Exploring the privacy concerns of smartphone app users: A qualitative approach

EXPLORING THE PRIVACY CONCERNS OF SMARTPHONE APP USERS: A QUALITATIVE APPROACH

Abstract

Purpose- The purpose of this study is to explore and identify the privacy concerns of smartphone app users pertinent to app usage.

Design/methodology- Adopting a qualitative phenomenological approach, we conducted semi-structured interviews with app users to explore their privacy concerns.

Findings- Credibility concerns, unauthorised secondary use, and vulnerability concerns are the three major privacy concerns of app users under which they have sub concerns, i.e., popularity, privacy policy, stalking, data sharing, hacking, and personal harm.

Practical implications- The findings are useful to app marketers, app developers, and app stores. They can use the findings to understand and properly address app users' privacy concerns thereby increasing the apps usage.

Originality/value- By exploring the privacy concerns of app users, our study extends the literature and provides a theoretical development of individuals' privacy concerns in the context of a widely used technology, i.e., smartphone applications. Accordingly, this study contributes to the consumer privacy literature.

Keywords: *Smartphone apps, privacy concerns, thematic analysis, qualitative*

1. INTRODUCTION

Smartphones are providing remarkable services to their users through various applications (apps) (Gokgoz, Ataman, & van Bruggen, 2021; Ho & Chung, 2020; Shankar et al., 2022). Smartphone users download and install various apps for use in their daily lives. The smartphone application market has experienced an enormous growth since its outset (Adil et

al., 2022; Ho & Chung, 2020), and in 2016, the global market size of this industry was $108,440 million and projected to reach $311,249 million by 2023 at a compound annual growth rate of 19.2% (Namde, 2017). These applications are used for many purposes, for example, for checking weather updates, making video calls, sending text and voice messages, reading e-newspapers, taking and editing pictures, securing mobile phones with app locker applications, and much more (Chen & Hsieh, 2012; Jingjun, Liao, & Li, 2008; Persaud & Azhar, 2012).

Smartphone applications require various permissions from users to access their personal information, for example, location, identity, photos/media, device and call information, app history, camera, Wi-Fi connection information, microphone, contacts and so on (Chen & Hsieh, 2012; Cheung, 2014; Maseeh, 2022). For example, location information is necessary for weather applications to provide exact weather conditions at a specific geographical location (Degirmenci, 2020; Jengchung et al., 2008). However, privacy concerns arise when users may become suspicious about the usage and storage of such information by another party (Degirmenci, 2020; Gu, Xu, Xu, Zhang, & Ling, 2017; Harris, Brookshire, & Chin, 2016; Maseeh et al., 2022; Varnali & Toker, 2010). When such notifications appear on the mobile screen, users might be reluctant to allow the app to access their location and/or personal information and may choose to not install the app (Boyles, Smith, & Madden, 2016; Jengchung et al., 2008).

People are suspicious about sharing their personal information with smartphone applications. Identity theft is a major concern, and it is a hard decision for smartphone users to share their personal information due to major privacy issues which could become a security threat (Ashaduzzaman et al., 2022; Jengchung et al., 2008). For example, app developers can continuously track users' location via some applications (e.g., weather app), where such information could be misused by service providers/app developers (Farnden, Martini, & Choo, 2015) or could be communicated to a harmful third person (Wall, 2007) with smartphone users

becoming victims of criminal activities. For example, robbery, sexual assault and murder cases have been committed by tracking app users' location information (Koubaridis, 2014; Wilson, 2014). Furthermore, users' private pictures and videos can be retrieved through apps, and used for illegal and unethical purposes (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

Although research has shown that privacy concerns influence users' behavioural intentions in the context of smartphone applications, individuals' privacy concerns pertinent to smartphone app usage remain unexplored. That is, researchers have adopted the constructs from the literature related to the other domains of privacy, such as internet users' information privacy concerns (IUIPC) (Malhotra, Kim, & Agarwal, 2004) to study the impact of smartphone app users' privacy concerns on their behavioural intentions. While smartphone app users are internet users, the intensity and the nature of privacy concerns of internet users in the context of apps might be different from those who access internet via desktop or laptop computers. Accordingly, a deeper exploration of individuals' privacy concerns specific to smartphone apps remains limited. Thus, the purpose of this study is to explore and identify the privacy concerns of smartphone app users pertinent to app usage.

Qualitative research design is considered appropriate for a deeper exploration of a phenomenon, and it allows people to describe their concerns and issues in their own words (Groenewald, 2004; Mukherjee, Jebarajakirthy, & Datta, 2020). Accordingly, to explore the privacy concerns of smartphone app users, adopting a qualitative phenomenological approach, semi-structured interviews were conducted with smartphone app users recruited using judgemental sampling technique. The findings show that credibility concerns, unauthorised secondary use, and vulnerability concerns are the major concerns of smartphone app users under which they have sub-concerns, i.e., popularity, privacy policy, stalking, data sharing, hacking, and personal harm.

Our study has academic significance. Adopting a qualitative lens, we have explored and identified the privacy concerns of smartphone app users pertinent to apps which is a contribution to the privacy literature. Further, our study extends the privacy calculus theory. Privacy calculus theory posits that because of privacy concerns, individuals assess potential risks before disclosing personal information (Trepte et al., 2017), however, it does not specify what those privacy concerns are. Our study extends privacy calculus theory in the context of smartphone applications by exploring the privacy concerns of smartphone app users (i.e., credibility concerns, unauthorised secondary use, and vulnerability concerns). Practically, the findings of this study are important for multiple stakeholders. The findings are useful to app developers and app marketers in addressing smartphone app users' privacy concerns. The findings are also useful to smartphone app stores, for example, *Google Play Store* and *Apple App Store,* in developing policies to control app developers' activities and behaviours in app stores. Lastly, the findings are useful for government organisations in controlling cyber-crimes.

2. THEORETICAL BACKGROUND

2.1 Literature on smartphone apps and privacy

Privacy concerns in the context of smartphone applications have been studied in the past. Table 1 summarises the key studies carried out on privacy concerns in the context of smartphone applications.

<Table 1>

Although privacy concerns have been studied in smartphones context, there exist two significant gaps in the context of app users' privacy concerns. First, researchers have mainly studied a causal link between privacy concerns and outcome variables (e.g. intention to use mobile health services, see Guo et al. (2012)) instead of exploring app specific privacy concerns. Second, to investigate privacy concerns, researchers adopted the frameworks from the other domains (e.g., Malhotra et al., 2004). Although smartphone app users are internet

users, the intensity and the nature of privacy concerns of internet users in the context of apps might be different from those who access internet via desktop or laptop computers. This lack of knowledge engenders a need for an exploratory research approach, to identify the privacy concerns of smartphone users pertinent to smartphone apps.

