Why Does Privacy Paradox Exist?

A Qualitative Inquiry to Understand the Reasons for Privacy Paradox Among Smartphone Users

Sakhhi Chhabra, Indian Institute of Managemen, Sambalpur, India*

ABSTRACT

In this exploratory study, the main aim was to find whypeople disclose information when they are concerned about their privacy. The reasons that provide a plausible explanation to the privacy paradox have been conjectural. From the analysis of the 18 in-depth interviews using grounded theory, themes were then conceptualized. The authors found rational and irrational explanations in terms of cognitive biases and heuristics that explain the privacy paradox among mobile users. They figured out some reasons in this context of mobile computing which were not emphasized earlier in the privacy paradox literature such as peanut effect, fear of missing out (FoMo), learned helplessness, and neophiliac personality. These results add to the privacy paradox discourse and provide implications for smartphone users for making privacy-related decisions more consciously rather than inconsiderately disclosing information. Also, the results would help marketers and policymakers design nudges and choice architectures that consider privacy decision-making hurdles.

KEYWORDS

Behavioural Biases, Heuristics, Privacy Paradox, Qualitative Inquiry, Smartphone Users

1. INTRODUCTION

With the rapid diffusion of smartphones, the mobile channel has morphed into an ultimate marketing vehicle (Varnali and Toker, 2010). Approximately 500 million smartphone users in India share immense digital data through apps with unidentified parties (Ians, 2020). Unlike the EU General Data Protection Regulation (GDPR), which mandates service providers to inform users about the purpose and terms of personal data processing (Betzing et al., 2020), in an emerging economy like India, there is no legal obligation on service providers for personal data processing. Mobile users ignore the fact that smartphones are considered ‘portable personal spy’, and the information collected through phones can be easily used in profiling them, and with always-on data transmission, there is a strong potential for privacy intrusion (FTC, 2009). On one end of the spectrum, individuals are anxious about the misuse of their data, but on the other end, they share personal data by clicking onto terms and conditions with the blink of an eye. In the quest for more convenience, or pursuit of personalization, individuals end up disclosing data, however, they articulate high privacy concerns (Acquisti, 2012). This has been documented as a ‘privacy paradox’ which is the essence of this research work.

Privacy paradox refers to the discrepancy between a consumer’s stated privacy risk beliefs and their actual behaviors (Norberg, et al, 2007). Users express the need for transparency and information

DOI: 10.4018/JECO.292470

*Corresponding Author

control, but the desire to own a specific app seems to offset its potential risks. Mobile users accept the 'all-or-nothing' policy by app stores just to download a particular app, whereby they voluntarily give permissions to apps for collecting their personal information (Betzing, 2020). Sometimes rationally and sometimes obliviously people behave paradoxically to their privacy concerns and behavior. Thus, finding the reasons for this paradox amongst the mobile users is significant to help the users make more accurate decisions which is beneficial for them to continue using mobile phones securely. Findings these reasons will add to the new facets of understanding the word-deed gap.

There have been numerous studies that have tried to propose theoretical explanations for the privacy paradox nevertheless no comprehensive explanation has been found so far (Kokolakis, 2017). Many studies have quantitatively tried to map the relation between privacy attitude (often operationalized as the assessment of privacy concerns or perceived risk,) and intention to disclose. In this research, we try to understand human behavior more precisely by digging into actual disclosure behavior.

Some social scientists have given rational explanations for this paradox, but some have debunked the assumptions that individuals make rational disclosure online (Kokolakis, 2017). Users are not always capable of making rational disclosure decisions, due to cognitive limitations. However irrational reasons in terms of cognitive and behavioral biases to privacy disclosure decisions have been conjectural. Thus, to understand this phenomenon and find out the reasons (rational and irrational explanations) of the privacy paradox, an exploratory investigation was most appropriate. Qualitative research would help in gaining new insights into a phenomenon as it is based on interpretation and understanding of opinions and motivations of the respondent. With the help of in-depth interviews, the interviewer could probe hidden issues, personal opinions, beliefs, and values more profoundly. Thus, the objective of this research is to find out the reasons which govern the explanation for the existence of the privacy paradox among smartphone users.

On figuring out which of the reasons function in privacy decisions making, individuals shall be able to make more conscious decisions that minimize adverse outcomes and avoid getting manipulated by design tricks of platforms to harm consumers' privacy. Also contrasting to the EU GDPR, which came into effect on 25th May 2018, to reduce information asymmetry by strengthening data protection for EU citizens (Betzing, et al., 2020), India does not have any legal privacy protection policy the same. In an emerging country with a vast majority of mobile users, it is significant that any processing of personal data must follow the principles of lawfulness, fairness, and transparency. This study shall add to building up understanding towards developing a useable privacy policy keeping disclosure behavior in mind. The results shall assist policymakers in developing more usable privacy and security tools, whereby user's privacy concern aligns with their disclosure behavior. Interventions can be designed to gently guide users towards safer practices rather than imposing decisions. The implications of the study will range in the area of 'nudging research' and 'soft paternalism'. In the following sections, we provide a review of relevant literature, elaborate on the method used in our study, and provide a detailed illustration of the reasons found in the analysis. The paper concludes with a discussion including implications for research and practice, and study limitations.

2. LITERATURE REVIEW

In 2001, Brown uncovered the concept of the 'privacy paradox' in a series of in-depth interviews with online shoppers. He inferred that individuals expressed their concerns about privacy infringement, but they still give their details to online retailers as long as they had some benefit in return (as cited in Kokolakis, 2017). Individuals who claim to perceive high amounts of privacy risk and low intention to disclose information still demonstrate relatively higher levels of actual information disclosure (Acquisti and Grossklags, 2005; Norberg et al., 2007). And this level of actual disclosure significantly exceeded individuals' intentions to disclose information for various categories of information like personally identifying, financial, demographic, etc. (Norberg and Horne, 2007). In many domains of human behavior, it has been observed that what people say and what they do are at times very different. Similar is the case in the context of privacy, where individuals who claim to be concerned about their personal information, act very differently when an information-sensitive situation actually arises. Some complete transactions without protecting personal information, some give away information for small rewards (Acquisti and Grossklags, 2003).

Information privacy concerns have augmented in the mobile context because personal information is often collected without the express consent of the customer (Chellappa and Sin, 2005) and behavioral intentions of the organization collecting personal data are not always evident (Betzing, 2020). Mobile operating systems regularly record and transmit location data without the consent of device owners (Angwin and Valentino-Devries, 2011). In an examination of 101 popular smartphone apps, the Wall Street Journal found that 47 apps transmitted the phone's location to outsiders and 56 apps transmitted the phone's unique identifiers to other companies without users' awareness (Thurm and Kane, 2010). The case of Cambridge Analytica, which used a mobile app to collect private information from 50 million Facebook users for voter profiling, is one of many examples of privacy invasions that happen without users' knowledge (Rosenberg, 2018). This ubiquity of mobile computing makes privacy concerns and disclosure decisions different from those encountered during desktop computing.

