunications services are identified.

FIGURE 2: THEORETICAL FRAMEWORK FOR USERS' ADOPTION OF BIG DATA IN TELECOMMUNICATIONS SERVICES



The theoretical framework for data subjects' adoption of big data in the telecommunications industry is proposed based on the Concern for Information Privacy (CFIP) Model and Trust, Confidence, and Cooperation (TCC) Model. In addition, the variables security and privacy awareness are added into the proposed model. The CFIP model was first developed by Smith et al. (1996) to measure individuals' concerns regarding organisational practices. CFIP consists of four dimensions of information privacy concerns: collection, errors, secondary use, and unauthorised access to information. Users with a high level of privacy concerns will doubt the trustworthiness of the telecommunications service provider.

LITERATURE REVIEW

On the other hand, the 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 a detrimental effect (Peter & M. J. Ryan, 1976). Based on previous studies in risk management, the relation between trust and risk is stronger (Larson et al., 2018). It is also found that trust significantly affects perceived risk, and both factors further determine user behaviour (Zhou, 2011). Telecommunications service providers who have successfully developed traditional or online channels will have an edge in gaining user trust. Security awareness is a state where individuals are aware of and ideally committed to their security mission (Al-Daeef et al., 2017). In contrast, data privacy awareness reflects how clearly users understand how their data is handled and processed by used applications (Chrysakis et al., 2021). 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).

The hypotheses of this study are as follows:

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

Hypothesis 2(a-d): The effect of CFIP antecedents towards users' adoption would be mediated by Perceived Risk.

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

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

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

Hypothesis 6: Perceived Trust would significantly predict Users' adoption.

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

METHODOLOGY

The proposed study will be conducted using mixed-methodology, qualitative and quantitative methodology. The research study is designed based on the mapping of the research objective, research phase, and main research deliverables. Each phase will be conducted concurrently and independently of each other. The mapping is summarised in Table 1.

TABLE 1: RESEARCH DESIGN

RESEARCH PHASE	RESEARCH ACTIVITIES	RESEARCH OBJECTIVE	RESEARCH DELIVERABLE
Phase 1: Qualitative Study	• Literature review • Interview instrument design • Data collection (Focus Group) • Data reduction • Data display • Conclusion drawing	Objective 1	Deliverable 1 Big data adoption assessment for Data Users
Phase 2: Quantitative Study	• Survey instrument design • Content validation • Forward-backward translation • Pilot study • Perform data collection using proportional quota sampling • Construct validation • Descriptive analysis • Path analysis	Objective 2	Deliverable 2 Big Data adoption assessment for Data Subjects

METHODOLOGY

RESEARCH PHASE	RESEARCH ACTIVITIES	RESEARCH OBJECTIVE	RESEARCH DELIVERABLE
Phase 3: Systematic Review	• Region and telco providers identification • Data collection: Code of practice and privacy notice collection • Review principles and features determination • Feature extraction: Content • Features classification	Objective 3	Deliverable 3 Privacy Notice Assessment for local and international telecommunications providers

FINDINGS AND ANALYSIS

Specific Research Question 1

Instrument Design and Data Collection

The focus group interview instrument has been designed according to the technological, organisational, and environmental (TOE) framework. A focus group protocol and interview questions have been developed based on the following sub-research questions:

RQ1a:
What are the perceived security and privacy risks and mitigation strategies by the telecommunications provider for big data adoption?

RQ1b:
What are the industry and/or internal standards being applied as mitigation strategies?

RQ1c:
What are the compliance requirements (external and internal) being applied in the organisation?

Before recruitment, field expert screening is done according to age (35-45 years old), gender, occupation (upper management and senior positions), and previous experience in cybersecurity and big data projects in Malaysia's four telecommunications operators. The recruitment process is done by sending an invitation to the representatives of the telecommunications providers using convenient sampling. Participant profiles are created based on the basic background questions before the interview is conducted. Ethics approval is obtained from the research ethics committee at Universiti Teknikal Malaysia Melaka. Although the chances are very small, there is a risk that someone could get access to the data being stored. The risk may include reputational harm, losing customers, fears of misuse of the information, and strong emotional relatedness to the organisational data.

All interviews are video-recorded and then transcribed verbatim and conducted in English. The data is analysed using NVIVO 1.6 software. The focus group session is conducted in two modes: a virtual interview and an email interview. The virtual interview is approximately one (1) hour and 30 minutes in length and is recorded for analysis purposes. The email interview is the follow-up question from the focus group session.

FINDINGS AND ANALYSIS

To address RQ1, three (3) main analyses are performed on the focus group data, namely data reduction, data display, and conclusion drawing. In the data reduction phase, first cycle coding and pattern coding are conducted. The first cycle coding uses a mix of in vivo, process, and descriptive coding approaches. To ease the coding process, a deductive coding method is applied, whereby a 'start list' of codes was first developed based on the emerging themes and concepts from the literature review. In the pattern coding stage, the large number of coding in the start list was revised again into a smaller analytical unit to see whether it possessed structural unity. All first cycle codes were transferred into nodes in NVIVO 1.6 to generate the Pattern codes. Later, a group of prominent themes emerged from each of the sub-research questions to present and organise the data display. In the conclusion drawing phase, the relationship of the selected themes with the research questions is observed and interpreted.

RQ1a: What are the perceived security and privacy risks and mitigation strategies by the telecommunications provider for big data adoption?

