Asia Pacific Journal of Information Systems
Vol. 28 No. 4 (December 2018), 258-273

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2018.28.4.258

To Reveal or Conceal? Understanding the Notion of Privacy among Individuals

Sana Ansari[a,*], Sumeet Gupta[b]

[a] *Ph.D Student, Management Information Systems, Indian Institute of Management Raipur, India*
[b] *Associate Professor, Department of Operations and Systems, Indian Institute of Management Raipur, India*

ABSTRACT

What is individuals' privacy notion, and does it change with the social roles taken up by them? We explored these questions using a qualitative interpretive research approach. We found that individuals have mixed notion of privacy. Individuals view privacy either as a commodity or as a control. Further, we found that an individual's privacy notion is a function of their social role within the society and their privacy preferences. Our research points to the importance of expanding the notion of privacy to encompass a broader understanding of privacy preferences. We theorize our findings using social penetration theory and presents a privacy model which provides the logical framework for interpreting people's views on privacy.

Keywords: Privacy, Self-disclosure, Social penetration theory, Social role, Interpretive research

Ⅰ. Introduction

In today's highly developed digitized society, it is easy to track a citizen, a consumer, or an employee. From good morning 'tweet' on Twitter to a private message on Facebook can reveal where in earth one is. This mysterious disclosure of location without the knowledge of user highlights the issue of privacy. Further, the networked world of technology heightens the concern for privacy as today's devices from electronic photo frames, recorders, to mobile phones have possibilities to access information, which further brings the issue of privacy management. This can be substantiated with a recent incident where Amazon's voice assistant Alexa, recorded and send personal conversations of a family to one of their contacts. The owner of the device was completely devastated and regarded the incident as *"a total privacy invasion. I'm never plugging that device in again because I can't trust it"* (Economic Times, 2018)[1]. Recent surveys too have revealed that privacy is a major concern for people in this digital age (Kokolakis,

*Corresponding Author. E-mail: sana.fpm2015@iimraipur.ac.in Tel: 918962206825

2017). However, this concern is paradoxical as these same people on one hand reveal their personal information over social networking sites and e-commerce sites for minute rewards and on other hand they get worried when e-commerce firms collect their information and product needs for their strategic promotions and profiling. This difference in attitude towards privacy and actual self-disclosure behaviour has led us to undertake this study by posing the fundamental question *"What is privacy for people?"*.

Despite the broader concern for privacy, there has been little work done on understanding the privacy (Bélanger and Crossler, 2011; Smith et al., 2011). The literature in Information Systems (IS) have predominately focussed on the concept of information privacy (Bélanger and Crossler, 2011; Pavlou, 2011), which mainly refers to understanding an individual's desire to control information about himself/herself. Understanding the information privacy in IS notion has been studied typically by focussing on samples pertaining to students and individuals from USA. Information privacy researchers in the past have found that individual's information privacy concern is reflected in their attitude, which in-turn, affects their preferences to use personalization (Chellappa and Sin, 2005), online transactions, willingness to get profiled (Van Slyke et al., 2006), and regulatory environment (Milberg et al., 2000). Various others try to identify the concerns individuals have from privacy practices followed by organizations (Smith et al., 1996). Despite the numerous attempts made by the previous scholars, the picture on privacy definitions and concepts is hazy and fragmented (Smith et al., 2011). Individuals engage in various roles in their life which results in the varied notions of privacy. Majority of the online users have refused to give out their personal information accurately on the websites due to their privacy concerns and have shown to avoid self-disclosure (Lwin and Williams, 2003). The focus of this paper is to present a picture which is not obscure and clears the clouds of doubt regarding what is privacy and how does this notion of privacy self-regulation vary among individuals.

Interplay of the status and role one has in the society constitutes the notion of privacy. Every individual has different take on privacy. Therefore, in order to understand it, we pose two research questions: (1) *What is privacy for people*? (2) *Does privacy notion changes with social roles*? This study discusses the privacy notion of people who occupy various positions in society as being a consumer, citizen, employee, or a family member. Mainly, this study highlights the boundary conditions of self-disclosure of private information. We have used social penetration theory as an appropriate lens to examine the self- regulation behaviour of an individual. We develop a privacy model, which helps in unbundling the self-disclosure boundary conditions for the individuals. Theoretically, we contribute to the literature by enhancing the understanding of the privacy spectrum as a function of individual self-disclosure and privacy preferences, practices, and concerns. Practically, we contribute by providing the marketers and e-commerce players with an understanding of their customer's privacy concerns and preferences.