Several studies have proved the existence of the privacy paradox, whereas other studies have challenged the same. Studies supporting the existence of phenomena like Zafeiropoulou et al. (2013), Taddicken (2014), Pentina, et al., (2016), and Lee et al. (2013) have confirmed that despite the privacy concern, users revealed personal information. Contrarily some studies challenge this paradox and state that mobile users value control over their personal information, but they are often unaware of the data collection and sharing practices of apps they use (Almuhimedi et al. 2015; Shklovski et al. 2014). When informed about their actual practices, users respond by uninstalling the apps (Balebako et al. 2013; Harbach et al. 2014; Shklovski et al. 2014). When privacy policies are displayed prominently, consumers tend to purchase from online retailers that protect their privacy (Kokolakis, 2017). A survey of smartphone users by the Pew Internet Project (Boyles et al., 2012) revealed that 54% of mobile application users decided not to install a cell phone application when they discovered how much personal information, they would need to share to use it. Nonetheless, it is still an unanswered question if the phenomenon of privacy paradox exists or not. Studies explaining why this gap exists are still diminutive (Michaelidou and Hassan, 2014).

Some studies have explained this paradoxical behavior from a rational perspective by arguing that users share their personal information in return for some benefit. They weigh the cost-benefit both consciously and rationally (Simon, 1955). Others have questioned this rational view by arguing that disclosure behavior is not wholly determined by rational thinking, but it is also embraced by the role of irrationality. Acquisti (2004) claims that people may not always be able to act as economically rational agents. Literature on decision-making is vast and it has evolved over the years. Simons's (1955) work on bounded rationality brought in a more realistic perspective of cognitive limitations constraining decision making. There is not one unilaterally accepted theory to explain the privacy paradox, nor is there a consensus on the mental process users rely upon when deciding whether to disclose information or not (Solve, 2021). When it comes to personal privacy, human decision-making is bounded by several cognitive biases. The reason that provides a plausible explanation for this paradox has been conjectural.

There is no complete explanation in relevant research to answer, 'why do people disclose information at all when they have privacy concerns?' It is a relatively under-researched area that demands research attention especially related to the reasons for this paradox. There is a need to investigate the causes of this contradiction between privacy concerns and behavior. Thus, the research question for the study is:

RQ1: Why does the privacy paradox exist?

3. METHODOLOGY

3.1 Rationale for Using In-Depth Interviews

An exploratory inquiry was carried out using semi-structured in-depth qualitative interviews to explore the existence of the privacy paradox and its reasons among smartphone users. Depth interview as a methodology was found suitable for this research because privacy is a sensitive and complex topic. It is difficult for people to accept that their decisions are paradoxical. They rather try to give logic to the choices they have made. Thus, to understand the reasons for the privacy paradox, it was important to make the informant comfortable and gradually let them describe their choices and drivers for those choices. Most research in the privacy area has been survey-based which explores beliefs, privacy attitudes, and consumers' intention to divulge information (Kokolakois, 2017 and Gerber, et al, 2018). In survey-based studies, respondents are likely to induce response bias perhaps leading to an over-reporting of privacy concerns or inaccurately reporting intention to disclose information. Also, not many experiment methodologies papers have successfully replicated realistic privacy scenarios and captured actual disclosure behavior (Barth, and De Jong, 2017). Qualitative studies delve deeper into consumers' psyches and explore the subconscious thoughts and feelings to explain this disconnect between attitudes and behaviors related to privacy. Sometimes people want to narrate an instance explaining their decisions which might not be possible in quantitative studies.

3.2 Sample Profile of the Respondents

Purposive judgment sampling was used for the study, as the objective of the study was to uncover reasons for a phenomenon, (Gliner, Morgan, and Leech, 2009). The sampling frame for the study was 18+ years of age, at least high school graduate, resident of National Capital Region (NCR) Delhi, India, smartphone users (with an operating system as Android, iOS, windows, or blackberry) and using the phone for over one year. The sample size was based on thematic saturation to ensure a deep contextual understanding of the phenomenon (Morse, 2015; Marshall, 1996). Saturation can occur at any number of interviews, but various researchers have figured out a point of thematic saturation which varies from 10 to 30 interviews (Mason, 2010).

3.3. Interview Process

Before the commencement of the interview, informants were asked about their willingness to be interviewed and their preference to be recorded or not. After the consent was taken, a response guide was used to conduct the semi-structured interviews (Leech, 2002) whereby some prepared questions were asked, and subsequently, logical follow-up questions were asked. Questions for the interview were carefully derived from the research objective (See the protocol in Appendix 1). They were constructed in such a way as to provide directions to respondents, but not restrict responses. Conversational prompts were employed, and a laddering technique was used. Each question had several open-ended probes that were used to encourage further discussion on the topic. Close-ended questions were asked about the demographics, occupation, number of apps on a smartphone, etc. The technique of interaction was one to one between the interviewer and a single informant. Interviews were transcribed verbatim within 48hr of the interview.

We started by asking questions related to the respondent's demographic to set the context and make the interviewee comfortable. Then we gradually asked questions associated with mobile applications regarding the kinds of apps, daily mobile usage, number of apps on your phone, most-used apps, etc. We did this purposely so that the respondent's answers are not sensitized by the topic which might cause them to act differently than they would have. We asked about the reasons for downloading mobile applications and gradually transitioning the conversation to disclosure behavior while signing up for an app. Then steadily we enquired about their privacy concern levels. Then we tried to bring back the reasons listed by them for disclosing information. We further probed informants on those same reasons to find out their subconscious motives in making the paradoxical decision of disclosing personal information when they have a privacy concern. We got some rational answers but some of these answers were indirect.

3.4 Data Analysis Technique

The data collected from the interviews were analyzed by Grounded Theory as propounded by Charmaz (2006). In this form of content analysis, the dominant messages and subject matter within the text are identified (McKeone, 1995). The process is like open coding as elaborated by Strauss and Corbin (1990). In this research, the open analysis of the text was done by reading the interview transcripts line by line, making notes for each instance, and identifying various themes. Hence, the transcript was analyzed to note the privacy concerns and reasons for disclosure. Once the phenomenon was identified, it was clubbed into categories (Strauss and Corbin, 1990). Constant comparison was done where new themes were compared with already emerged themes. The constant comparison process helped to unravel new insights from each interview (Charmaz, 2006). Appropriate labels were given to each category. The process of coding was iterative with multiple rounds of back and forth between data, existing themes, and emergent themes. This inductive approach to content analysis was apt as limited previous studies had explored the privacy paradox in the mobile context. See Appendix 2 for the Framework of Grounded theory.