14 themes were found to address sub-research question 1a. The themes are categorised under the context of technological challenge (4 themes), organisational challenge (2 themes), environmental challenge (3 themes), and mitigation strategies (5 themes). The explication for each theme is summarised in Table 2. The number in parentheses () indicates the number of references in the focus group data. From the findings, the Data Management theme is of highest concern, followed by Data Privacy, Data Compliance, and Data Governance, respectively.

In this study, the researchers have concurred that the three TOE challenges do influence big data adoption, and the findings show that there are distinctive challenges pertaining to the telecommunications industry in Malaysia. The salient themes shown in Table 2 have emerged from the collective opinions of the participants in the focus group interview. Among the 14 challenges identified, four concurred with the original TOE framework (Tornatzky et al., 1990). These differences can be explained due to the national and industry type influences towards the adoption (Baker, 2012).

FINDINGS AND ANALYSIS

TABLE 2: SUMMARY OF EMERGING THEMES

CONTEXT	THEME	DIMENSION	EXPLICATION
Technological Challenge	Integrity and Reactive Security (7)	Advanced security analytics (3)	Real-time threat detection tool with enhanced network-based security analytics and forensics.
		Reactive security (1)	A measure was taken based on detected threats from real-time monitoring.
		Security automation (3)	Security tools and technology that monitor, detect, troubleshoot, and remediate cyber threats without human intervention.
	Data Management (16)	Data over-collection (1)	Collection of users' data more than its original function while within the permission scope.
		High volume (3)	A large number and diverse sets of data from multiple sources.
		Data discrimination (1)	A bias occurs when predefined data types or data sources are intentionally or unintentionally treated differently from others.
		Data integration (2)	Process of bringing data from disparate sources together to provide users with a unified view.
		Data quality and usability (6)	The ability of data users to derive useful information from data.

FINDINGS AND ANALYSIS

CONTEXT	THEME	DIMENSION	EXPLICATION
Technological Challenge	Data Privacy (14)	Data anonymisation (3)	Process of masking personally identifiable information with an irreversible value from datasets.
		Data encryption (2)	Process of encoding data from plaintext (unencrypted) to ciphertext (encrypted) to protect data confidentiality.
		Granular access control (8)	The practice of granting different levels of access to a particular resource to a particular user.
	Data Compliance (13)	Comp-Data collection (6)	The practice of ensuring the process of data collection is following legal requirements.
		Comp-Data injection (3)	The practice of ensuring the process of data injection is following legal requirements.
		Comp-Secondary use (4)	The practice of ensuring the use of personal information is following legal requirements and is within what has been authorised.

FINDINGS AND ANALYSIS

CONTEXT	THEME	DIMENSION	EXPLICATION
Organisational Challenge	Data Governance (9)	Data stewardship (5)	Responsibility for assuring that the right data gets to the right processes/ parties in the proper format and is compliant with the regulations.
		Data transposition (2)	Process of restructuring values or shape of dataset.
	Subject Matter Expert (1)		Professionals who have advanced and specialised knowledge in the field.
Environmental Challenge	Competition Intensity and Market Structure (1)	Competition intensity (1)	The degree of rivalry between providers within the telecommunications industry.
		Market structure (2)	The number of providers and their market share.
	Relevant Laws and Regulations (6)	Regulatory change (1)	Any regulatory changes at a national and regional level that substantially affect the industry.
		Regulatory orchestration (5)	A form of regulatory actors' engagement with industry players at different levels to address a target in the pursuit of public goals.

FINDINGS AND ANALYSIS

CONTEXT	THEME	DIMENSION	EXPLICATION
Environmental Challenge	Technological Support (2)	Vendor support (1)	The availability and ability of vendors to fulfil the implementation and use of a given technology.
		Open Source (1)	Open and publicly available tools and software.
Mitigation Strategies	Advanced Security Tools		Real-time threat detection tool with enhanced network-based security analytics and forensics.
	Security Talent Development		The development of an employee's human capital as a resource for improving professional skills and quality in the security domain.
	Continuous Security Assessment	Security assessment	Process of comprehensively analysing and evaluating the security attributes of the business operation.
		Audit	Examination of the practices, procedures, technical controls, personnel, and other resources that are leveraged to manage companies' security risks and assure that they adhere to best practices.

CONTEXT	THEME	DIMENSION	EXPLICATION
Mitigation Strategies	Security Plan	Key performance indicator (KPI)	A set of quantifiable measures to evaluate organisational success in meeting the strategic goal.
		Strategic roadmap	A plan that defines the organisation's objectives, strategies, and pathways for the future.
	Security Culture Promotion	Awareness programme	Activities that are designed to influence employees' secure behaviour by promoting understanding of endpoint security.
		Awareness training	Activities that are designed to influence employees' secure behaviour by introducing knowledge, skills, and competence of endpoint security.
		Leadership support	The organisation attitudes and behaviours of the top management in providing support and required direction to employees.

FINDINGS AND ANALYSIS

When we compare the emerging themes found in this study with the literature review, our findings differ slightly from the initial categorisation of security and privacy challenges found in the literature review of technological, organisational, and environmental (TOE) contexts. New themes have been added to reflect the analysis of the focus interview. Data Compliance categories have been added in the technological challenge, while Infrastructure Security themes have been removed from the category. Data Governance has emerged as a new theme in the organisational context; while under the environmental context, Competition Intensity and Market Structure themes have been included.

There are some themes from our initial study in the literature that have been removed from the final findings. Although big data requires organisation-wide adoption, the findings show that very few themes were extracted under organisational challenge. On the other hand, considering the uncertainty of the political landscape in Malaysia and the global COVID-19 pandemic situation, it is expected that geopolitical factors may have a significant effect on big data adoption in the telecommunications industry. Surprisingly, this study found that the telecommunications industry does not regard geopolitical factors as a challenge.