The rest of the paper is organized as follows. First, the relevant literature on privacy and self-disclosure is presented. Next, theoretical and research approach for addressing the research question are described. The following section presents the general notion of privacy amongst the individuals. Finally, the paper

1) Reuters, May 25 2018, Amazon Alexa overhears family's private conversation, sends it to random contact, Economic Times, accessed on 1 June 2018; https://economictimes.indiatimes.com/magazines/panache/amazon-alexa-overhears-familys-private-conversation-sends-it-to-random-contact/articleshow/64313764.cms

concludes by presenting the interpretation of the data, drawing upon the social penetration theory.

Ⅱ. Literature Review and Theoretical Background

2.1. Privacy as a Construct

Privacy in literature in definitional form is classified into two different views, namely, value and cognition. Value-based view regards privacy as an integral part of the moral value of the society, which considers privacy '*as a right*' and '*as a commodity*'. On the contrary, cognitive-based view used in empirical research, considers privacy as individuals' cognition and perceptions, unlike value-based view which considers privacy as moral value or norms. Cognition-based view recognizes privacy '*as a state*' and '*as a control*'. We try to understand the notion of privacy amongst individuals. As per privacy *as a right* perspective, privacy is a human right (Milberg et al., 2000). According to the *commodity view* (Bennett, 1995), individual view privacy as a commodity which can be assigned an economic value to be considered in cost-benefit calculation. For instance, websites collect customer's personal information for understanding customer's needs in exchange for personalized gifts (Smith et al., 2011) or financial rewards (Wang et al., 1998). As per privacy *as a state*, privacy is considered as consisting of four sub-states, namely, anonymity, solitude, reserve, and intimacy (Westin, 1967). Finally, privacy *as a control* equates the privacy definition to ability to control (Westin, 1967). When individuals are comfortable with the management of their personal information, lesser are their privacy concerns (Sheehan and Hoy, 2000), which is more psychological in nature.

The extant literature has studied privacy both as a psychological as well as a behavioural concept (Margulis, 2003). Most of the research work on privacy is guided by the privacy theories provided by Altman and Westin (Margulis, 2003). According to Westin (1967), "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is a voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve.*"

As per Westin's definition, privacy is a dynamic process (Buchmann, 2014), wherein individuals try to control the flow of information i.e., "control of input from others" and "control of output to others". Manoeuvring of information includes act of concealing certain aspects of one's identity and revealing some aspects. This suggests that it is an individual's call on how they reveal themselves in front of the social world. Interplay of the status and role influences people's self-display. Moreover, societal and customary definition defines people's privacy preferences (Buchmann, 2014) and concerns (Pavlou, 2011). Privacy preferences means what, how, how much, where, and when people want to reveal or conceal information and varies from person to person (Buchmann, 2014).

Privacy concern has gained prominent focus by IS researchers as well in the last few decades (Bélanger et al., 2011; Cao et al., 2008; Pavlou, 2011). One of the reasons for the increase in the number of papers in privacy area is the transition from traditional to the digital era. However, most of the research in IS field hovers around "*how to preserve privacy*"

rather than "*what privacy is*" (Milberg et al., 2000; Smith, 2001). We in this paper try to bridge this gap by focussing on what is privacy for people and does privacy changes with different social roles. The reason these questions are crucial to examine because it helps us understand the paradoxical nature of humans. As individuals today openly compromise their privacy concerns for incentives on online platforms however remains sceptical in sharing information when asked offline. Moreover, individual's identity varies with the groups they belong to. Mostly they have multiple identities as being part of various groups simultaneously, be it lunch group, product development group or a work group. For instance, an individual share his personally, identifiable information freely on the internet. But when in a group which has social norms of not disclosing their information online, the person has to modify his risk beliefs in order to get socially recognized. This suggests that the social role individuals occupy has influence on their privacy behavior. Prior research also supports the positive impact of social influence in an individual's behaviour (Deutsch and Gerard, 1955). These questions thus, helped us unveil the exact attitude of individuals towards privacy and the role of social role in shaping the same.