3.5 Data Collection

We conducted eighteen qualitative in-depth interviews with smartphone users. The authors settled for the above-stated numbers as theoretical saturation was seen to be achieved at this stage. The interviews were conducted over two months between Jan 2019- Feb 2019. Each interview lasted between 30 minutes to 90 min. The data was collected at a place of convenience as per the informants. The sample comprised of 7 male and 11 female informants, with age groups ranging from 20-54. Respondents belong to varied occupations like NGO worker, doctor, teacher, architect, data analyst, consultant, stay-at-home mom, and recent college graduate. See Appendix 3 for details.

4. FINDINGS

Before we figure out the reasons for the privacy paradox, we asked some surface descriptive questions and then gradually started probing on the behavioral aspect of the disclosure.

4.1 Mobile App Related Questions

We started by asking questions related to mobile usage, the number of apps on your phone, most-used apps, how long they use the mobile phone in a day, to set the context of the study.

In terms of various categories of mobile applications used by respondents, we found that respondents used apps ranging from shopping apps, messenger, travel, food, news, entertainment (gaming, music), taxi, social media, bank and wallet-based apps, sports, and grocery. Apart from the pre-installed app, the majority of people had downloaded WhatsApp messenger, Flipkart- shopping app, and UBER- taxi app. Respondents also informed that they have on an average 22 mobile apps on their smartphone, (refer to Appendix 3 for the number of apps by each interviewee) and daily self-reported usage varies between 1-2 hrs. The most used app reported was WhatsApp messenger, Facebook, and Gmail.

4.2 Process of Decision-Making For Downloading A Mobile App

The following questions were asked:

- Describe the process of decision-making when you must download any mobile app.
    - Do you see the reviews or watch the videos before downloading?

    - Do you read the privacy terms and conditions?
- What are the sources of information you seek while taking decisions to download any mobile app?

Understanding the decision-making process for downloading a mobile app would help in finding the real motive of using an app. Respondents described they downloaded an app after realizing the need for an app or receiving the recommendation from friends/relatives, or through WOM or social media. Some of them also read reviews or saw the videos before downloading, and if they liked it, they sign up by giving their information. The frequency of download depended on the requirement and they rarely uninstalled any app. N=13 people claim that they read the privacy terms and conditions but not always. Only a few of them claimed that they did not read it completely.

This helped us in setting the preliminary background for digging into the reasons for downloading the app. The analysis of the interviews revealed various themes, however, for this study, we focused on codes related to the objective of the research. We categorized raw data into different themes.

4.3 Privacy as a Concept

We found that each person had their interpretation of privacy, clearly indicating that it is not an absolute concept (Solve, 2008). These findings are similar to Smith et. al., (2011) which have demonstrated privacy is not a singular concept that crosses all disciplines and that is embraced by all observers. Some of the respondents in our study related it to allied concepts like “secrecy”, “anonymity”, “confidentiality”, “limited access”, and “control of information” in their hands.

- “Privacy for me is my space. Only a few people know about me. If someone wants to enter my space, he/she should take permission.” (Respondent E, Age 26)
- “I don’t want to tell others about my family/ internal affairs. My husband, my house, my financial status is considered private. I want to decide as to what information should be told and what should not be.” (Respondent F, Age 54)
- “For me, privacy means- No interference, there is a boundary” (Respondent 0, Age 28)

However, one common theme noticed from all the above descriptions was that; privacy is like a frontier between private and public which should be respected and valued. Every individual should be able to decide who can access information about them and their whereabouts. Thus, the definition of information privacy given by Culnan and Bies as “the ability of individuals to control the terms under which their personal information is acquired and used” (2003, p. 326) is appropriate in the given context. It was considered important by all informants.

4.4 Privacy Concern

To comprehend the individual’s privacy concern, we indirectly probed the respondents and asked them to share an instance of data misuse.

- You have signed up for many applications by giving your personal information, are you bothered that these apps may sell your information to other parties?
- Have you read anywhere that your personal information is being used by a social media company or e-commerce website without your authorization?

Then gradually we asked if they are concerned that mobile apps are collecting too much information about them; if they are losing control of their information by using apps, how would they rate their privacy concern on a scale of 1-5, 5 being the highest and why?

The majority of respondents (N=17) in the interviews felt that over time they have less control of their information. They did acknowledge that private information about themselves is more readily available to others due to the open nature of internet-based technologies. This is in line with the existing literature where users have exhibited privacy concerns (Brandimarte et.al., 2013; Acquisti, et al., 2015; Norberg, et al., 2007, Barth and de Jong, 2017). Especially with smartphones, they felt as if they are being spied by an unknown party. They are aware that data is being compromised, but they do not know which apps are exploiting or selling their information to other parties. Respondents reported they are concerned about privacy.

- "Yes, these apps can sell my information to unknown parties, I'm uneasy about this but I cannot imagine my life without my phone. Moreover, I'm not a celebrity, what will these apps do with my information?" (Respondent J, Age 24)
- "I know apps have access to my location, websites can easily track brands I like but I'm okay compromising till the time it doesn't do any harm to me" (Respondent E, Age 26)

On asking respondents to rate their privacy concern score out of five, on average, they gave four out of five as a concern score. The noteworthy point here is that despite these scores, none of the respondents had taken any step to overcome their concerns. They continue to use apps on their smartphones and disclose their personal information. The reason for reporting this high score could be either to comply with the social norm or to satisfy the interviewer by providing what they consider as correct answers which could be a limitation of in-depth interviews.

4.5 Bounded Rationality as a Reason for Privacy Paradox

Progressing the previous set of questions regarding information privacy concerns, we asked respondents, if they have ever received any spam calls or spam messages. If yes, what scenario?

Interviewees, N=5, shared their experiences. It was noticed that respondents under 30 years of age, were getting spam mails from matrimonial sites and credit card companies whereas the elderly 30+ age group got mails from real estate agents, diagnostic centers, and insurance companies without subscribing or signing up. Email Ads or messages were being specially targeted keeping the demographic of the user in mind. Some of the respondents informed that they are aware that their activities are being monitored through mobile or web browsers.

- "I know WhatsApp is extracting a lot of my data even if I disable it, I read it in a newspaper editorial, also these taxi apps can track my location even when I'm not using them" (Respondent L, Age 31)
- "I saw a video where a man shared that Facebook information is sold to different companies since then I have limited my usage of these apps". (Respondent G, Age 28)
- "A lot of my apps are always logged in. I know it is unsafe, people can misuse it" (Respondent N, Age 31)

Most of the people confirmed that they have heard or read a lot of instances about the potential misuse of the information collected from devices. They had seen many videos on social networking platforms of such instances which adds to their concern. But they do not have any idea about the privacy threats they might expose themselves by giving information to apps. Classic economic literature assumes humans to be rational in all aspects of life (Gerber, et al., 2018). However, even in situations with full information, humans have limited mental resources to evaluate all possible options as per the theory of bounded rationality, i.e., cognitive limitations of both knowledge and computational capacity (Simon, 1982). In simple words, human beings are bounded by the limitation of processing all information in their hands. They are often uncertain about the risks associated with disclosure.