2.2 Dimension of consumer privacy concerns

Consumer privacy concerns have been studied from a multidisciplinary perspective, such as law, information systems, and organisation behaviour (Caudill & Murphy, 2000; Culnan & Regan, 1995; Malhotra, Kim, & Agarwal, 2004; Smith, Milberg, & Burke, 1996). However, the dimensions of individuals' privacy concerns vary across contexts, for instance, information systems and organisation behaviour (Malhotra et al., 2004; Jebarajakirthy et al., 2023). Accordingly, researchers introduced various frameworks to understand privacy concerns. These frameworks include global information privacy concerns (GIPC), concerns for information privacy (CFIP), internet users' information privacy concerns (IUIPC), and mobile users' information privacy concerns (MUIPC). The details of these frameworks are presented in Table 2.

<Table 2>

GIPC framework has been used to examine privacy concerns in general. That is, GIPC does not examine dimensions of privacy concerns in a particular context (Malhotra et al., 2004). To address this shortcoming, Smith et al. (1996) developed a multidimensional information privacy concerns framework, i.e., CFIP. Comprising of four dimensions, i.e., collection, unauthorised secondary use, improper access, and errors, CFIP reflects individuals' concerns about organisations' practices regarding information collection. Smith et al.'s (1996) work provided a steppingstone for future work on privacy concerns. Building on Smith et al. (1996), Malhotra et al. (2004) proposed IUIPC framework to examine individuals' privacy concerns in

the context of internet services. Employing social contract theory and justice theory, Malhotra et al. (2004) proposed three dimensions of internet users' privacy concerns, namely collection of personal information, control over personal information, and awareness of organisational privacy practices. However, individuals' privacy concerns in mobile environment might differ from those of internet users. Accordingly, to understand mobile users' privacy concerns, drawing on Communication Privacy Management theory, Xu et al. (2012) proposed MUIPC framework with three dimensions; perceived surveillance, perceived intrusion, and secondary use of information.

The gradual development of the dimensions/frameworks of information privacy concerns (i.e., GIPC, CFIP, IUIPC, and MUIPC) indicates that privacy concerns evolve/transform with the development of new technology. Accordingly, the exploration of privacy concerns in the context of new technology becomes vital (Jebarajakirthy et al., 2021; Yun, Lee, & Kim, 2019). Due to a transformative nature of consumer privacy concerns, researchers call for continuous research to explore privacy concerns in various contexts (Bélanger & Crossler, 2011; Malhotra et al., 2004; Phelps, Nowak, & Ferrell, 2000; Xu, Gupta, Rosson, & Carroll, 2012; Yun, Lee, & Kim, 2019). Despite the fact that researchers have proposed various dimensions of privacy concerns, they acknowledge that *"the dimensionality is neither absolute not static, since perceptions of advocates, consumers, and scholars could shift over time"* (Smith et al., 1996, p. 190). Accordingly, scholars recommend that *"the theoretical operationalisation assumptions underlying the structure of constructs such as CFIP should be reinvestigated in light of emerging technology, practice, and research"* (Stewart & Segars, 2002, p. 37).

Smartphone app users are unable to hide their identity on internet because smartphones are identified by a unique ID (Xu et al., 2012). Accordingly, smartphone applications can collect rich customer data thereby posing privacy threats that are unique from those posed in other contexts. However, the literature on smartphone applications does not explore individuals'

privacy concerns pertinent to smartphone apps, instead, the dimensions of CFIP, IUIPC, or MUIPC are adopted to examine smartphone app users' privacy concerns which may result in biased, incomplete, and inaccurate understanding of apps users' privacy concerns. Accordingly, the current knowledge about customers' privacy concerns pertinent to smartphone apps is limited. This lack of knowledge suggests a need for exploratory research to explore and identify the privacy concerns of smartphone users.

2.3 Problem statement

Smartphone applications provide personalised services to app users by accessing their personal information, for example, location, age, gender, and so on (Sutanto, Palme, Tan, & Phang, 2013) with these apps mainly developed for personalised advertising (Dinsmore, Swani, Goodrich, & Konus, 2021; Gupta, Mukherjee, & Jayarajah, 2021; Le & Nguyen, 2014). By accessing the personal information of mobile app users, application developers try to understand their shopping interests and lifestyle. Accordingly, smartphone app advertisements are highly personalised based on app users' personal information (Meng, Ding, Chung, Han, & Lee, 2016). Advertising is a major source of income for app developers, while mobile marketing campaigns are highly dependent on smartphone applications (Dinsmore et al., 2021; Gupta et al., 2021; Kemp, 2012; Le & Nguyen, 2014) as organisations use customised marketing strategies through mobile applications (Fong, Fang, & Luo, 2015; Gupta et al., 2021; Le & Nguyen, 2014; Luo, Andrews, Fang, & Phang, 2014). However, app users' personal information can be misused and/or communicated to third parties which engenders their privacy concerns (Mehta et al., 2022; Zang, Dummit, Graves, Lisker, & Sweeney, 2015). Accordingly, the value of app marketing campaigns (from marketers' perspective) could be affected if smartphone users have privacy concerns (Jengchung et al., 2008).

2.4 Theoretical underpinnings

Privacy calculus theory explains that *"individuals determine their disclosures by assessing whether they can manage the information to be shared while minimising the negative consequences of these self-disclosures"* (Trepte et al., 2017, p. 2). This indicates that when an app asks users to share their personal information, they perform a risk-benefit analysis (Chopra et al., 2023). A main consideration for a risk-benefit analysis might be app users' privacy concerns pertinent to disclosing personal information. As such, individuals weigh potential risk of disclosure (e.g. privacy breach) against the proposed benefits (e.g. personalised services). Accordingly, their decision to disclose information and install an app is based on the outcomes of the risk-benefit analysis, i.e., if the value of benefit(s) is higher than risk(s), individuals will be prone to disclose their privacy (Smith, Dinev, & Xu, 2011). Thus, the *Privacy Calculus Theory* is appropriate for understanding app users' privacy concerns pertinent to smartphone apps.

3. METHODOLOGY

3.1 Research approach

The literature suggests employing exploratory research designs to examine a phenomenon that is not well explained (Mukherjee et al., 2020). The privacy concerns of app users need a deeper exploration which generates a need for exploratory research to unearth new themes relating to privacy concerns of app users (Johnson & Sohi, 2016). A qualitative phenomenological approach helps understand a *"phenomenon from the perspectives of people involved"* (Welman & Kruger, 1999, p. 189). Accordingly, a qualitative phenomenological approach is considered appropriate for this study as it facilitates the understanding of a concept by directly interpreting the views of study's participants.

3.2 Sampling technique, and selection of participants

Judgemental sampling technique enables identifying appropriate individuals for a study based upon their experience and knowledge, thereby providing a deeper understanding of the phenomenon (Strauss & Corbin, 1998). Hence, judgemental sampling was considered most suitable for recruiting interviewees for the current study (Palinkas et al., 2015). More than 80% of Australians own smartphone devices (Pew Research Center, 2019) with almost every Australian between the age of 14-54 years having a smartphone (Hughes, 2019). Most of the smartphone applications are installed by 18-54-year-old Australian smartphone users (Drumm, White, & Swiegers, 2016). Therefore, Australian smartphone users from this age group were approached for this research. To recruit participants, we visited university campus, fast food shops, bus stops and shopping centres. This approach enabled us to recruit a diverse group of participants with different demographic status.