RQ1b: What are the industry and/or internal standards being applied for the mitigation strategies?

The mapping of the industry and/or internal standards being applied by the telecommunications providers is provided in Table 3.

TABLE 3: STANDARDS BEING APPLIED FOR THE MITIGATION STRATEGIES

RISK/ CONCERN	INDUSTRY AND/OR INTERNAL STANDARDS
Data Privacy	• Data protection impact assessments (DPIA) • ISO27701 – Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • General Data Protection Regulation (GDPR)

RISK/ CONCERN	INDUSTRY AND/OR INTERNAL STANDARDS
Data Management	• Data protection impact assessments (DPIA) • ISO27701 – Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • ISO27001 – Information Security Management • Payment Card Industry Data Security Standard (PCI DSS)
Data Compliance	• Information Security Readiness Assessment • Cloud Security Alliance (CSA) practices • ISO27001 – Information Security Management • ISO27701 – Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • General Data Protection Regulation (GDPR) • Information Security Framework (ISF)
Advanced Security Technology	Critical Security (CIS) control

RQ1c: What are the compliance requirements (external and internal) applied in the organisation?

The compliance requirements applied in the telecommunications provider are presented in Table 4. The compliance requirements are classified according to internal and external requirements.

TABLE 4: COMPLIANCE REQUIREMENTS APPLIED IN THE ORGANISATION

TYPE	COMPLIANCE REQUIREMENT	DESCRIPTION
Internal	Data protection impact assessments (DPIA)	A process that is designed to identify and minimise risks associated with the processing of personal data.

FINDINGS AND ANALYSIS

TYPE	COMPLIANCE REQUIREMENT	DESCRIPTION
Internal	Information Security Readiness Assessment	Assessment mechanism that enables organisations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining information security readiness.
	Critical Security (CIS) control	Recommended set of actions for cyber defence that provide specific and actionable ways to stop pervasive and dangerous attacks.
	Cloud Security Alliance (CSA) practices	Best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.
	ISO27001 – Information Security Management	The framework that helps organisations establish, implement, operate, monitor, review, maintain, and continually improve an Information Security Management System.
	ISO27701 – Privacy Information Management System (PIMS)	Procedures and organisational structures that are designed to protect personal data from unauthorised access, processing, or use for purposes other than those originally given, as well as to ensure privacy data security.
	Payment Card Industry Data Security Standard (PCI DSS)	Set of security standards designed to ensure that ALL companies that accept, process, store, or transmit credit card information maintain a secure environment.
	Information Security Framework (ISF)	Documented processes that define policies and procedures around the implementation and ongoing management of information security controls.

TYPE	COMPLIANCE REQUIREMENT	DESCRIPTION
Internal	IT Audit	IT audit determines whether IT controls protect corporate assets, ensure data integrity, and are aligned with the business' overall goals.
	Security Audit	Security audit measures an information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations.
External	Personal Data Protection Act (PDPA)	The Act that regulates the processing of personal data in regard to commercial transactions.
	General Data Protection Regulation (GDPR)	The legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

Specific Research Question 2

Instrument Design and Data Collection

This study used a structured questionnaire for data collection. The sources of the items, and operational definitions of the dependent variables, independent variables, and modifying variables are shown in Table 5.

TABLE 5: OPERATIONAL DEFINITIONS AND SOURCES OF ITEMS

VARIABLES	OPERATIONAL DEFINITION	SOURCES OF ITEMS
Collection (C)	Users' concern whether their personal information is overly collected by the telecommunications service provider.	Smith et al. (1996); Stewart & Segars (2002)

FINDINGS AND ANALYSIS

VARIABLES	OPERATIONAL DEFINITION	SOURCES OF ITEMS
Improper Access (IA)	Users' concern about whether telecommunications providers fail to protect access to their personal information from unauthorised entities.	Smith et al. (1996); Stewart & Segars (2002)
Error (E)	Users' concern as to whether their personal information is appropriately protected from errors.	Smith et al. (1996); Stewart & Segars (2002)
Secondary Use (SU)	Users' concern about whether telecommunications providers use personal information for illegal or unauthorised purposes.	Smith et al. (1996); Stewart & Segars (2002)
Perceived Trust (PT)	Users' belief or confidence in telecommunications providers' trustworthiness.	Chiou (2004); Zhou (2011)
Perceived Risks (PR)	Users' expectation of losses associated with the release of personal information to the telecommunications service provider.	Pavlou & Gefen (2004); Zhou (2011)
Security Awareness (SA)	Level of knowledge and understanding regarding information security and the relevant protection mechanisms.	Alzubaidi (2021)
Privacy Awareness (PA)	Level of knowledge and understanding regarding the options for privacy available to them and the privacy practices of the telecommunications provider.	Yusoff (2011)
User Adoption (UA)	The acceptance, integration, and use of telecommunications services.	Zhou et al. (2010)

FINDINGS AND ANALYSIS

There are a total of 46 items in the survey instrument. Content validity was carried out to verify the representation and relevance of the items in measuring the variables. The questionnaire is validated by six (6) experts with minimum experience of ten (10) years. 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 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.