4.5.1 Information Asymmetry

Further probing on the same question, interviewees (N=17) stated that they are concerned that mobile apps are collecting too much information about them, but they are not sure of the potential risks. Bandara et al. (2017), in their studies, disclosed that information asymmetry is a major issue in the current digital marketplace, especially among mobile app providers.

It was observed from the interviews that even if individuals expressed their concern about privacy, they still disclosed because they are not aware of the potential consequences of such disclosure.

- "I'm not aware as to what potential misuse can happen with my information. For example, if my fitness band asks my weight, height, etc. I will give that information because I'm getting the benefit regardless of the risk." (Respondent G, Age 28)
- "Yes, we are not aware, so we are not bothered, many people don't know about privacy infringement." (Respondent N, Age 31)
- "I don't know the implications for sharing information on a mobile app. How much is being misused or sold." (Respondent A, Age 34)

When users' signup for an app they tend to share their information, but they cannot discern whether the mailing list might be sold to a third party or not, who could then send unsolicited messages (Bandara et al., 2020). They are in a position of information asymmetry to the party with whom they are transacting as also given in previous work (Bashir, et al., 2015 and Acquisti, and Grossklags, 2005). Technology is changing fast, and users are not able to cope with these growing threats. It is nearly impossible for users to fully assess what security and privacy vulnerabilities they might expose themselves to if they decide to interact with a given system (website/ mobile app). They are concerned but they are not aware of privacy threats, the intensity of risks, and how they can protect themselves. Thus 'information asymmetry' turns out to be one of the reasons for the existence of the privacy paradox.

4.6 Rational Reason for Privacy Paradox

To find the other reasons for the privacy paradox we tried to bring back the question of why smartphone users have downloaded applications (Talking about each installed app from the informant's phone).

Respondents gave varied reasons for downloading applications and information sharing, despite the inherent risks. Momentary answers were convenience, the app makes life simpler, promotions and discounts, to stay connected and get quick information. It was inferred that first people try to give logical answers to the choices they have made. All these reasons were categorized as rational reasons, where a person discloses information in exchange for social or economic benefit.

- "I need this app because I feel connected, it is easy and accessible." (Messenger app like WhatsApp) (Respondent D, Age 20)
- "If I'm getting a better deal with these apps like a free ride or a discounted movie ticket, I'm happy. I want the instant benefit." (coupon-based app Groupon) (Respondent C, Age 29)
- "I downloaded these apps because everybody is using them, else I would have never done." (Messenger app like WhatsApp) (Respondent P, Age 29)

Mobile users signed up and gave information in return for the benefits of a specific app which is claimed as the 'give to get the factor. The potential benefit seems more worthy to them in comparison to unanticipated risks. This cognitive trade-off among privacy risks and perceived benefits is known as privacy calculus (Dinev and Hart, 2006).

4.6.1 Privacy Calculus

Privacy calculus theory postulates that often perceived benefits outweigh the perceived risks, which results in disclosing information in exchange for social or economic benefit (Culnan and Armstrong, 1999). This theory is based on rationality and it assumes that individuals act in ways that will maximize positive outcomes and minimize negative ones (Stone and Stone 1990). The final behavior of individuals is determined by the outcome of the privacy trade-off (Jiang et al., 2013; Xu et al., 2011; Dinev & Hart, 2006).

Several studies concerning social networking sites have confirmed that an individual's intention and behavior to disclose information is based on a calculus whereby they consider inhibitors and drivers of information disclosure (Debatin et al., 2009, Lee et al., 2013 and Jozani et al., 2020). Smartphone users disclose information in return for the benefits of a particular app, ignoring the risks and privacy concerns (Kehr et al., 2014). They weigh the benefits of apps more than the risks.

- "We don't have to pay for WhatsApp messages whereas we have to pay for SMS. It is cheaper and wherever there is wifi, we can use WhatsApp for free. Apps are convenient, accessible, provide discounts. I'm calculative, I take informed decisions." (Respondent D, Age 20)
- "I need these apps. I feel connected. I look out for convenience and ease. In this case I know how much I'm gaining but no idea how much I'm losing." (Respondent K, Age 33)
- "I don't mind if these apps show me ads, they offer personalization based on my likings or preferences. After all, these apps are free so they will take something. And I don't know what I will lose, so when awareness increases about the misuse of information, I will do a better calculation." (Respondent C, Age 29)

Individuals are likely to give up a degree of privacy in return for potential benefits related to information disclosure. They tend to make a trade-off in their mind; based on which they try to maximize their potential gain of disclosure and minimize the expected loss of privacy.

4.7 Irrational Reasons for Privacy Paradox

Decades of psychological research have proved that individuals are ambivalent (Shrum, McCarty, and Lowrey, 1995) and do not always make rational decisions. Irrationality is the reality in human decision-making (Ariely, 2009; Simon, 1982). Keeping this aspect in mind, to answer the incongruity between privacy concern and privacy behavior we investigated irrational reasons along with the rational reasons for privacy paradox and found different explanations for the phenomenon.

It was obvious that consumers would not self-report their hidden motivations for downloading the app. To uncover their subconscious drive, we had to probe the respondents by asking indirect questions. We inquired about specific apps they downloaded and simultaneously tried to nudge them with their reported concern level again. To understand their biases and reasons for the paradoxical decision we probed informants of the reasons for disclosing personal information and concern level at the same time. Following were some of the explanations provided by the respondents.

4.7.1 Optimism Bias

One of the most common reasons observed for this paradoxical decision was unrealistic optimism (N=18). Optimism Bias refers to an underestimation of a belief by an individual that they are at less risk of experiencing a negative event compared to the others (Acquisiti, et al., 2015). Even if they are concerned about privacy, they tend to underestimate the chances of experiencing a negative event for themselves as compared to others. People tend to judge their vulnerability of a threat to be lower than that of their peers to encounter even privacy threats. Thus, they keep disclosing information despite privacy concerns.

- "I'm not an important person or a celebrity. What will these apps do with my information? I don't have any critical information. I'm not as worried until I'm personally attacked." (Respondent M, Age 27)
- "Why would anyone want to misuse my information, I'm not so important. What can happen to me as an individual?" (Respondent F, Age 54)
- "I'm not a very high-profile guy who is being monitored. Even if these app companies take my info what maximum they can do" (Respondent I, Age 34)

Studies across disciplines have shown unrealistic optimism is robust. It has been simulated in various risk assessment scenarios, such as when people misjudge their probability of being victims of a heart attack, auto accidents, earthquakes, bird flu, and negative Internet events (Campbell et al., 2007; Chapin, 2000; Shepperd et al., 2003; Wei, et.al, 2007). Baek, Kim & Bae (2014) through an online survey confirmed that individuals perceive their likelihood of privacy infringement to be lower in comparison to other individuals.