3.3 Sample size

In qualitative studies, determination of final sample size depends on the saturation point; therefore, the sample size can be decided only after the initial analysis of the data (Mukherjee et al., 2020). Saturation point is a level in qualitative data collection and analysis where new information stops emerging (Strauss & Corbin, 1998). Accordingly, following the common practice in qualitative studies (e.g. Mukherjee et al., 2020), the data collection process was continued till the saturation occurred. Overall, 30 people were interviewed. After 27 interviews, researchers realised that saturation has occurred because the codes were similar. However, three more interviews were held to ensure the saturation.

3.4 Semi-structured interviews

Privacy is a sensitive topic and participants might be reluctant to discuss their privacy concerns and privacy related past experiences in a group of people. Thus, we preferred interviews over focus group method for data collection. Semi-structured interviews consist of a number of

open-ended questions. Adopting semi-structured interviews, a researcher can follow up particular points raised by an interviewee and can deeply explore a phenomenon by expanding on the interviewee's responses (Al Khasawneh, 2009; Fossey, Harvey, McDermott, & Davidson, 2002; McMurray, Pace, & Scott, 2004). A qualitative researcher may use unstructured or semi-structured interviews (Foley & Timonen, 2015). However, the literature suggests using interview guides, i.e., semi-structured interviews, with a maximum of 10 questions to keep the interviewee focused on the topic under investigation (Foley & Timonen, 2015). Thus, current research adopts semi-structured interview approach to explore the privacy concerns of app users.

3.5 Interview procedure and demographic profile of the respondents

All the interviews were audio recorded. Interviewees were given an information sheet, and informed consent form with confidentiality explained in the information sheet and consent form. Respondents were ensured that their identity would not be divulged in any stage of data collection or reporting.

Following the semi-structured interview approach, an open-ended interview guide was designed. General questions were asked first, for example, type of smartphone used, and number of applications in their smartphone. Next, the interviewees were asked what types of applications they have installed in their smartphones, what applications they use most frequently, what factors they consider before installing an app, and what permissions they have given to them. They were then asked what permissions they have not given and the reasons for not giving those permissions. Further, the interview guide was refined based on the responses gathered from the initial interviews. That is, we interviewed the first five participants with the initial interview guide, however, the structure of the interview guide was slightly refined and adjusted after the initial analysis of first five interviews.

Upon the end of the interview process, the interviewees were thanked and advised that interview has concluded. The gender distribution was female=53%, male=47% with ages ranging from 18 to 54 years. All the respondents were smartphone owners and the frequent users of smartphone applications.

4. THEMATIC ANALYSIS

A thematic analysis was performed following the guidelines of Braun and Clarke (2006).

4.1 Transcription

One researcher in the team transcribed the audio recordings into a Microsoft office word document. After transcription, each transcript was double checked for errors. For this purpose, the audio recordings were listened to again while reading the transcription text with any changes made immediately. This, process was performed twice for each transcript.

4.2 Coding

After transcription process, all transcript files were imported into NVivo 12 Pro software package. This package enabled researchers to perform a computer assisted analysis of the qualitative data while ensuring the rigour of the thematic analysis (Al Khasawneh, 2009; Bazeley & Jackson, 2013). The coding process was performed by two researchers. Krippendorff's alpha was calculated to examine inter-coder reliability which reported 82% similarity in the coding process, hence ensured the inter-coder reliability (Krippendorff, 2013). The coding process generated 53 codes that were grouped into categories for thematic analysis.

4.3 Themes

A theme captures groups of data that has a meaning to answer a research question (Braun & Clarke, 2006). The rationale for developing each theme was based on the objective of the study, i.e., *to explore and identify the privacy concerns of smartphone users pertinent to app usage.* Since the process of developing a theme is subjective by nature, another expert in qualitative

research reviewed the process. Both researchers explained the themes and justified the reasons(s) to classify codes into categories and themes. This process added an extra layer of validity by ensuring that themes were accurate and justified (Gibbs, 2007).

4.4 Authenticity and Credibility

The rigor in qualitative research is ensured through the authenticity and credibility of a study's findings (O'Reilly & Marx, 2011). According to Armour, Rivaux, and Bell (2009): *"authenticity and credibility of a study's findings refer to either or both methodological thoroughness and precision of criteria used to judge the trustworthiness of the results"*. Two approaches were used to test the authenticity of the findings. First, as suggested by qualitative experts (O'Reilly & Marx, 2011; Seale & Silverman, 1997), judgemental sampling was used to recruit research participants which ensures the authenticity of any qualitative research study (Seale & Silverman, 1997). Second, the coding process was performed by two coders with the assessment of inter-coder reliability ensuring the reliability and reproducibility of a qualitative analysis. The Krippendoff's alpha value of 82% was above the threshold value of 80% (Krippendorff, 2013).

Multiple methods were adopted to ensure the credibility of the findings. According to Shenton (2004), providing a detailed description or thick description of the context that surrounds the respondents is a primary method for establishing credibility. Accordingly, explanation of the context was given throughout the analysis and discussions of the findings. Second, analysis was done by merging respondents' views with the theoretical underpinnings, giving insightful interpretations to the findings (Yvonna & Guba, 1985). Third, coding procedure and thematic maps were discussed with other experts working in the relevant domain helping to ensure the credibility of the codes and themes. Finally, the entire coding was computer assisted, thereby minimising biases.

5. FINDINGS

The findings indicate that privacy concerns of app users can be divided into three major concerns (main themes) under which there are six sub concerns (sub-themes). These major concerns are credibility concerns, unauthorised secondary use, and vulnerability concerns with popularity, privacy policy, stalking, data sharing, hacking, and personal harm emerging as the sub concerns. The discussion of these major and sub concerns is as follows.

5.1 Credibility concerns

Credibility refers to the individuals' perceptions of trustworthiness and believability of an object or a person (MacKenzie & Lutz, 1989; Maseeh et al., 2021). Our findings show that app users are concerned with the credibility of apps and app developers. Under credibility, they are mainly concerned about popularity and privacy policy of the app. If the app is popular and has a well-defined privacy policy, it is considered a credible app. Individuals are reluctant to disclose personal information to an app which is unpopular and do not have well-defined privacy policy. Each of these sub concerns are elaborated below.