As society transition towards digitization, literature raises the concern towards privacy. For instance, Mason (1986) raised serious ethical informational debate, and accurately predicted that increased reliance of society on information would increase concerns for privacy, accuracy, property, and accessibility. Later in 1999, dimensions of privacy were identified as the individual privacy, privacy of behaviour, communication privacy, and personal data privacy (Clarke, 1999). After the advent of digitization of information, researchers began treating personal communication and data privacy as a single construct and named it as *information privacy* (Malhotra et al., 2004).

The definition of Information Privacy has been explored heavily in the extant literature (Culnan et al., 1999; Malhotra et al., 2004; Smith et al., 2011; Smith et al., 1996). However, most of the definitions hover around information control and offer little variation. For instance, Smith et al. (1996) discuss information privacy under pillars of personally identifiable information storage and data collection, secondary usage of collected information, access of data to unauthorized people, and inadequacy of prevention of purposeful and inadvertent errors, whereas a few researchers define privacy around collection, processing, dissemination and invasion of information (Solove, 2004; Solove, 2008). Clarke (1999) ornately refers information privacy as an *individual's view on the usage of data about themselves by third parties through accessing control and granting possession permission.*

Information privacy researchers in the past have found that individual's information privacy concern is reflected in their attitude, which in-turn, affects their preferences to use personalization (Chellappa and Sin, 2005), online transactions, willingness to get profiled (Van Slyke et al., 2006), and regulatory environment (Milberg et al., 2000). Their research reveals that people are concerned about sharing personal information online (Vladlena et al., 2015). Online users adopt various privacy-protection measures to protect their personal information such as providing false information (Fox et al., 2000). Posey et al. (2013) highlighted protection motivation behaviours as an approach to understand privacy-protection measures. According to (Goodwin, 1991) privacy protection means *"managing the release of the personal information while diverting unwanted intrusions"*. Individuals may either take logical or use technological protection tools (software and hard-

ware) as a tool to self-regulate their privacy behaviour.

Most of the extant literature measure privacy as privacy concerns (Culnan, 1985; Malhotra et al., 2004; Pavlou, 2011) with an immediate focus on individual level. Apart from extensive focus on individual level of analysis, literature has also focussed on societal level with the main focus on regulation. Notable works are on market regulation pertaining to information privacy, and on protection of citizen's right to privacy through industry and government regulation (Bennett and Raab, 1997; Bowie and Jamal, 2006). In general, privacy concerns are associated with personality differences (Bansal and Gefen, 2010), cultural differences (Dinev and Hart, 2006), and demographic differences (Culnan and Armstrong, 1999; Sheehan and Hoy, 2000). Furthermore, it is found that individual differences impact privacy-related behaviour (Taddicken, 2014). Various individual differences such as gender (Hichang, 2010), culture (Bellman et al., 2004), internet experience (Bellman et al., 2004), and level of activity (Lewis et al., 2008) has been considered in the past. However, not much focus on individual's social roles and individual's self-regulation behaviour towards privacy notion has been examined yet. Researchers have tried to identify the concerns individuals have from privacy practices followed by the organizations (Smith et al., 1996). We try to expand the horizon of understanding on privacy by focussing on people's self-disclosure, privacy preferences, concerns, and practices they engage in. To do so, we use the theoretical lens of social penetration theory as discussed below.

2.2. Social Penetration Theory

Developed by Irwin Altman and Dallas Taylor in 1973, social penetration theory (SPT) was used primarily by communication studies while studying relationship bonding. SPT describes the process of making a relationship bond from superficial to more intimate (Altman and Taylor, 1973). According to this theory any relationship begins or deepens through self-disclosures. For instance, when people first start interacting with any website, be it e-commerce site, a government site, or a social networking site. People initially hesitate to share all their details publicly and once they gain confidence with the site and are satisfied with their handling of personal data, they increase they self-disclosure boundary. Self-disclosure can be applied in varied contexts including friendships, social groups, work relationships, and family relations. In case of computer-mediated communication SPT has previously been applied to the context of online dating (Whitty, 2008) and online communities (Posey et al., 2010).