4.7.2 Bandwagon Effect

In this fast-paced digital marketing era even when individuals wish to act privately, they fall prey to use a particular mobile application or a social networking platform to achieve conformity with the admired peer group (Lutz and Strathoff, 2011). The desire of belonging to a social network overrides any fears of data misuse (Lutz and Strathoff, 2011). Individuals neglect privacy concerns and anchor their disclosure decisions based on what others have disclosed. In this study also we found that interviewees (N=12) reported downloading an application and use it because their significant others have downloaded it. They rely on their trusted peers' decisions and recommendations as a reference point for what is appropriate to download or post, regardless of their privacy concerns. Correspondingly individuals anchor their information disclosure decisions based on what others have disclosed (Leon et al., 2015). This is interpreted as the bandwagon/herding effect, a form of groupthink in social psychology.

- "I also see how many people have recommended those apps. Till the time everyone is using it, I'm okay. I'm not the only one sharing." (Respondent P, Age 29)
- "Major reason is if others have it so why not me. It is a status symbol. I downloaded Instagram based on recommendation." (Respondent M, Age 27)
- "Everyone uses PayTM. And when everyone uses, it makes it even more convenient." (Respondent B, Age 23)

4.7.3 Hyperbolic Discounting

In the case of privacy, the advantages of sharing private information may be instantaneous (convenience of using the application or service), but the cost of losing information or identity theft may be invisible and spread over future periods. (e.g., identity theft) (Acquisti, 2004). This tendency of hyperbolic discounting i.e., valuing future benefits less than present ones, has significant implications for privacy decision making (Acquisti, 2004). A positive present monetary gain often trumps privacy concerns. This was also confirmed from our in-depth interviews with the smartphone users (N=17). They are more interested in immediate offers or discounts regardless of high privacy concern levels. Some of the excerpts from the interviews are:

- "When I use these apps, this immediate benefit is more important, say to book a movie ticket it should be right now. It doesn't matter what information you are taking till the time I'm getting the benefit." (Respondent J, Age 24)

- "If an app is taking my info and giving me a benefit, I'm not bothered as to what it will do with my information after two years. Who knows when true colors will come out?" (Respondent 0, Age 28)
- "If I am getting deals or coupons by sharing information, I'm happy. I want instant benefit; I will give my information." (Respondent P, Age 29)

At this stage, it is important to understand that hyperbolic discounting and privacy calculus seem very closely related, but there is a difference between the two. In the case of hyperbolic discounting, the immediacy of benefits is considered (smaller-sooner reward over a larger-later reward); whereas in the case of calculus cognitive trade-off is considered. The above statements were categorized under the hyperbolic discounting theme due to the usage of the word 'immediately' or 'instantly'.

4.7.4 Status Quo Bias

Users forget that in the case of mobile applications if apps are lying dormant on phone, it is still using the information of the users, thus users end up losing a lot of information without realization. Many applications are designed in such a way that by default they access contacts, photo galleries, location, media files, and other accounts on the device. In our research as well, there were many users (N=11) who had default apps that were not used ever or not used for a long time, but they tend to ignore the same. On asking people if they have ever changed their privacy settings; the respondent replied.

- "I don't change my default setting. I do not take any action". (Respondent B, Age 23)

Thus, we could infer that even if users are concerned, they stick to default settings.

- "Yes, few apps are just lying on phone says Myntra (shopping app), I don't shop every day. I know Google has my information. I don't bother if these apps are just lying around." (Respondent G, Age 28)

. We could infer that they have inertia to change their privacy setting or learn about privacy protection mechanisms. People tend to resist change and 'go with the flow' of pre-set options, even when alternatives may yield better outcomes Thus, the privacy paradox can also be attributed to status quo bias where despite privacy concern subjects do not process all the information necessary to make informed decisions as they rather choose to satisfy themselves with default choices. Status quo bias refers to individuals' preference for being in the current state of affairs (Leon et al., 2015).

4.7.5 Sunk Cost Fallacy

Some respondents (N=6) stated that they disclosed their personal information despite privacy concerns because they had already shared similar pieces of information earlier. The information which has already been released, sharing it another time for another mobile application will not be counted as an additional cost. Respondents stated that:

- "I have already left so much digital footprint; anyone can hack me already. We buy sim cards, rent agreements, etc. From these documents, I have already left my information at many places." (Respondent A, Age 34)
- "There is already a lot of information about me on Facebook, Naukri.com, LinkedIn, etc." (Respondent C, Age 29)
- "Many people already know a lot about me, so it's okay to sign up for one more app" (Respondent H, Age 29)

We could relate this phenomenon to "Sunk Cost". Once resources (money, time, or effort) have been invested in a particular endeavor that cannot yield the desired result then throwing good money after bad is counted as a sunk cost (Garland, 1990). In the case of an online scenario, individuals have the feeling that they have already given their personal information at many places thus giving it one more time for using another service shall not lead to any further harm (Leon et al., 2015). Thus, even when people were concerned about privacy, they keep giving information to recover the sunk cost by using additional apps.

4.7.6 Peanut Effect

All the interviewees (N=18) in this study at some point informed that to get the benefit of the mobile application, disclosing basic demographic details like age, gender, phone number or emails would be a small price. These demographic details are referred to as peanut information for this study, as participants believe that disclosure of such pieces would not lead to any adverse negative consequences. Participants reported.

- "How much will I lose anyways, my phone number, email, name, age, etc. It is okay. I have a threshold. I can risk it as it is a small gamble." (Respondent R, Age 34)
- "Risk behavior keeps changing with the gambling stake." (Respondent N, Age 31)
- "It's okay if others know about my name, Date of Birth, phone number, email, gender, etc. It does not matter. What matters to me is a stake. So, I'm ready to gamble for small things, I think you should only put that much information that you are comfortable in sharing. Don't put your pricy possessions at stake." (Respondent M, Age 27)
- "I don't have much data, only the basic info which is okay if someone is using. I don't upload my photos in Google drive, etc. My liking, preferences, gender, everyone knows about me." (Respondent B, Age 23)

Markowitz (1952) noted that people are more willing to gamble when playing for 'peanuts' (small monetary amounts). People are more risk-seeking for smaller-stake gambles than for large stakes Thus, the peanut effect refers to a tendency to be more risk-seeking for smaller gambles, than for larger stakes (Prelec and Loewenstein, 1991). In the case of privacy decision making people tend to give basic or less sensitive information to obtain a benefit. Thus, the privacy paradox can be witnessed when privacy-concerned individuals disclose peanut information as a small gamble in exchange for a reward (Frederiks, et al., 2015). However, they forget that the cumulative effect of such smaller disclosures can add to their digital dossier which can be misused anytime in the future.