5.1.1 Popularity

Our findings show smartphone users' decision to disclose personal information to an application is impacted by the popularity of the app, indicating that popularity is an important factor in shaping customers' privacy concerns. For example, participant no. 11, a 32-year-old female stated;

> *"If the application is very famous and the people I know, use that kind of app very much then, I don't even consider the permission."*

Few respondents indicated that when disclosing personal information to an uncommon and unpopular app, they consider the number of downloads of the app as an indicator of popularity. For example, participant no. 26, a 23-year-old male, said;

"Yeah. I will have a look if it is like only a couple of hundred people have downloaded and they are asking this much information I will not trust it."

The findings of our study suggest that the popularity of an application is an indication of its credibility and smartphone users look for the number of downloads as a proxy for popularity when considering downloading uncommon and unpopular application and giving permission to access their personal information. Thus, the following proposition is proposed.

Proposition 1: *Popularity and number of downloads of an application are considered indicators of the credibility of the app, which is a privacy concern for smartphone app users.*

5.1.2 Privacy policy

Privacy policy reflects an application's regulations and duties regarding managing customers' personal information (Zhao, Lu, & Gupta, 2012). Privacy policy is an important concern of app users which affects their decision to disclose their personal information to apps. Several of our respondents believe that privacy policies provided by apps are unclear and vague. For example, participant no. 6, a 34-year-old female said;

"They have to say in their privacy policy that they will not sell your personal details to any outsourcing companies. Because I have noticed that many of apps won't say this in their policy, it is dangerous. I will not download such app."

Some participants mentioned whilst privacy policies may be well-defined, app developers may change their privacy policies without notifying customers, triggering the probability for information misuse, again, a concern for app users. For example, participant no. 26, a 23-year-old male said;

"But the privacy policies are always changing you never know. To misuse my data, they can remove a condition from their policy."

Interestingly, a few respondents indicated though app developers provide well-defined privacy policies, they may not always stick to terms and conditions in the policy. Therefore, the existence of privacy policy does not guarantee that their data will not be misused. For example, participant no. 30, a 27-year-old female said;

> *"Who knows whether they are actually following their policies or not? So, it doesn't matter how comprehensive their privacy policy is, they can still misuse my personal information."*

Overall, our findings showed that the existence of a privacy policy alone is not sufficient to address customers' privacy concerns. Consistency of privacy policy and adherence to privacy policy also matter to address customers' privacy concerns. Thus, the following proposition is proposed.

Proposition 2: *Well-defined, and consistent privacy policy and adherence to the privacy policy of an application are considered indicators of the credibility of the app, which is a privacy concern for smartphone app users.*

5.2 Unauthorised secondary use

Smith, Milberg, and Burke (1996) argued that internet users are concerned about unauthorised secondary use of their personal information. Though this issue has been studied in the past (Degirmenci, 2020; Fodor & Brem, 2015), the literature mainly specifies data sharing or selling to third parties as the main unauthorised secondary use (Fodor & Brem, 2015; Smith et al., 1996).

Consistent with the online privacy literature (Smith et al., 1996), our findings show that app users are concerned with the unauthorised secondary use of their personal information. App users indicated that personal information is accessed via apps to provide personalised services, however, this information is used for other purposes, such as stalking, and earning revenues by

selling their data to third parties, which is then used for personalised marketing. The discussion of each of the sub concerns follows.

5.2.1 Stalking

Stalking is defined as *"a series of actions directed at one individual by another that taken as a whole amount to unwanted persistent personal harassment"* (Sheridan, Davies, & Boon, 2001, p. 152). The findings suggest that app users are concerned about stalking through apps. Participants indicated that app developers stalk them via their smartphones by tracking their location. For example, participant no. 12, a 22-year-old male said;

> *"I don't want to be stalked by the apps. I don't really feel good about that. I feel that I am being stalked 24 hours a day."*

Besides stalking through location tracking, a few participants believe that they can be stalked by audio recording using the microphone in their smartphone. Some of the interviewees shared their experiences with how apps record their voices without their knowledge and tailor the advertisements accordingly. For example, participant no. 4, a 21-year-old female said;

> *"I did an experiment on my friend's phone, we switched the phone off, and just kept saying something about kitchen appliances near the phone. And when we opened the phone on Facebook, Instagram even Amazon, the exact we got was related to kitchen appliances. Like fridge and everything like that. It means they are always recording our voices."*

Similarly, participant no. 17, a 20-year-old female said;

> *"It can be scary sometimes, once, I discussed a clothing brand with my friend. We didn't search anything, but I had that brand advertisement pop up everywhere which was scary."*

Our findings show app users are concerned about both their location tracking and recording of their voices. These are two basic forms of stalking they often encounter which trigger their privacy concerns. As such, the following proposition is proposed.

Proposition 3: *Stalking, particularly in the forms of location tracking and voice recording, is considered an unauthorised secondary use of app users' personal information, which is a privacy concern for them.*

5.2.2 Data sharing with third parties

Our findings suggest that sharing app users' data is shared with third parties without their consent triggers privacy concerns. For example, participant no.1, a 48-year-old male said;

> *"App developers ask to access as much personal data as possible to sell it to others to have business."*

Interestingly, a few participants indicated that although they have concerns about selling their data to third parties, they will have less concerns if data sharing is backed by monetary incentives. For example, participant no. 24, a 40-year-old female said;

> *"I know they are going to sell my information to others and make money from it. If they are doing so, I am concerned about money they are making because of my data and not giving me money."*

App developers access users' personal information and try to understand their shopping interests and lifestyle (Meng et al., 2016) and use it for personalised marketing (Degirmenci, 2020; Kim et al., 2017; Swain et al., 2023) which is a major source of income for app developers. The literature suggests that sharing of personal data with third parties is a concern for internet users (Smith et al., 2011). However, our findings show that app users are concerned not only about data sharing, but also about the marketing based on their shared personal information. Accordingly, it is considered as an unauthorised secondary use of personal

information triggering privacy concerns. For example, participant no. 10, a 32-year-old female said;

> *"After installing that app, someone called me and said that because I have already installed ABC app, I should also install XYZ app. It was annoying that they marketed their app just because I downloaded a similar app and gave access to my data. It is kind of creepy, so I just uninstalled that app."*

Similarly, participant no 13, a 30-year-old female said;

> *"Once I downloaded a selfie app, after that, I got several advertisements appearing on my phone. This was worst experience I had. Then I immediately deleted that app because unnecessary advertisements were appearing on my phone screen."*

Our participants believe that app advertisements communicated to them are not only personalised based on their information, but also based on the photos contained in the phones. For example, participant no. 4, a 21-year-old female said;

> *"I don't like apps to access my photos because app owners look at your photos and tailor their promotional messages based on the clothes that you wear in your photos. I think that is really a misuse of my privacy so that's why I don't like it."*

This study shows that app users are not only concerned about data sharing by app developers to third parties, but also about the monies involved by disclosing their personal information. Marketing is considered another unauthorised secondary use of individuals' personal information, because getting access to app users' photos and customising advertising messages according to their dressing styles are considered privacy invasions. Thus, the following proposition is proposed.