Respondent Profile

A total of 400 respondents participated in this study. Six (6) demographic criteria are collected, namely age, gender, monthly income, education level, areas of living, and telecommunications provider. The gender distribution was found to be **male (n=148, 37 percent)** and **female (n=252, 63 percent)**. Respondents varied from below 20 to above 65 years of age. Many of the respondents were around **20-23 years (n=191, 47.8 percent)**, followed by respondents aged **35-49 years (n=102, 25.5 percent)**, respondents aged below **20 years (n=50, 12.5 percent)** and subsequently, respondents of **50-64 years old (n=48, 12 percent)**. The fewest respondents were at the age of **above 65 years (n=9, 2.3 percent)**.

400
respondents participated in this study. Six (6) demographic criteria are collected, namely age, gender, monthly income, education level, areas of living, and telecommunications provider.

FINDINGS AND ANALYSIS

Most respondents have a monthly income of RM1,000-RM 4,850 (n=142, 35.5 percent), followed by a monthly income of RM4,851-RM10,971(n=69, 17.3 percent) and respondents with an income of RM999 and below (n=35, 8.8 percent). The fewest respondents' income was RM10,971 and above (n=32, 8.0 percent). Most respondents originated from urban areas (n=252, 65.0 percent). The rest of the respondents are from rural areas (n=148, 37.0 percent). Most respondents use Celcom as their telecommunications service provider (n=123, 30.8 percent), followed by U Mobile (n=79, 19.8 percent), Maxis (n=60, 15.0 percent), Digi (n=52, 13.0 percent), Unifi Mobile (n=40, 10 percent), TuneTalk (n=19, 4.8 percent) and redOne (n=18, 4.5 percent). The least number of respondents were using other telecommunications service providers (n=9, 2.3 percent).

Descriptive Analysis

This section presents the findings of the descriptive analysis for each variable in this study. Eight (8) variables are used in this study namely, collection, improper access, errors, secondary use, perceived trust, perceived risks, security awareness, data privacy awareness and user adoption. The results reveal that the highest privacy concern among data subjects is about Errors. Most of the data subjects are concerned as to whether their personal information is appropriately protected to minimise accidental and intentional errors by the telecommunications service provider.

Several comparisons have been done in this study, such as comparison of gender groups, age groups, monthly income, education level and areas of living. The results for the Mann-Whitney test, which is utilised to compare two independent gender groups in the study, show that there is no significant difference for all variables across the categories of gender, age, monthly income and areas of living. However, from all variables, collection, improper access, and security awareness show significant difference across the category of education level.

Inferential Analysis

This section presents the findings of the inferential analysis in this study. 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 are a total of 33 items in independent variables after

FINDINGS AND ANALYSIS

EFA was carried out. Two (2) items were removed from the survey instrument. All items were grouped into eight factors based on their highest factor loadings. The extracted factor structure explained 74.1 percent of the variance, which is sufficient for social science research. None of the factors were dropped.

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 based on the guideline given by Hair Jr et al. (2021). 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 telecommunications services. Table 6 summarises the results for hypothesis testing.

TABLE 6: 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

FINDINGS AND ANALYSIS

HYPOTHESES	FROM ▶ TO	PATH COEFFICIENT			MEDIATION	RESULT
		PT	PR	UA		
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; R2 = 0.657; adjusted R2 = 0.66

Due to the increased demand for secure Big Data implementation, the telecommunications service provider needs to understand and capture the market needs pertaining to security and privacy. Therefore, this study sought to investigate the influence of security and privacy concerns on user adoption of Big Data in telecommunications services. In addition, this study investigates the effect of security awareness and data privacy awareness on user adoption.

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 telecommunications services. The influence of users' concern on collection towards Big Data adoption was fully mediated by perceived trust and perceived risk in telecommunications 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 telecommunications service provider. Besides this, the effect of users' 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 perceived trust. Therefore, H2b is not supported. The findings seem to suggest that when evaluating the potential damage from security and privacy breaches, telecommunications users are more concerned about the technical ability of the telecommunications service provider in mitigating the risks. A possible explanation for this might be due to the users' 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 the four (4) variables of security and privacy concerns, the improper access variable has a significantly higher effect on perceived trust. The findings indicate that the users feel that the telecommunications service provider is deemed trustworthy when the provider has the technical ability to protect access to their personal information from unauthorised entities. The significant relations between service providers' technical competency and customers' trust have been reviewed extensively in other industries, such as e-commerce (Connolly & Bannister, 2007) 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 previous studies (Zhou, 2011), where users feel that the telecommunications service provider is deemed trustworthy when the provider does not over-collect their personal information.

Telecommunications 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 telecommunications providers and how their data is being processed, this 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. The TCC Model (Siegrist et al., 2012) offers a possible explanation for the results. Under the condition where the perceived importance of the issue is low, and the users' awareness (i.e. knowledge) is high, trust will be irrelevant to perceived risk.

Specific Research Question 3

Online privacy regulations are notorious for their inconsistencies in appearance and content (Kaur et al., 2018; Ahmad et al., 2020). They are also difficult to comprehend, and do not adequately assist users in making informed judgements regarding internet service providers' data practices (Kaur et al., 2018). In addition, as stated in a study by Chua et al. (2017), to address concerns about data privacy, many countries in European, American, and Asian regions have enacted data protection legislation such as the European General Data Protection Regulation (GDPR), the USA Federal Trade Commission's (FTC) Fair Information Practice Principles (FIPs) and the UK Data Protection Act 2018

FINDINGS AND ANALYSIS

(DPA). In Malaysia, this legislation is known as The Personal Data Protection Act 2010 (PDPA, 2010), and was enforced in November 2013.