SPT posits that *people assess interpersonal rewards and costs and satisfaction and dissatisfaction gained from interaction with others, and that the advancement of a relationship is heavily dependent on the amount and nature of the rewards and costs* (Altman and Taylor, 1973; Posey et al., 2010). In other words, SPT views privacy as a commodity. Altman and Taylor (1973), in their seminal paper laid down the onion metaphor to explain the concept of self-disclosure amongst individuals. Onion as a metaphor depicts the layers each individual possesses. Similar to onion, outer layers of an individual are visible and easily assessable to the outer world. As the layers deepen towards the centre, individual's vulnerability increases. The central layers contain information which a person shares with another entity only if the relationship deepens.

The case is similar to that of people on social media platform, whereby, initially while building their profile they reveal information which is easily assessable without much probing. Later as they be-

come comfortable on the site, people start sharing their personal thoughts and activities. Distal layers of individual's personality are not shed at once but opens up gradually as the relationship deepens. SPT talks of two important variables: depth and breadth. Depth is the degree of intimacy and breadth is the number of topics discussed.

With every information disclosed, vulnerability of an individual increases. The extent to which an individual wants to reveal the information depends on the cost-reward assessment (Posey et al., 2010). An information is shared when rewards outweigh costs. For instance, people reveal their information on e-commerce (or social networking site) site if they see the benefits of sharing the information. However, factors such as gender, religion, social status, culture inhibits one's self-disclosure behaviour. The cost calculus taken by individuals does not consider individual's social status and cultural inclinations into account. We argue that social status and cultural inclinations affect individual's privacy notion measured in terms of self-disclosure. To test our hypothesis, we tried to understand people's privacy notion, which helped in expanding the privacy spectrum by analysing people's privacy preferences, concerns, and practices.

Ⅲ. Research Approach

In order to test the hypothesis, we conducted semi-structured interviews (refer <Appendix A> for interview questions). As we are interested in testing influence of social status and roles on privacy self-disclosure behaviour, we selected housewives, students, software engineers, teachers, and bank employees as respondents for this study. We talked to 12 respondents for understanding their views on privacy. Descriptive statistics of the respondents are presented in <Table 1>. The questions asked to all 12 interviewees remained the same. However, some additional questions emerged as we proceeded with the interview. During the entire duration of the interview, we made sure that interviewees did not feel pressured and were comfortable in answering the questions. Furthermore, the word *privacy* was never revealed to the interviewees during the discourse. Rather we were trying to make sense of their ideas on privacy based on their behaviour of revealing and concealing information using interpretive research technique. The subsequent section outlines individual's views on privacy by describing what is privacy to them as being a consumer, an Indian citizen, an employee or a caring family member. The reason we are considering different roles into account so as to obtain a clear picture of an individual's privacy notion spectrum and to understand if privacy is just treated *as a commodity, as a right, as a state,* or *as a control* by individuals. Mostly, as an individual as a customer might reveal (or conceal) more hidden information in a hope of getting personalized attention but not reveal as much as an employee.

<Table 1> Descriptive Statistics of Respondents

Variable	Category	Frequency (%)
Gender	Male	5 (41.67%)
	Female	7 (58.33%)
Age	Under 30	8 (66.6%)
	Above 30	4 (33.33%)
Total		12 (100%)

Ⅳ. Privacy and Its Notion Amongst Individuals

4.1. As a Customer

"Marriage is around the corner and I haven't finalized my dresses...but why am I getting these obnoxious mails from Amazon....now whole Facebook page is filled with advertisements of dresses I have window shopped online. This is now allowing me to live freely."

The above are the feelings of a distressed female customer. The enormous usage of digital marketing and recommendation systems by e-commerce sites for making a customer's life easy is actually invading people's life. However, it may not be true as another customer who works as a software engineer holds the contrary view and states that, *"I like receiving them as it helps me in knowing the offers and at times help me in grabbing great deals. In fact, I bought my recent mini Bluetooth speakers because of personalized offer given to me."*

Simultaneously, there seems unanimity amongst the participants regarding the trust they have on the e-commerce brands known to them. People are comfortable revealing their mail address, residential addresses and phone number on these well-known established sites as they feel that information can hardly be misused. One of the customers mentions that "*I always think twice before revealing my details especially my contact number to the lesser known sites... I don't think mail id can cause any harm. But, I give my mail id which is not linked to my bank accounts as it helps me get offers and discounts*."

Contrary to the trust factor people have on e-commerce platforms regarding personal information being used sensibly, they do not have the same amount of trust when it comes to saving their cards on online shopping portals. This is revealed in the following excerpts.