Proposition 4: *Data sharing with third parties and app-based marketing are considered unauthorised secondary uses of app users' personal information, which are privacy concerns for them.*

5.3 Vulnerability concerns

Perceived vulnerability refers to potential risk(s) associated with disclosing personal information on online platforms (Alashoor, Han, & Joseph, 2017). In the context of smartphone applications, app users' perceptions of vulnerability have not been studied much, i.e., the literature does not show app users' perceptions of the potential risk(s) to which they are vulnerable when disclosing personal information to an application. Our findings suggest that app users perceive they are vulnerable to hacking, scamming, and personal harms, including sexual attacks if apps access their personal information. These risks are elaborated below.

5.3.1 Hacking

The term *hacking* refers to penetrating into a computer system without owner's permission for criminal purposes (Richterich & Wenz, 2017). Our participants believe that app developers can hack their smartphones and steal their information which is a privacy concern for them. For example, participant no. 29, a 23-year-old male said;

> *"If I let apps access my phone, they will have all the technical information about my device which will make it easy to hack my phone. Which I don't want them to do."*

A few participants mentioned that are they concerned not only about the perceived vulnerability of hacking of their smartphone, but also about hacking of an app they have installed. In other words, it was indicated that because of technical flaws, most of the apps are vulnerable to hacking, and if someone installs such apps and gives access to personal information, a third party can hack that application and invade the app user's privacy. For example, ABC app may not have access to a specific information, such as contacts, while a user may have given the

same access to XYZ app. In that case, there is a possibility that someone can hack XYZ app thereby accessing the user's contacts through that app. For instance, participant no. 17, a 20-year-old female said;

> *"I have lots of applications on my phone, I do feel that they could be easier to hack. So, if someone hacks those apps, they can access all the information I have disclosed to those apps."*

Interestingly, some participants indicated vulnerability to scamming when hackers steal their information. For example, participant no. 11, a 32-year-old female said;

> *"Because people can hack my phone and get all the personal information, there are more chances to get scammed. So, it is very important to protect my privacy because if get scammed, I may lose some money."*

Similarly, participant no. 3, a 30-year-old female said;

> *"I would not allow any app to access my device information because through that, they can access my phone number. I have shared my phone number with my bank. And if someone gets access to my phone number, they can hack my mobile banking app and rip me off."*

Our findings indicate that hacking either users' smartphone or the apps they have installed in a smartphone is a privacy concern because it triggers the possibility for getting scammed. Therefore, they perceive that they are vulnerable to hacking and scamming if they disclose their personal information to an application. Thus, the following proposition is proposed.

Proposition 5: *App users perceive that disclosing personal information to apps makes them vulnerable to hacking and scamming, which are the privacy concerns for them.*

5.3.2 Personal harm

Our participants believe that their personal information can be misused by app developers to cause personal harm. For example, participant no. 23, a 20-year-old male said;

> *"If app developers track my physical location, they can see what time I am at home and what time I am away. So, from my information privacy, they can get into my physical privacy then they can find me and harm me"*

A few participants mentioned that people could use their personal information to break-in their property for criminal activities. For example, participant no. 19, a 19-year-old male said;

> *"Using my personal information, people can see my daily activities. And if they track me that I am outside my home, I am worried that they can come to my home, steal my things, and damage my property."*

Interestingly, a few female participants indicated concerns about sexual abuses that may be caused using their personal information. That is, app developers may use app users' personal information to approach them and sexually abuse them. For example, participant no 17, a 20-year-old female said;

> *"I feel like people can probably do a lot more with personal information. Then they can find the place where I live. They can chase me by monitoring my physical location and catch me and sexually abuse me."*

Overall, our findings show that app users are highly concerned about personal harms caused by disclosing their personal information. Thus, the following proposition is proposed.

Proposition 6: *App users perceive that disclosing personal information to apps make them vulnerable to personal harm, such as physical harm, property damage, and sexual assaults, which are privacy concerns for them.*

5.4 Development of framework of smartphone app users' privacy concerns (SAUPC)

In Figure 1, we have developed a framework that presents app users' privacy concerns and the propositions derived from the findings.

<Figure 1>

The framework shows app users are concerned about the credibility of an application. They perceive that a popular application (proposition 1) with a consistent and well-defined privacy policy (proposition 2) is credible. Accordingly, for an application to be considered popular, it should be a commonly used application with a larger number of downloads. In case of privacy policy, app users believe that mere existence of privacy policy is not enough. App developers should have a well-defined privacy policy with unambiguous terms and conditions. Furthermore, the findings suggest that app developers should keep the policy consistent and adhere to its terms and conditions. Accordingly, the credibility of an application plays an important role in deciding to install and disclose personal information to an app.

Unauthorised secondary use of information is the second major privacy concern of app users, i.e., they perceive that applications access their personal information to provide personalised services, however, app developers use this information for other purposes. Figure 1 shows that stalking (proposition 3) and data sharing (proposition 4) are considered unauthorised secondary uses of app users' personal information. App users perceive their data can be used to stalk on them via location tracking and voice recording. Moreover, app developers can sell their data to third parties/marketers to earn money.

Vulnerability concerns is the third major privacy concern of app users. The framework shows that app users are concerned about vulnerability to hacking (proposition 5) and personal harm (proposition 6) through disclosing their personal information to smartphone apps. They perceive that app developers can hack either their devices or applications they have installed in their smartphones and steal their personal information that can be later used for scamming,

resulting in monetary loss. App users also believe their information can be used to cause them physical harm and property damages. Additionally, app users perceive that they are vulnerable to sexual assaults if someone has access to their personal information including photos and location.

6. ACADEMIC CONTRIBUTIONS

This study has multiple academic implications. First, although privacy concerns have been studied in mobile/smartphones context (e.g., Nikkhah & Sabherwal, 2017), an understanding of app users' privacy concerns remains limited. This is because the privacy concerns of app users have not yet been explored. As discussed in the literature review section, instead of specifically exploring app related privacy concerns, researchers adopted existing frameworks (i.e., GIPC, CFIP, IUIPC or MUIPC) (See Table 2) to study app users' privacy concerns. Privacy concerns are transformative in nature and vary across contexts (Yun et al., 2019). Thus, researchers recommend continuous research on privacy concerns in the context of new technologies (Xu et al, 2012). Accordingly, previous frameworks on privacy concerns do not represent the actual privacy concerns of app users, therefore, applying existing frameworks in the context of smartphone apps might result in biased, incomplete, and inaccurate understanding of smartphone apps users' privacy concerns. We have explored individuals' privacy concerns pertinent to smartphone app usage. By doing this, our study extends the literature and provides a theoretical development of individuals' privacy concerns in the context of a widely used technology, i.e., smartphone applications. Table 2 presents a comparison between the existing frameworks of privacy concerns and the newly proposed framework of app users' privacy concerns thereby highlighting the contributions of this study.