In each piece of legislation, several principles exist that differ in name but refer to the same underlying idea. Therefore, this research focused on the review of codes of practice and privacy notices, based on PDPA principles and its features, as summarised in Table 7. The table shows the features identified from the PDPA and used in reviewing the Telecommunications code of practice and privacy notice. The scopes of the codes of practice and privacy notices are also extracted and named as General principles. They consist of two (2) features: a) Personal data is adequate, relevant, and not excessive; and b) Personal data is processed with consent and for lawful purposes.

TABLE 7: PDPA PRINCIPLES' FEATURES

PRINCIPLES	FEATURES
Notice and Choice	1. Purpose personal data is processed 2. Purpose personal data is collected 3. Purpose personal data is disclosed 4. Notice Cancellation
Disclosure	Individual consent about their personal data
Security	1. Protect personal data from loss 2. Protect personal from misuse 3. Protect personal data from unauthorised access 4. Protect personal data from other incidents
Retention	1. How much personal data is retained 2. How long does it take 3. How to store the personal data 4. Personal data handling after the retention period
Data Integrity	1. Personal data is accurate / not altered 2. Personal data is up to date 3. Personal data is verifiable
Access	The rights to the personal data

FINDINGS AND ANALYSIS

In this research, the comparative review was carried out based on three (3) main regions, namely Asia, Europe, and America. On top of the regions reviewed, seven telecommunications providers were selected to be reviewed in terms of their privacy policy notices that are published publicly. They are Maxis, Celcom, Digi, TM ONE, Verizon, AT&T, Vodafone and Deutsche Telekom AG. In this research, the sample was taken between 22 July 2021 and 10 August 2021. Updates made after 10 August 2021 will not be reflected in our reviews. Owing to the PDPA's effective date on 15 November 2013, we assume that most companies would have had enough time to complete their privacy notices before our data collection period.

Table 8 summarises the features that exist in the privacy notices from the selected telecommunications organisations. Based on the analysis, Table 8 shows the issue discovered with regard to the Retention principle. Three of the selected Telcos did not disclose anything about retention features. From our review, it is discovered that many companies, especially in Malaysia, rarely revise their privacy notices after they have been publicly published to customers. The findings also discovered that some of the rules are unclear in the privacy notice or code of practice and need further investigation. For example, in the AT&T Privacy Policy, the retention segment is unclear in terms of the process. In TM ONE and Maxis' privacy notices, three retention features are not stated, except for the how to store the personal data feature. Another reason that the privacy notices are unclear is because the term used for the notice cancellation feature stated in the privacy notices is different among telecommunications organisations. For example, the term 'opt-out' is used by Digi and Celcom to describe the cancellation notice to their users, whereas for Maxis, users need to understand the whole statement in the notice.

Based on the research findings, most privacy policies are drafted to shield organisations from potential privacy litigation, rather than to address consumers' privacy notice (Earp et al., 2005). This indicates that there is no standard for what and how privacy notices should be disclosed on a website, although most legislation require organisations to provide notices informing customers about their privacy practices (Chua et al., 2017). Hence, most organisations choose the content of the policy that has the most influence on their customers. Meanwhile, Scaub et al. (2017) and Ebert et al. (2021) stated that due to the complexity and indiscernibility of the privacy notice design, the privacy practices do not provide actual transparency to customers as the telecommunications organisation's objective in publishing a privacy notice is to meet the letter of the law.

FINDINGS AND ANALYSIS

TABLE 8: COMPARATIVE REVIEW RESULT ANALYSIS

REGULATORY	SOURCES	COUNTRY / REGION	PROVIDERS	PRINCIPLES OF DATA PROTECTION						
				GENERAL		NOTICE AND CHOICE (INFORM THE PURPOSE OF PERSONAL DATA)				DISCLOSURE
				Personal data adequate relevant & not excessive	Processed with consent and for a lawful purposes	Purpose of personal data is processed	Purpose of personal data is collected	Purpose of personal data is disclosed	Notice cancellation	Individual consent about their personal data
General Consumer Code (GCC), Personal Data Act 2010 (PDPA)	Privacy Notice	Malaysia / Asia	Maxis	√	√	√	√	√	√	√
			Celcom	√	√	√	√	√	√	√
			TM	√	√	√	√	√	√	√
			Digi	√	√	√	√	√	√	√
USA Federal Trade Commission (FTC)'s Fair Information Practice Principles (FIP)	Privacy Notice	USA / North America	AT&T	√	√	√	√	√	√	√
			Verizon	√	√	√	√	√	√	√
European General Data Protection Regulation (GDPR), Data Protection Act (DPA)	Privacy Policy	UK / EU	Vodafone	√	√	√	√	√	√	√
	Rules Privacy	German / EU	Deutsche Telekom AG	√	√	√	√	√	√	√

Notes: √ denotes the existence of the features, × denotes features that may exist but are unclear, unknown or not mentioned