Interviewer: *Do you have your debit/credit cards details saved on Amazon?*

Customer 1: *No, due to cyber security issues. The thing is that if cards are stored on sites, then there is a probability that the card and password combination might get hacked.*

Customer 2: *I particularly am afraid regarding credit card information being stored on Amazon website. Generally, whenever I do any transaction through credit card, immediately once the transaction is done, there will be a call, saying that they are calling from such and such credit card company, telling that you are using so and so credit card, and we would like to offer you another credit card, for which we require certain information. This phone call happens immediately after any credit card transaction; and it's not authorized. Because of this reason, I generally don't prefer to use credit card, I use it only when no other option is available. In credit card, such a foul game always happens. So, I fear that some third party will use my data without my permission.*

Customer 3: *Yes, I do have saved my card details. However, those details cannot be used unless I enter my CIV (Card Identification Value) information, which is available only with me.*

Customer 4: *I only prefer COD (cash on delivery), as I am afraid to operate through net banking, and I 'm not even aware that there is a provision to save cards as well.*

This passage shows that there is a clear distinction regarding which information people want to reveal. Most of the people are worried revealing their financial information, even on the sites which they find trustworthy. However, there seems no dissonance in the disclosure of demographic information, including residential address, mail id and contact number in exchange of personalized offers and discounts.

4.2. As an Indian Citizen

People are aware that all of their demographic information, financial transactions, and biometric details (for Aadhar card holders) are available with the government. In spite of that people have no fear of losing information or information being misused by the government because of the immense trust they have on the system. They are free to share the information which is not private if requested by the government. The following excerpt depicts this.

Interviewer: *What type of information you are willing to share with the government?*

Interviewee: *I can give my details but not the private ones. For example, if they ask me about my girlfriend, I am not willing to share it. I can share any official details.*

Though people are happily willing to share their official information with the government but when comes to the method of the data collection used by the government, it bothers them. As one of the interviewees mentions "*I am hesitant to share my details when a third party is involved in collecting information on behalf of government. I feel more secure when I have to fill data directly in the form (online or offline) and directly have to submit it on the prescribed centre/ website*."

This suggests that digitization of the data collection process for any governmental scheme will enhance its transparency and trust for the scheme. Of course, this requires a cautious attitude by the government for ensuring data security.

4.3. As an Employee

Most people as employees prefer to reveal most confined information to their employer. Most

of the participants in case of relocation have not informed their updated residential address. While for the central and state government employees, employer has all of the information as that of government. Most employees have added their parents and spouse as their dependents for accessing benefits of health insurance. Respondents stated that they reveal only such information to their employers which is beneficial for them in professional career.

This suggests that when sharing information with the employer, people have greater restrictive boundaries as compared to when they are in the role of a customer. Also, people make calculative moves.

4.4. As a Family Member

Most of the participants were puzzled when the question "*What does your family know about you?*" was put forth to them. The immediate response received was "*Everything*". However, after a deeper thinking, people started opening up and revealed that mostly family knows about their eating preferences, as their family members always poke them asking what they would like to have. The question mostly comes from their mothers.

One of the participants responded "*Almost everything. They know my preferences. They know What I like and what I don't like. What kind of person I am though not completely because recently I have been away from my family for last six years. They don't probably know what kind of person I am right now. But yeah, the basic taste and basic nature I have, like my temper, my favourite food, my dislikes, the way I react to situations, the way I talk to people. So, they know basic information about me*".

This passage suggests that, individuals though very close to their family, reveal information mostly about

their preferences and nature. However, there are possessions which they confine it to themselves. Clearly, it is evident that people have less privacy concern when it comes to family. Next section tries to explore what forms the privacy attitude for an individual.

4.5. The Interpretation of Privacy

This section first defines privacy for individuals through a hierarchal model. Later privacy model is developed to understand the notion of privacy.