Second, the concerns identified in our study add to privacy calculus theory. Privacy calculus theory explains that *"individuals determine their disclosures by assessing whether they can manage the information to be shared while minimising the negative consequences of*

these self-disclosures" (Trepte et al., 2017, p. 2). That is, individuals assess the potential outcomes of privacy disclosure before sharing their personal information. Accordingly, when smartphone app users are asked to share their personal information, they perform a risk-benefit analysis. Smith et al. (2011) suggest that privacy concerns may influence individuals' privacy risks, however, they did not specify what those privacy concerns are. We have explored individuals' privacy concerns pertinent to smartphone apps (i.e., credibility concerns, unauthorised secondary use, and vulnerability concerns). Accordingly, our findings advance the privacy calculus theory in the context of smartphone applications. Figure 2 depicts our contributions to the privacy calculus theory.

<Figure 2>

Third, although customers' perceptions of unauthorised secondary uses of their personal information have been studied in the past (Degirmenci, 2020; Fodor & Brem, 2015), the literature does not explore app users' perceptions of unauthorised secondary uses in smartphone app context. Additionally, the literature mainly specifies data sharing or selling to third parties as the main unauthorised secondary use (Fodor & Brem, 2015). However, our findings suggest that along with data sharing with third parties, stalking is considered an unauthorised secondary use of personal information in the context of smartphone applications. App users perceive that they can be stalked by tracking their location as well as recording their voice. Thus, our study enhances the understanding of app users' concerns about unauthorised secondary use of their personal information.

Finally, the literature suggests that vulnerability triggers individuals' privacy concerns (Hsu, 2016;), however, the literature does not show app users' perceptions of vulnerability, i.e., possible situations where they are vulnerable due to the disclosure of personal information to an application. Our study demonstrates that app users are vulnerable to hacking and personal harm. They perceive that giving access to their device can result in unpleasant outcomes, i.e.,

app developers can hack their device as well as applications and then steal their personal information that can be used for scamming. Furthermore, they can be tracked and physically harmed or sexually abused by app developers, or their properties can be damaged. Accordingly, our study contributes to the literature by identifying app users' perceptions of vulnerability resulting from information disclosure trough apps i.e., hacking, and personal harm.

7. PRACTICAL IMPLICATIONS

Practically, the findings of this study are important for multiple stakeholders. First and foremost, privacy concerns have been a barrier to the success of a marketing campaign, specifically in the context of personalised marketing in online environments, such as smartphone apps (Meng et al., 2016; Strycharz, van Noort, Helberger, & Smit, 2019). A deeper knowledge about consumer privacy concerns pertinent to apps may help mitigate those concerns thereby increasing the installation and usage of apps and the viewership of marketing contents. Our findings provide insights to app developers and app marketers into the privacy concerns of app users. This information helps them design apps considering users' privacy concerns. It is expected that mitigating privacy concerns may trigger the installation and usage of apps thereby addressing a barrier to the success of personalised marketing campaigns.

Second, the findings suggest that well-defined and consistent privacy policies address users' privacy concerns, and hence it is recommended that app developers have unambiguous terms and conditions in their privacy policies and stick to the conditions. In case they change their policies, it should be communicated to app users. Third, since customers look at the number of downloads as an indicator of the popularity and credibility of an app, it would be challenging for new apps to gain customer trust. Thus, app developers can enhance the number of downloads by offering incentives to app users, such as free premiums, for some time from their launch.

Fourth, the findings show that although app users are concerned about data selling, they will have fewer concerns if data sharing is backed by monetary incentives. Accordingly, to address their privacy concerns, it is recommended that app developers provide incentives to app users in exchange of their personal information.

Fifth, the findings are useful to smartphone app stores, for example, *Google Play Store* and *Apple App Store,* in understanding and integrating app users' privacy concerns into policies, terms and conditions put forwarded for app developers. Lastly, the findings are useful for government organisations in controlling cyber-crimes. They may use these findings to design and implement cybersecurity policies to protect the privacy of smartphone application users. It may also help reduce the possibility for cyber-crimes. In addition to these implications, Table 3 enlists some more implications for apps and policy makers emerging from each key finding.

<Table 3>

8. LIMITATIONS, FUTURE RESEARCH DIRECTIONS AND CONCLUSIONS

Even though this study has multiple academic and practical implications, it has a few limitations that should be acknowledged. First, using a qualitative methodology, we adopted a phenomenological approach, accordingly, the findings are based on the coding of the qualitative data which limits the possibility for direct replication (Strauss & Corbin, 1998). Second, the appropriateness of the sample size could be questioned, however, a number of qualitative studies have considered similar smaller samples sizes (Quach, Jebarajakirthy, & Thaichon, 2017). We wish to note that in qualitative studies, the sample size depends on the point of saturation (Thomson, 2010). Accordingly, the data collection process was stopped after interviewing the 30th participant when the saturation point was reached. Lastly, as privacy is a sensitive topic, participants' responses might suffer from social desirability. Accordingly,

it is possible that participants might have experienced a reluctance in sharing their privacy concerns in the context of smartphone applications.

The present research opens some directions for future research. First, we have developed a framework that summarises the privacy concerns of app users (see Figure 1). Future researchers can test this framework using quantitative research method to statistically examine and confirm app users' privacy concerns. This framework provides a steppingstone to identify the constructs, propose hypotheses and develop a measurement instrument (i.e., to develop survey items) for such a quantitative study. Accordingly, future researchers can use a larger sample which will help generalise the findings to a wider population of app users. Specifically, though our research has demonstrated privacy concerns about smartphone app usage, we did not propose items to measure these concerns. Thus, we call future researchers to develop a scale to measure these concerns.

Second, future researchers can examine how privacy concerns of app users impact their behaviour. That is, future studies can be carried out to examine the influence of these privacy concerns on app installation and usage behaviour or app recommendation behaviour of app users. Third, unauthorised secondary use of app users' personal data might trigger the possibility of hacking or personal harm thereby making app users vulnerable to such incidences. However, it is not known whether app users' concerns of unauthorised secondary use engender their vulnerability concerns. As such, future researchers may empirically examine the influence of app users' perceptions of unauthorised secondary use on their vulnerability concerns. Finally, in present research, we did not specify any apps, i.e., the privacy concerns of app users were explored in general. Thus, current study can be replicated for a particular app, such as Uber Eats, or a particular type of app, such as dating apps, to explore the privacy concerns that are specifically related to the users of such applications.

In conclusion, although privacy concerns have been studied in various contexts, the privacy concerns in the context of smartphone apps remains unexplored. Accordingly, we have explored and identified customers' privacy concerns pertinent to smartphone app usage. The findings show that credibility concerns, unauthorised secondary use, and vulnerability concerns are the major privacy concerns of app users. Based on the findings, we proposed insightful recommendations for app businesses. Our study advances the literature by proposing a framework for smartphone app users' privacy concerns (SAUPC) which is the silver lining of this study.