4.7.7 Fear of Missing Out FoMo

N=7 respondents also reported that they downloaded applications and disclosed their personal information despite privacy concerns because of Fear of Missing Out (FoMO). It is defined as "a pervasive apprehension that others might be having rewarding experiences from which one is absent" (Przybylski, et al., 2013, p. 1841). People have a belief if they do not have the app, they might miss the experiences which may be potentially rewarding for them. FoMO is characterized by the desire to stay continually connected with what others are doing (Przybylski, et al., 2013). This was also interpreted in our interviews with smartphone users as.

- "I downloaded WhatsApp because I want to be updated and move with time. I don't want to be backward. I don't want anyone to come and tell me that she doesn't know about WhatsApp". (Respondent F, Age 54)
- "I deleted Facebook account, but for the business purpose I had to reinstall. They are a lot of updates on Facebook." (Respondent D, Age 20)

- "I tried uninstalling the app but then felt that I would miss the fun" (Respondent L, Age 31)

4.7.8 Learned Helplessness

It was also found that even though people are concerned about privacy, they still give their personal information because there are no alternatives (N=12). Mobile operating ecosystems lead to a systematic provocation of paradoxical behavior by employing an all-or-nothing policy, whereby users must accept all permissions to download a particular app (Shklovski, et al., 2014). This could ultimately lead to the overall acceptance of privacy risks with the user's sense of inability and vulnerability to handle privacy invasion.

- "If Airtel (phone carrier) is selling information to a third party, I can't do anything; I cannot stop using the phone. What is the guarantee that Vodafone will not do it? I have to choose one of these." (Respondent A, Age 34)
- "Sometimes there is no choice but to give information. It might be due to legal compulsion or I need to use that app." (Respondent K, Age 33)
- "I don't think even alternative options are safe either. Even if I use the alternative say hike rather than WhatsApp, my friends won't be using that option, it's of no use as others don't have it." (Respondent Q, Age 36)

Users are submissive to the fact that they possess little power to change the situation anyway and suppress these negative feelings as part of the 'cost of doing business' (Bandara, Fernando & Akter, 2020). This condition is called learned helplessness in which a person suffers from a sense of powerlessness, arising from a persistent failure to succeed (Alloy and Abramson, 1982).

4.8 Trust as a Reason for Privacy Paradox

Smartphone users (N=16) in our study informed us that their concern level is reduced due to trust in the service provider, to protect and secure their information.

- "I trust Facebook and WhatsApp; they are registered and renowned. I have given my credit card details to wallet app PayTM. I don't feel unsecured, as nothing has happened" (Respondent B, Age 23)
- "I don't have a problem giving access until the company is reputed. I have a fear of unknown." (Respondent C, Age 29)
- "I trust these companies to some extent and also my abilities to manage privacy. I have the power to block those numbers which disturb me." (Respondent D, Age 20)
- "It's the company which has information about my location, not an individual, I trust these apps, only then I download." (Respondent L, Age 31)

It has been found in previous studies as well that Trust in the service provider is reckoned as a reason where people share their information despite concern. Trust is considered to be one of the simple decision-making heuristics in situations of uncertainty and risk (McWilliam, 2000). Consumers who trust a firm are more willing to provide personal information and less concerned about their privacy (Schoenbachler and Gordon, 2002; Wakefield, 2013).

4.9 Personality Type as a Reason for Privacy Paradox

4.9.1 Neophiliac Personality

There were (N=3) respondents who expressed that they are eager to use a service as soon as they get to know about a new technology or new app regardless of privacy concerns. They download regardless of information required and tend to overlook privacy statements.

- "I'm inquisitive about new apps, I download when someone recommends me. e.g. Limeroad (clothing app) I downloaded the app to try and then I deleted." (Respondent C, Age 29)
- "I'm inquisitive and I try new things. If there are some apps that I have not downloaded, I would like to know and try them once." (Respondent E, Age 26)

This is related to a personality type known as 'Neophiliac personality', people who are novelty-seeking individuals who belong to inquisitive temperament (Whitbourne, 2012). Similarly, those enthusiastic to use novel devices might bypass privacy agreements and disclosure conditions for the sake of using the app once. Even though they are concerned about privacy; they are impulsive.

5. DISCUSSION

5.1 Theoretical Contribution

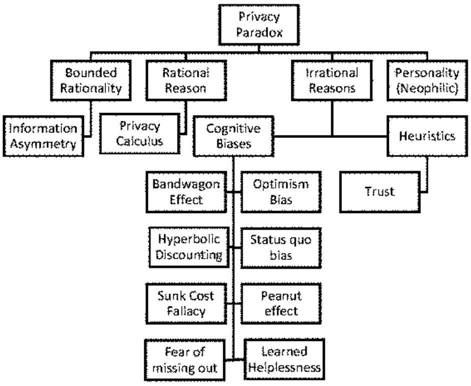
In an interconnected world where technology governs numerous aspects of our lives, privacy is inevitably embedded in our interactions online. It is not just a few paragraphs that are buried deep in the 'terms and conditions page of a website. Privacy infringement can impact a brand, disrupt the customer experience, and potentially damage a company's reputation. With the advent of smartphones and aggressive practices of data access, privacy concern among users has aggravated (Xu, et al., 2012). Although consumers increasingly protest against invasions of privacy, they routinely disclose more information than their disclosure intent. They articulate high privacy concerns, but they also voluntarily post vast amounts of information on the social network pages, tweets, or while signing up for mobile applications. The purpose of this exploratory study was to understand the reasons for this discrepancy between a consumer's stated privacy risk concern and their actual behaviours.

Current research has tried to bring logical explanations to this complex phenomenon by answering "why" this paradox exists amongst smartphone users. The analysis of in-depth interviews of eighteen smartphone users from different walks of life revealed that the privacy paradox exists. Earlier studies which have quantitively tried to answer this question; have not been empathetic to the fact that people try to give socially desirable answers to please the interviewer. Thus, in this study, we tried to apprehend the actual disclosure behavior, by interviewing smartphone users and finding out reasons for this paradox.

Apart from adding new facets to privacy paradox discourse, this study has comprehensibly mapped the cognitive biases apart from rational explanations as reasons for the privacy paradox. On finding different reasons for this paradox, we categorized each of these in different themes such as bounded rationality, rational explanations, irrational explanations in terms of cognitive biases, trust as a heuristic, and neophiliac personality. Some of these explanations have been found in previous works like information asymmetry (Bandara et al. (2017), Privacy calculus (Jozani et al., 2020), optimism bias (Acquisiti, et al., 2015), and Trust (Wakefield, 2013). However, we also figured out some reasons in this context of mobile computing in an emerging market like India which were not emphasized earlier in the privacy paradox literature like Peanut Effect, Fear of Missing Out- Fomo, Learned Helplessness, and Neophiliac Personality. This work brings together all the above reasons in a comprehensive framework.