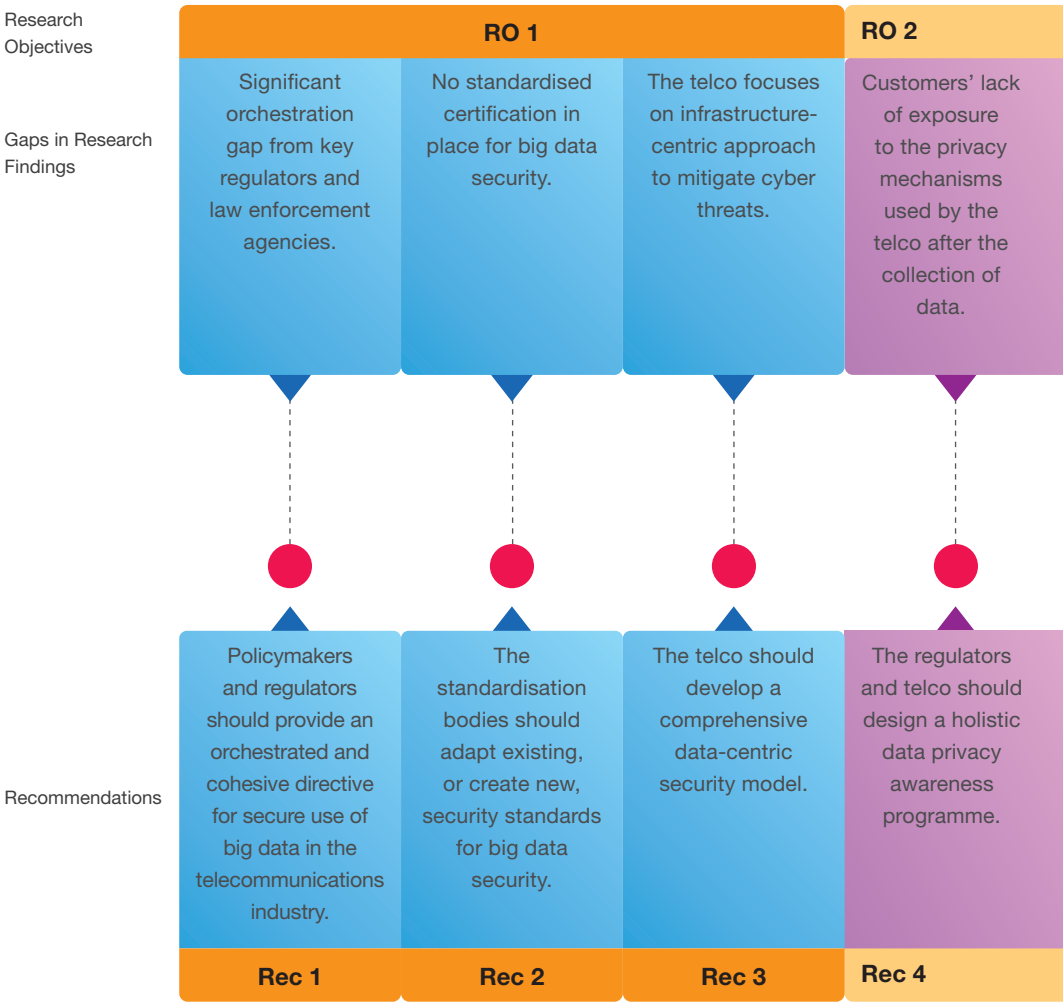
FINDINGS AND ANALYSIS

	SECURITY				RETENTION				DATA INTEGRITY			ACCESS
	Protect personal data from loss	Protect personal data from misuse	Protect personal data from unauthorised access	Protect personal data from others incident	How much to retain the personal data	How long does it takes	How to store the personal data	Pd handling after retention period	Personal data is accurate / not altered	Personal data is up to date	Personal data is verifiable	Rights to personal data
	√	√	√	√	x	x	√	x	√	√	√	√
	√	√	√	√	x	√	√	√	√	√	√	√
	√	√	√	√	x	x	√	x	√	x	√	√
	√	√	√	√	√	√	√	√	√	√	√	√
	√	√	√	√	√	√	√	√	√	√	√	√
	√	√	√	√	√	√	√	√	√	√	√	√
	√	√	√	√	√	√	√	√	√	√	√	√
	√	√	√	√	√	√	√	√	√	√	√	√