References

Adil, M., Sadiq, M., Jebarajakirthy, C., Maseeh, H. I., Sangroya, D., & Bharti, K. (2022). Online service failure: antecedents, moderators and consequences. *Journal of Service Theory and Practice*, *32*(6), 797-842.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model. *CAIS, 41*, 4.

Al Khasawneh, M. (2009). An exploration of Consumer Response towards Sponsored Search Advertising (SSA) from a Consumer Behaviour Perspective. *Griffith University*.

Armour, M., Rivaux, S. L., & Bell, H. (2009). Using context to build rigor: Application to two hermeneutic phenomenological studies. *Qualitative Social Work, 8*(1), 101-122.

Ashaduzzaman, M., Jebarajakirthy, C., Weaven, S. K., Maseeh, H. I., Das, M., & Pentecost, R. (2022). Predicting collaborative consumption behaviour: a meta-analytic path analysis on the theory of planned behaviour. *European Journal of Marketing, 56*(4), 968-1013.

Bazeley, P., & Jackson, K. (2013). *Qualitative data analysis with NVivo*: SAGE publications limited.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1042.

Boyles, J. L., Smith, A., & Madden, M. (2016). Privacy and data management on mobile devices. Pew Research Center 2012. In: Sept.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Center, P. R. (2019). *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*. Retrieved from https://www.pewresearch.org/global/2019/02/05/global-technology-use-2018-appendix-e-detailed-tables/

Chang, S. E., Shen, W.-C., & Liu, A. Y. (2016). Why mobile users trust smartphone social networking services? A PLS-SEM approach. *Journal of Business Research, 69*(11), 4890-4895.

Chen, & Hsieh. (2012). Personalized mobile advertising: Its key attributes, trends, and social impact. *Technological Forecasting and Social Change, 79*(3), 543-557. doi:10.1016/j.techfore.2011.08.011

Cheung, A. S. (2014). Location privacy: The challenges of mobile service devices. *Computer Law & Security Review, 30*(1), 41-54.

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management, 39*, 49-59.

Choi, B. C. F., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management, 53*(7), 868-877.

Chopra, I. P., Jebarajakirthy, C., Acharyya, M., Saha, R., Maseeh, H. I., & Nahar, S. (2023). A systematic literature review on network marketing: What do we know and where should we be heading? *Industrial Marketing Management, 113,* 180-201.

Culnan, M. J., & Regan, P. M. (1995). Privacy issues and the creation of campaign mailing lists. *The Information Society, 11*(2), 85-100.

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

Dinsmore, J., Swani, K., Goodrich, K., & Konus, U. (2021). Introduction: Advancing understanding of mobile applications in marketing. In: Elsevier.

Drumm, J., White, N., & Swiegers, M. (2016). *Mobile Consumer Survey 2016: The Australian Cut*. Retrieved from https://landing.deloitte.com.au/rs/761-IBL-328/images/tmt-mobile-consumer-2016-final-report-101116.pdf

Farnden, J., Martini, B., & Choo, K.-K. R. (2015). Privacy risks in mobile dating apps. *arXiv preprint arXiv:1505.02906*.

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior, 53*, 344-353.

Foley, G., & Timonen, V. (2015). Using grounded theory method to capture and analyze health care experiences. *Health Services Research, 50*(4), 1195-1210.

Fong, N. M., Fang, Z., & Luo, X. (2015). Geo-conquesting: Competitive locational targeting of mobile promotions. *Journal of Marketing Research, 52*(5), 726-735.

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian and New Zealand journal of psychiatry, 36*(6), 717-732.

Gibbs, G. R. (2007). Thematic coding and categorizing. *Analyzing Qualitative Data. London: Sage*, 38-56.

Gokgoz, Z. A., Ataman, M. B., & van Bruggen, G. H. (2021). There's an app for that! understanding the drivers of mobile application downloads. *Journal of Business Research, 123*, 423-437.

Groenewald, T. (2004). A phenomenological research design illustrated. *International journal of qualitative methods, 3*(1), 42-55.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19-28.

Guo, X., Sun, Y., Yan, Z., & Wang, N. (2012). *Privacy-Personalization Paradox in Adoption of Mobile Health Service: The Mediating Role of Trust.* Paper presented at the PACIS.

Gupta, R., Mukherjee, S., & Jayarajah, K. (2021). Role of group cohesiveness in targeted mobile promotions. *Journal of Business Research, 127*, 216-227.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management, 36*(3), 441-450.

Ho, M. H.-W., & Chung, H. F. L. (2020). Customer engagement, customer equity and repurchase intention in mobile apps. *Journal of Business Research, 121*, 13-21.

Hsu, H.-M. (2016). *Does Privacy Threat Matter in Mobile Health Service? From Health Belief Model Perspective.* Paper presented at the PACIS.

Hughes, C. (2019). Smartphone ownership in Australia as of March 2018, by age. Retrieved from https://www.statista.com/statistics/730101/australia-smartphone-ownership-by-age/ Accessed on 11-10-2019

Jebarajakirthy, C., Maseeh, H. I., Morshed, Z., Shankar, A., Arli, D., & Pentecost, R. (2021). Mobile advertising: A systematic literature review and future research agenda. *International Journal of Consumer Studies*, *45*(6), 1258-1291.

Jebarajakirthy, C., Weaven, S., Arli, D., & Maseeh, H. I. (2023). Guest editorial: Consumer privacy in the technological era. *Journal of Consumer Marketing*, *40*(2), 153-154.

Jengchung, C., Ross, W., & Huang, S. F. (2008). Privacy, trust, and justice considerations for location-based mobile telecommunication services. *info, 10*(4), 30-45.

Jingjun, X. D., Liao, S. S., & Li, Q. (2008). Combining empirical experimentation and modeling techniques: A design research approach for personalized mobile advertising applications. *Decision support systems, 44*(3), 710-724.

Johnson, J. S., & Sohi, R. S. (2016). Understanding and resolving major contractual breaches in buyer–seller relationships: a grounded theory approach. *Journal of the Academy of Marketing Science, 44*(2), 185-205.

Kang, H., Shin, W., & Tam, L. (2016). Differential responses of loyal versus habitual consumers towards mobile site personalization on privacy management. *Computers in Human Behavior, 56*, 281-288.

Kemp, S. (2012). Social, digital and mobile in Vietnam. *We Are Social (October 30), https://wearesocial. com/uk/blog/2012/10/social-digital-mobile-vietnam*.

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior, 78*, 174-182.

Keith, M. J., Babb, J., Lowry, P. B., Furner, C., & Abdullat, A. (2011). The Roles of privacy assurance, network effects, and information cascades in the adoption of and willingness to pay for location-based services with mobile applications. *Network Effects, and Information Cascades in the Adoption of and Willingness to Pay for Location-Based Services with Mobile Applications (June 30, 2013)*.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Kim, H.-S. (2016). What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior, 54*, 397-406.