There have been studies validating the existence of privacy paradox in general online contexts, e-commerce websites, and social networking platforms but studies exploring this gap among smartphone users are still diminutive. In an emerging country like India, with millions of smartphone users, and no legislative protective mechanisms for the privacy of data, the results of this research will help in designing policies that will aid in privacy protection among smartphone users. All the reasons for the privacy paradox that have been mapped can be considered in designing policies that are safer and more secure for mobile users to give them a more protective environment. The results have been summarized in Figure 1 below.

Figure 1. *Reasons for privacy paradox- Findings from the exploratory study*



5.2 Practical Implications

The results of this research have implications for multiple stakeholders including business leaders, privacy activists, scholars, government regulators, and individual consumers as information privacy is a mounting concern. The findings of the study i.e., the reason for the existence of privacy paradox can guide smartphone users to align their privacy concerns and with their disclosure behavior. Making them aware of the phenomenon will help them overcome this paradox and will help them make information disclosure decisions prudently, rather than getting manipulated by mobile apps and inconsiderately disclosing information. Users tend to forget the fact that small pieces of the disclosure can cumulatively add to a huge digital dossier which can be misused anytime in the future, as decisions about their lives can be taken in secret without awareness. Consumers will get benefited from this work as they would be able to defend the control of their decision making by becoming more conscious of their biases,

Not just smartphone users but for businesses also need to understand that privacy matters to customers. Online environments are built not only to constrain users but to coerce disclosure and trigger cognitive biases that encourage us to give up and cede control over our privacy. With the findings of this work, app creators can redesign platforms in a way that will provide a secure environment to mobile users. In this highly competitive environment, privacy protection can lead to an edge over the competition. A connection between users and service providers built on trust and transparency in data handling mechanisms would hold online platforms to a higher standard of loyalty, authenticity, and dependability.

The results of this research can aid marketers in designing interventions to gently guide users towards safer online practices. The implications of the study will range in the area of 'nudging research'. Almuhimedi et al., (2015) showed how daily nudges like informing the android user about the frequency with which their mobile apps access their sensitive data, can motivate them to review and modify permission settings. Privacy policies should be brief, user-friendly, and simple to comprehend. Along with crafting privacy awareness support systems, warning messages should be signalled to users that, they are equally vulnerable to an adverse situation as anybody else (Dogruel, 2019). The false perception of being less susceptible to privacy risks must be dismissed.

This study will also have implications in the area of 'soft paternalism' which is the study about interfaces and services which can be designed to counter biases responsible for disadvantageous security and privacy decisions (Chiasson et al. 2008; Acquisti 2012; Wang et al. 2014; Almuhimedi et al. 2015). The results can assist in developing choice architectures and user-orientated solutions in the form of usable privacy and security tools that protect privacy even if the information has been revealed due to biases. This will add value to the lives of consumers.

5.3 Limitations

One of the limitations of this exploratory study is that with only eighteen interviews taken in India, the results of the work are not generalizable to a large population. Privacy is a context-dependent phenomenon, and we should not expect individuals to demonstrate the same behavior in different contexts. Caution must be exercised in trying to generalize the findings of this work into different contexts. Thus, it remains to be seen whether the results of this study retain their validity with different contextual variables. A mixed-methods study may provide data triangulation and add to the rigor of this study.

Another inherent limitation of the in-depth interviews as a qualitative methodology is that due to human intervention, sometimes respondents tend to comply with the social norm and give answers to satisfy the interviewer. To overcome this issue, necessary consideration was taken by the interviewer like utilizing positive engagement techniques such as establishing rapport, knowing when to stay silent and let the interviewee talk freely, and asking questions that indicate the interviewer is listening carefully to the interviewee. For future research, these reasons should be empirically tested with a larger set of samples and measuring actual disclosure as the outcome variable.

5.4 Conclusion

In this study, we have tried to find reasons for the privacy paradox where smartphone users state that they are concerned about privacy, yet they disclose their information. With the eighteen interviews, we have found twelve reasons that explain this paradoxical behavior. Some of these reasons are rational explanations, whereas others are irrational reasons explanations in human behavior. In an emerging economy like India where there are millions of smartphones but no legislation to protect the privacy of phone users, this study adds new facets to the knowledge of how human beings make disclosure decisions despite privacy concerns. This work does not claim to change the behavior of people, but it does encourage people to make more conscious privacy decisions by balancing the optimum level of revelation and protection of data.

REFERENCES

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21-29). ACM. doi:10.1145/988772.988777

Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. *Digital Enlightenment Yearbook*, *2012*, 193–197.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi:10.1126/science.aaa1465 PMID:25635091

Acquisti, A., & Grossklags, J. (2003, May). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (*Vol. 3*, pp. 1-27). Academic Press.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision-making. *IEEE Security and Privacy*, *3*(1), 26–33. doi:10.1109/MSP.2005.22

Alloy, L. B., & Abramson, L. Y. (1982). Learned helplessness, depression, and the illusion of control. *Journal of Personality and Social Psychology*, *42*(6), 1114–1126. doi:10.1037/0022-3514.42.6.1114 PMID:7108740

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., & Agarwal, Y. (2015, April). Your location has been shared 5,398 times: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 787-796). ACM. doi:10.1145/2702123.2702210

Angwin, J., & Valentino-Devries, J. (2011). Apple, Google collects user data. *The Wall Street Journal*.

Ariely, D. (2009). The end of rational economics. *Harvard Business Review*, *87*(7-8), 78–84.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. doi:10.1016/j.chb.2013.10.010

Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013, July). " Little brothers watching you" raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (pp. 1-11). Academic Press.

Bandara, R., Fernando, M., & Akter, S. (2017). The privacy paradox in the data-driven marketplace: The role of knowledge deficiency and psychological distance. *Procedia Computer Science*, *121*, 562–567. doi:10.1016/j.procs.2017.11.074

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*, 101947. doi:10.1016/j.jretconser.2019.101947

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1–10. doi:10.1002/pra2.2015.145052010043

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2020). The impact of transparency on mobile privacy decision making. *Electronic Markets*, *30*(3), 607–625. doi:10.1007/s12525-019-00332-3

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. *Pew Internet & American Life Project, 4*.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological & Personality Science*, *4*(3), 340–347. doi:10.1177/1948550612455931

Brown, B. (2001). *Studying the Internet experience*. HP Laboratories Technical Report HPL, 49.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284. doi:10.1016/j.chb.2004.12.005

Chapin, J. R. (2000). Third-person perception and optimistic bias among urban minority at-risk youth. *Communication Research*, *27*(1), 51–81. doi:10.1177/009365000027001003

Charmaz, K. (2008). Reconstructing grounded theory. The Sage handbook of social research methods, 461-478.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181–202. doi:10.1007/s10799-005-5879-y

Chiasson, S., Forget, A., Biddle, R., & Oorschot, P. V. (2008). Influencing users towards better passwords: Persuasive cued click-points. *People and Computers XXII Culture, Creativity*, *Interaction*, *22*, 121–130.