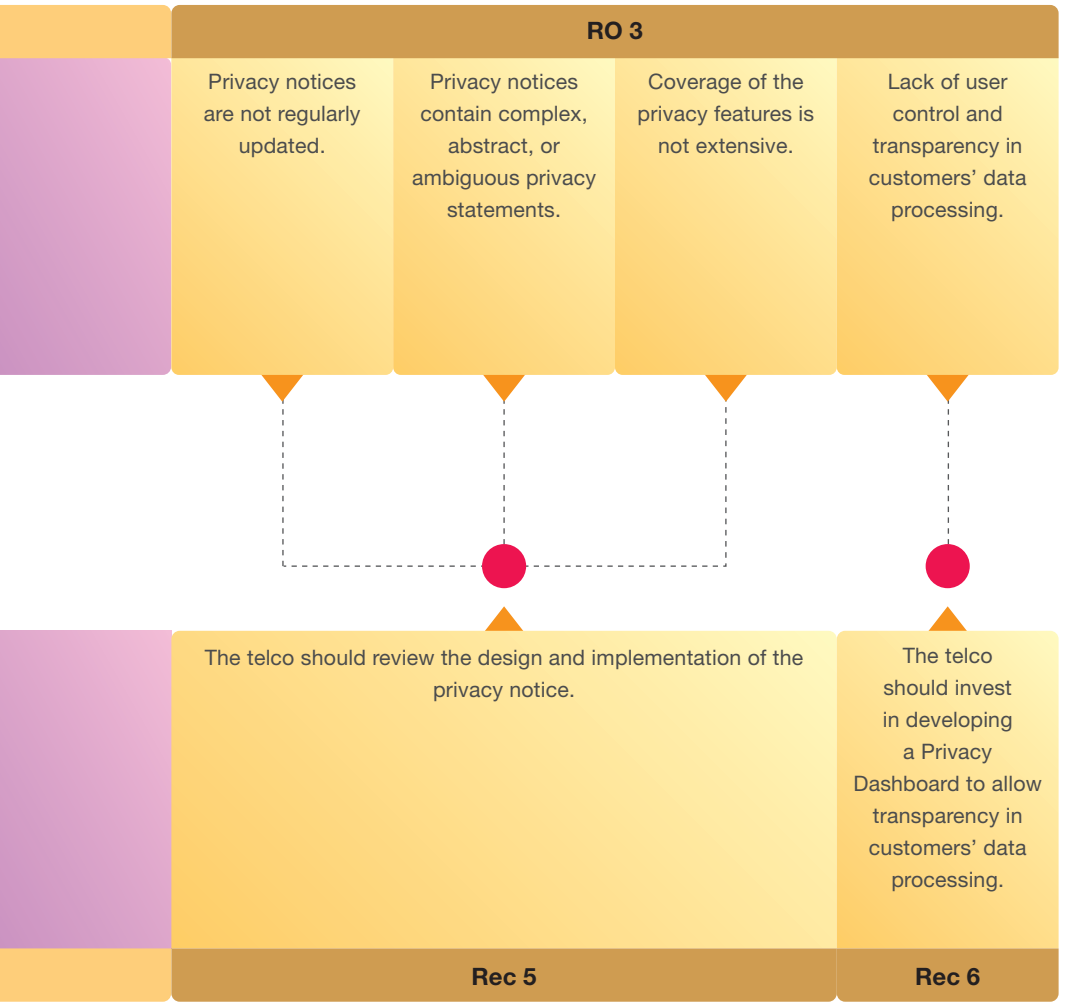
RECOMMENDATIONS

Based on the research findings, several gaps have been identified. In this section, we propose recommendations to address the gaps, as outlined in Figure 6.1.

FIGURE 6.1: MAPPING OF RECOMMENDATIONS TO GAPS IN RESEARCH FINDINGS



RECOMMENDATIONS



RECOMMENDATIONS

Recommendation 1: Policymakers and regulators should focus on providing an orchestrated and cohesive directive for secure use of big data in the telecommunications industry.

The telecommunications industry faces a significant orchestration gap from all key regulators and law enforcement agencies. Malaysia's telecommunications industry requires one party to act as an orchestrator to bridge the gap. All stakeholders participating in the publication of guidelines should tackle big data security holistically. Security and privacy must be considered not only in terms of static regulatory compliance, but must also be inclusive of the development of the industry's best practices for secure big data management.

Recommendation 2: The standardisation bodies should adapt existing, or create new, security standards for big data security.

There is currently no standardised certification in place for big data security. Adapting or adopting standards will aid the industry's growth while also improving user service. Therefore, standardisation bodies should form industry groupings that consist of big data providers, users, and regulators from relevant industries to develop uniform standards and certifications.

Recommendation 3: The telecommunications provider should develop a comprehensive data-centric security model.

Telecommunications providers are leaning towards an infrastructure-focused approach to mitigate cyber threats and cyberattacks. Findings indicate that the data subject's concern on data error directly influences big data adoption of telecommunications services. Telecommunications providers need to shift the focus of their security solutions with the aim of securing and protecting their customers' data. This includes investing in advanced automated security solutions for data anonymisation, data encryption, data tagging, data classification, data governance, and data compliance.

RECOMMENDATIONS

Recommendation 4: Regulators and telecommunications providers should design a holistic data privacy awareness programme.

Data subjects often assume that the data that has been collected by the telecommunications provider is not stored and processed properly. Therefore, regulators and telecommunications providers are responsible for making data subjects aware on how data is stored and processed by the telecommunications provider and the regulations it is bound to through their privacy notices. Regulatory agencies such as CyberSecurity Malaysia (CSM), Malaysian Communications and Multimedia Commission (MCMC) and National Cyber Security Agency (NACSA) need to sit down with telecommunications providers to discuss privacy issues that often occur among data subjects and cooperate to design and organise privacy awareness programmes. The aspect that needs to be emphasised is empowering individuals and telecommunications providers to respect privacy, protect data, enable trust, raise awareness, and promote privacy and data protection best practices.

Recommendation 5: Telecommunications providers should review the design and implementation of the privacy notice.

a. Update the privacy notice frequently and improve principal features

Many telecommunications providers rarely revise their privacy notices to reflect current risks. We suggest that the privacy notices should be regularly updated. We also propose adding a feature to the Retention principle, which is the step taken in handling personal data after the retention period, to improve data processing transparency and subsequently gain more trust in using the services.

b. Reduce the complexity and increase the readability of privacy notice content

Current privacy notices contain complex, abstract, or ambiguous privacy statements. We suggest using GDPR as the guideline for developing the privacy rules or notices because GDPR includes a comprehensive feature considered within business processing activities by design and by default.

RECOMMENDATIONS

Recommendation 6: Telecommunications providers should invest in developing a Privacy Dashboard to allow transparency in customers' data processing.

Telecommunications providers have to protect and respect their customers' privacy, including the choices they make on the use of their data. We recommend that telecommunications providers invest in developing Privacy Dashboards to allow transparency in the customers' data processing. Data subjects can view a summary of their collected information, get a copy of their information, and remove unnecessary information, as demonstrated by the Verizon Dashboard (Verizon, 2022). We also suggest an infographic data protection and data security portal be developed by providers to educate and provide awareness to their customers that is easy to access, manage, and understand, as published on Telekom AG's portal (Deutsche Telekom, 2022).