Kim, J. S., Yoon, S., & Zemke, D. M. V. (2017). Factors affecting customers' intention to use of location-based services (LBS) in the lodging industry. *Journal of Hospitality and Tourism Technology, 8*(3), 337-356.

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision support systems, 119*, 46-59.

Koubaridis, A. (2014). Tourist sexually assaulted in Sydney by several men after meeting on Tinder. Retrieved from https://www.news.com.au/national/tourist-sexually-assaulted-

in-sydney-by-several-men-after-meeting-on-tinder/news-story/f30af6eb552e5d2a201514b112faa14b Accessed on 17-7-19
Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109-125.
Krippendorff, K. (2013). Component of content analysis. *Content Analysis: An Introduction to its Methodology*, 82-184.
MacKenzie, S. B., & Lutz, R. J. (1989). An empirical examination of the structural antecedents of attitude toward the ad in an advertising pretesting context. *Journal of Marketing, 53*(2), 48-65.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.
Maseeh, H. I. (2022). *Impact of privacy concerns on smartphone users' app usage behaviour: An exploratry research* [Doctoral dissertation, Griffith University]. https://doi.org/10.25904/1912/4906
Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e-commerce: A multilevel meta-analysis. *Psychology & Marketing*, *38*(10), 1779-1798.
Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Ashaduzzaman, M., Arli, D., & Weaven, S. (2021). A meta-analytic review of mobile advertising research. *Journal of Business Research*, *136*, 33-51.
Maseeh, H. I., Sangroya, D., Jebarajakirthy, C., Adil, M., Kaur, J., Yadav, M. P., & Saha, R. (2022). Anti-consumption behavior: A meta-analytic integration of attitude behavior context theory and well-being theory. *Psychology & Marketing*, *39*(12), 2302-2327.
McMurray, A., Pace, R. W., & Scott, D. (2004). *A commonsense approach*: Thomson Learning.
Mehta, P., Jebarajakirthy, C., Maseeh, H. I., Anubha, A., Saha, R., & Dhanda, K. (2022). Artificial intelligence in marketing: A meta-analytic review. *Psychology & Marketing*, *39*(11), 2013-2038.
Meng, W., Ding, R., Chung, S. P., Han, S., & Lee, W. (2016). *The Price of Free: Privacy Leakage in Personalized Mobile In-Apps Ads.* Paper presented at the NDSS.
Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120-130.
Mukherjee, S., Jebarajakirthy, C., & Datta, B. (2020). Retailer selection compulsion in the subsistence markets. *Journal of Retailing and Consumer Services, 52*, 101904.
Namde, A. (2017). *Mobile Application Market by Marketplace and App Category - Global Opportunity Analysis and Industry Forecast, 2016 - 2023*. Retrieved from https://www.alliedmarketresearch.com/mobile-application-market
Nikkhah, H. R., & Sabherwal, R. (2017). Mobile Cloud-Computing Applications: A Privacy Cost-Benefit Model.
O'Reilly, K., & Marx, S. (2011). How young, technical consumers assess online WOM credibility. *Qualitative Market Research: An International Journal, 14*(4), 330-359.
Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.
Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409-419.

Persaud, A., & Azhar, I. (2012). Innovative mobile marketing via smartphones: are consumers ready? *Marketing Intelligence & Planning, 30*(4), 418-443.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Qin, L., Kim, Y., & Tan, X. (2016). Understanding the intention of using mobile social networking apps.

Quach, S., Jebarajakirthy, C., & Thaichon, P. (2017). Aesthetic labor and visible diversity: The role in retailing service encounters. *Journal of Retailing and Consumer Services, 38*, 34-43.

Richterich, A., & Wenz, K. (2017). Introduction. Making and hacking. *Digital Culture & Society, 3*(1), 5-22.

Seale, C., & Silverman, D. (1997). Ensuring rigour in qualitative research. *The European Journal of Public Health, 7*(4), 379-384.

Shankar, A., Jebarajakirthy, C., Nayal, P., Maseeh, H. I., Kumar, A., & Sivapalan, A. (2022). Online food delivery: A systematic synthesis of literature and a framework development. *International Journal of Hospitality Management*, *104*, 103240.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*(2), 63-75.

Sheridan, L., Davies, G. M., & Boon, J. C. (2001). Stalking: Perceptions and prevalence. *Journal of Interpersonal Violence, 16*(2), 151-167.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

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.

Stocchi, L., Michaelidou, N., & Micevski, M. (2019). Drivers and outcomes of branded mobile app usage intention. *Journal of Product & Brand Management, 28*(1), 28-49.

Strauss, & Corbin, J. (1998). Basic operations: asking questions and making comparisons. *Corbin J, Strauss AC. Basics of qualitative research: techniques and procedures for developing grounded theory. Thousand Oaks, CA: Sage*, 73-85.

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2019). Contrasting perspectives–practitioner's viewpoint on personalised marketing communication. *European Journal of Marketing, 53*(4), 635-660.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 1141-1164.

Swain, S., Jebarajakirthy, C., Sharma, B. K., Maseeh, H. I., Agrawal, A., Shah, J., & Saha, R. (2023). Place Branding: A Systematic Literature Review and Future Research Agenda. *Journal of Travel Research*, 00472875231168620.

Swain, S., Jebarajakirthy, C., Maseeh, H. I., Saha, R., Gupta, N., & Grover, R. (2023). Permission marketing: a systematic review of 22 Years of research. *Marketing Intelligence & Planning*, *41*(3), 310-328.

Thomson, S. B. (2010). Sample size and grounded theory. *Thomson, SB (2010). Grounded Theory-Sample Size. Journal of Administration and Governance, 5*(1), 45-52.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media+ Society, 3*(1), 2056305116688035.

Varnali, K., & Toker, A. (2010). Mobile marketing research: The-state-of-the-art. *International Journal of Information Management, 30*(2), 144-151.

Wall, M. (2007). „The hi-tech way to mind that child". *Sunday Times [UK]*, 14.
Wang, Y., Min, Q., & Han, S. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. *Computers in Human Behavior, 56*, 34-44.
Welman, J., & Kruger, S. (1999). Research methodology for the business and administrative sciences. Johannesburg, South Africa: International Thompson. Wenglinsky, H.(2002). The link between teacher classroom practices and student academic performance. *Education Policy Analysis Archives, 10*, 12.
Wilson, L. (2014). Warriena Tagpuno Wright murder: Does Tinder leave you exposed? Retrieved from https://www.news.com.au/technology/online/social/warriena-tagpuno-wright-murder-does-tinder-leave-you-exposed/news-story/7725889c92b1a2626c2c25f969fa8078 Accessed on 17-7-19
Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44-52.
Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. Paper presented at the ICIS.
Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56*(4), 570-601.
Yvonna, L., & Guba, E. (1985). Naturalistic Inquiry. In: Newbury Park, CA: Sage.
Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science, 30,* 1-53.
Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.