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

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *The Journal of Social Issues*, *59*(2), 323–342. doi:10.1111/1540-4560.00067

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. doi:10.1287/isre.1060.0080

Dogruel, L. (2019). Privacy nudges as policy interventions: Comparing the US and German media users' evaluation of information privacy nudges. *Information Communication and Society*, *22*(8), 1080–1095. doi:10.1080/1369118X.2017.1403642

Frederiks, E. R., Stenner, K., & Hobman, E. V. (2015). Household energy use: Applying behavioral economics to understand consumer decision-making and behavior. *Renewable & Sustainable Energy Reviews*, *41*, 1385–1394. doi:10.1016/j.rser.2014.09.026

FTC. (2009). *Beyond Voice: Mapping the Mobile Marketplace*. www.ftc.gov/opa/2009/04/mobilerpt.shtm

Garland, H. (1990). Throwing good money after bad: The effect of sunk costs on the decision to escalate commitment to an ongoing project. *The Journal of Applied Psychology*, *75*(6), 728–731. doi:10.1037/0021-9010.75.6.728

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. doi:10.1016/j.cose.2018.04.002

Gliner, J. A., Morgan, G. A., & Leech. (2009). *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis*. Academic Press.

Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014, April). Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2647-2656). doi:10.1145/2556288.2556978

Jiang, Q., Ma, J., Li, G., & Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications*, *68*(4), 1477–1491. doi:10.1007/s11277-012-0535-4

Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, 106260. doi:10.1016/j.chb.2020.106260

Kehr, F., Wentzel, D., & Kowatsch, T. (2014). *Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure*. Academic Press.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. doi:10.1016/j.cose.2015.07.002

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), 862–877. doi:10.1016/j.ijhcs.2013.01.005

Leech, B. L. (2002). Asking questions: Techniques for semi-structured interviews. *PS, Political Science & Politics*, *35*(4), 665–668. doi:10.1017/S1049096502001129

Leon, P. G., Adjerid, I., Balebako, R., Brandimarte, L., Komanduri, S., Schaub, F., Sleeper, M., Wang, Y., Wilson, S., Acquisti, A., Cranor, L. F., & Sadeh, N. (2015, September). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *1*(1), 1–40.

Lutz, C., & Strathoff, P. (2014). *Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses*. Academic Press.

Markowitz, H. (1952). The utility of wealth. *Journal of Political Economy*, *60*(2), 151–158. doi:10.1086/257177

Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, *13*(6), 522–526. doi:10.1093/fampra/13.6.522 PMID:9023528

Mason, M. (2010, August). Sample size and saturation in Ph.D. studies using qualitative interviews. In Forum Qualitative Sozialforschung/Forum: qualitative social research (Vol. 11, No. 3). Academic Press.

McKeone, D. (1995). *Measuring your media profile: A general introduction to media analysis and PR evaluation for the communications industry*. Gower Publishing.

McWilliam, G. (2000). Building stronger brands through online communities. *MIT Sloan Management Review*, *41*(3), 43.

Michaelidou, N., & Hassan, L. (2014). *New advances in attitude and behavioral decision-making models*. Academic Press.

Morse, J. M. (2015). *Data were saturated*. Academic Press.

News 18. (2020, January 30). *Smartphone Users in India Crossed 500 Million in 2019, States Report*. Retrieved February 5th, 2020, https://www.news18.com/news/tech/smartphone-users-in-india-crossed-500-million-in-2019-states-report-2479529.html

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. *Psychology and Marketing*, *24*(10), 829–847. doi:10.1002/mar.20186

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x

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. doi:10.1016/j.chb.2016.09.005

Prelec, D., & Loewenstein, G. (1991). Decision making over time and under uncertainty: A common approach. *Management Science*, *37*(7), 770–786. doi:10.1287/mnsc.37.7.770

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, *29*(4), 1841–1848. doi:10.1016/j.chb.2013.02.014

Rosenberg, M. (2018, Mar. 17). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*(3), 2–16. doi:10.1002/dir.10033

Shepperd, J. A., Helweg-Larsen, M., & Ortega, L. (2003). Are comparative risk judgments consistent across time and events? *Personality and Social Psychology Bulletin*, *29*(9), 1169–1180. doi:10.1177/0146167203254598 PMID:15198085

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in-app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2347-2356). ACM. doi:10.1145/2556288.2557421

Shrum, L. J., Lowrey, T. M., & McCarty, J. A. (1995). Applying social and traditional marketing principles to the reduction of household waste: Turning research into action. *The American Behavioral Scientist*, *38*(4), 646–657. doi:10.1177/0002764295038004013

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99–118. doi:10.2307/1884852

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3). MIT Press.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems Quarterly*, *35*(4), 989–1016. doi:10.2307/41409970

Solove, D. J. (2008). *Understanding privacy*. Academic Press.

Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, *89*, 1.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, *8*(3), 349–411.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research*. Sage publications.

Taddicken, M. (2014). The ‘privacy paradox ’in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. doi:10.1111/jcc4.12052

Thurm, S., & Kane, Y. I. (2010). Your apps are watching you. *The Wall Street Journal, 17*(1).

Varnali, K., & Toker, A. (2010). Mobile marketing research: The-state-of-the-art. *International Journal of Information Management*, *30*(2), 144–151. doi:10.1016/j.ijinfomgt.2009.08.009

Wakefield, R. (2013). The influence of users affects online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. doi:10.1016/j.jsis.2013.01.003

Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014, April). A field trial of privacy nudges for Facebook. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2367-2376). ACM. doi:10.1145/2556288.2557413

Wei, R., Lo, V. H., & Lu, H. Y. (2007). Reconsidering the relationship between the third-person perception and optimistic bias. *Communication Research*, *34*(6), 665–684. doi:10.1177/0093650207307903

Whitbourne, K. S. (2012, March 6). *Are You a Neophiliac?* Retrieved March 5th, 2020 from https://www.psychologytoday.com/us/blog/fulfillment-any-age/201203/are-you-neophiliac

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. doi:10.17705/1jais.00281

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). *Measuring mobile users’ concerns for information privacy*. Academic Press.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O’Hara, K. (2013, May). Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463-472). ACM. doi:10.1145/2464464.2464503

Sakhhi Chhabra is a professor for Marketing at IIM-Sambalpur, Odisha. She is a PhD from MDI- Gurgaon and MSc. Marketing from Manchester Business School, UK. She has been teaching core and elective marketing subjects to post-graduate students and executives at various MBA institutes She has successfully published research papers, case studies, and book chapters in renowned International and National Journals. She has presented her research work at various reputed conferences in India and abroad.