CONCLUSION

This study is significant in that it provides empirical evidence, where two (2) independent empirical studies jointly provide empirical support for the perspectives of telecommunications data users and data subjects in addressing privacy and security issues that are related to big data adoption. The outcomes of this study may serve as guidelines for regulators, telecommunications providers, and stakeholders for securing big data systems and for promoting security best practices within telecommunications industry operations.

This study offers contributions in three (3) major aspects. First, this study presents a thematic classification of security and privacy challenges and their mitigation strategies for big data adoption in the telecommunications industry. The thematic classification highlights potential gaps for future research in the big data security domain. Next, this study proposes an extended Concern for Information Privacy (CFIP) framework to address security and privacy concerns and awareness, and their association with big data adoption in telecommunications services. The extended CFIP framework may provide insights to telecommunications providers on how to alleviate data subjects' privacy concerns in order to encourage their

adoption and usage of telecommunications services. Finally, this study explores the potential gaps in codes of practice and standards being used by local and international telecommunications providers for future improvements.

REFERENCES

- *Ahmad, W. U., Chi, J., Tian, Y., & Chang, K. W. (2020). Policy QA: A reading comprehension dataset for privacy policies. Findings of the Association for Computational Linguistics: EMNLP 2020, November 16 - 20, 2020, Pp. 743–749.*
- *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).*
- *Ardagna, C. A., Ceravolo, P., & Damiani, E. (2016, December). Big data analytics as-a-service: Issues and challenges. In 2016 IEEE international conference on big data (big data) (pp. 3638-3644). IEEE.*
- *Baker, J. (2012). The technology–organization–environment framework. Information systems theory, 231-245.*
- *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 inBioinformatics), 12840 LNCS, 259–277.*
- *Chua, H. N., Chang, Y., Wong, S. F., & Tan, C. M. (2015). Privacy protection policy for big data analytics in the Malaysian telecommunications sector, In Proceeding of the 26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24th-27th June, 2015, Pp. 1-14.*
- *Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telematics and Informatics,Volume 34, No 4, Pp. 157-170.*

REFERENCES

- *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*
- *Cuzzocrea, A. (2014, November). Privacy and security of big data: current challenges and future research perspectives. In Proceedings of the first international workshop on privacy and securityof big data (pp. 45-47).*
- *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.*
- *Deutsche Telekom AG 9 (n.d). [Accessed on 29 March 2022 from https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/your-data-at- dt].*
- *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).*
- *Earp, J.B., Antón, A.I., Aiman-Smith, L., Stufflebeam, W.H., 2005. Examining Internet privacy policies within the context of user privacy values. IEEE Trans.*
- *Ebert, N., Alexander Ackermann, K., & Scheppler, B. (2021, May). Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Pp. 1-12.*
- *Fang, W., Wen, X. Z., Zheng, Y., & Zhou, M. (2017). A survey of big data security and privacy preserving. IETE Technical Review, 34(5), 544-560.*
- *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.*
- *Hardy, K., & Maurushat, A. (2017). Opening up government data for Big Data analysis and public benefit. Computer law & security review, 33(1), 30-37.*
- *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*

REFERENCES

- *Leonardo A, M., Albin, Z., Smeets, B., Sheikh M, H., Johansson, T., & Nahid, S. (2012). Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry. In The Third International Symposium on Multidisciplinary Emerging Networks and Systems (MENS2012). IEEE-Institute of Electrical and Electronics Engineers Inc..*
- *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.*
- *Narayanan, A., & Shmatikov, V. (2008, May). Robust de-anonymization of large sparse datasets. In 2008 IEEE Symposium on Security and Privacy (sp 2008) (pp. 111-125). IEEE.*
- *Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15(1), 37–59.*
- *Personal Data Protection Act 2010, Laws of Malaysia Act 709, [Accessed on 10 August 2021 from https://www.pdp.gov.my/jpdpv2/akta-709/personal-data-protection-act-2010/], Pp. 1-52.*
- *Peter, J. P., & M. J. Ryan. (1976). An investigation of perceived risk at the brand level. Journal of Marketing Research, 13(2), 184–188.*
- *Salleh, K. A., & Janczewski, L. (2016). Technological, organizational and environmental security andprivacy issues of big data: A literature review. Procedia computer science, 100, 19-28.*
- *Schaub, F., Balebako, R., & Cranor, L. F. (2017). Designing effective privacy notices and controls. IEEEInternet Computing, Pp. 1-12.*
- *Siegrist, M., Earle, T. C., & Gutscher, H. (2012). Trust in cooperative risk management: Uncertainty andscepticism in the public mind. In Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind*
- *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 HumanBehavior, 32, 15–22. https://doi.org/10.1016/j.chb.2013.11.008*
- *Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 167-196.*
- *Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36-49.*

REFERENCES

- *Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). Processes of technological innovation. Lexington books.*
- *Verizon Privacy Dashboard (n.d). [Accessed on 14 January 2022 from https://www.verizon.com/privacy/your-data].*
- *Wang, Z., Wei, G., Zhan, Y., & Sun, Y. (2017). Big data in telecommunication operators: data, platform,and practices.*
- *Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronicbanking. ,. Technovation, 23(11), 847–860.*
- *Yusoff, Z. M. (2011). The Malaysian personal data protection act 2010: A legislation note. NZJPIL,9(119).*
- *Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. IndustrialManagement and Data Systems, 111(2), 212–226.*
- *Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking useradoption. Computers in Human Behavior, 26(4), 760–767.*