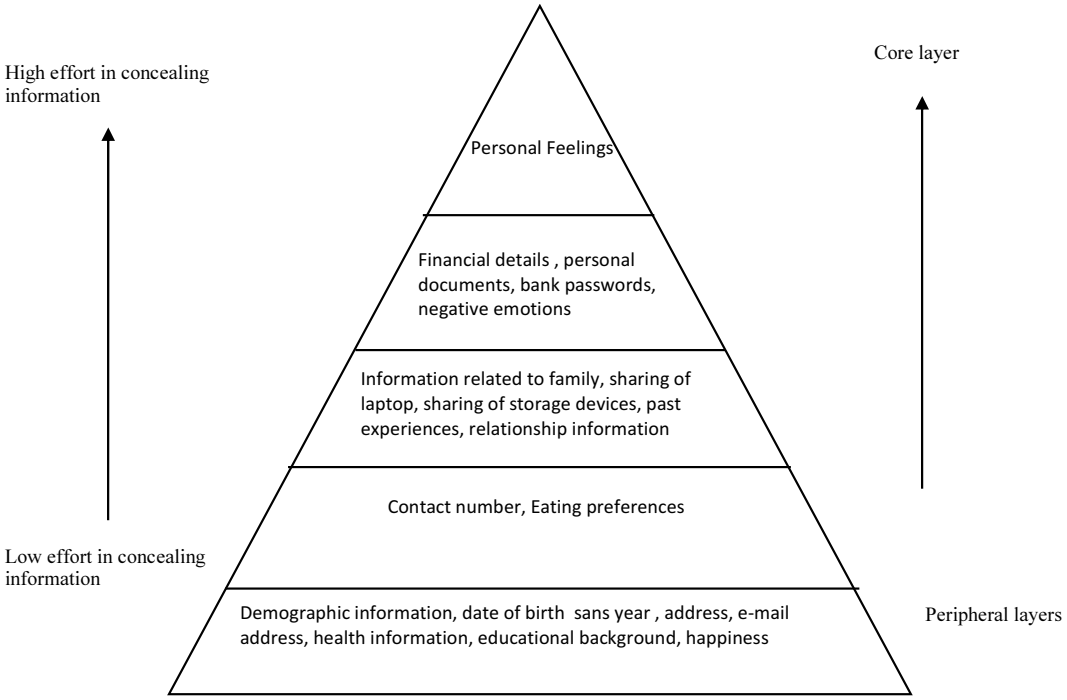
4.5.1. What is Privacy

There are certain matters which people try hard to conceal. For instance, revealing financial details at times occupies low status than revealing personal feelings. One of the interviewees mentions: "*I prefer to write about my feelings in diary. Initially I used to write in a diary. But now I write in random places, mostly in my laptop, which is password protected. It's not very easy for any random stranger to make out my thoughts and views from that. It's only me, who can club the pieces of puzzle, and justify my feelings.*" This suggests that people don't anticipate the fear of information misuse by others while they try to conceal it as much as they can due to the fact that they consider it as a signal of freedom.

Another instance depicts different notion of privacy, according to a respondent "*I prefer not to reveal my shopping expenses to others. Also, I do not share the contents which is likely to upset/disturb my husband, this could also include my shopping expenditure. At times I lower the shopping expenditure, if it exceeds my upper limit and then reveal it to my husband. I always want to portray a good picture to my family or for husband. I would never reveal any bad experience of mine with them as it may disturb them.*"

Privacy, if looked into the above statement, will include all those feelings which are likely to stress one's life. Like for example in this case, the respondent discusses shopping expenditure, which at times can cause trouble in her life. Thus, she prefers to reveal all such information which portrays a good picture about her. Moreover, privacy notion also includes protecting all that information which helps people avoiding misperceptions and judgement against them. There are other feelings which are also not known to the inner circle of the individual. For most people future career aspiration plans, negative emotions; stress, bank passwords, mental state, personal documents, including photographs; financial documents involving investment and salary slips are hard to reveal. From the above discussions, it is clearly revealed that the notion of privacy amongst individuals vary depending upon the role they are assuming. Family occupies the position where people have lowest concern revealing their privacy with. While as an employee they have highest concern revealing their information to their employer. Thus, it implies that individual's privacy notion shifts with transition in the role in life. Additionally, people have informed consent issue, which means they get offended, if their information is being shared by a third party in the absence of their knowledge. Based on the findings from the interviews, we developed a hierarchal model of information disclosure (<Figure 1>).

It can be inferred from the interviews that people mostly view notion of privacy as a mix of *commodity and control*. In other words, people like to receive the benefits of revealing information in most of the cases but enjoy further if the revealed information is in their control. Further, it can be seen that people's social roles influences their privacy notion. Individuals are subjected to think and follow as per their peers. For instance, an individual explained that due to



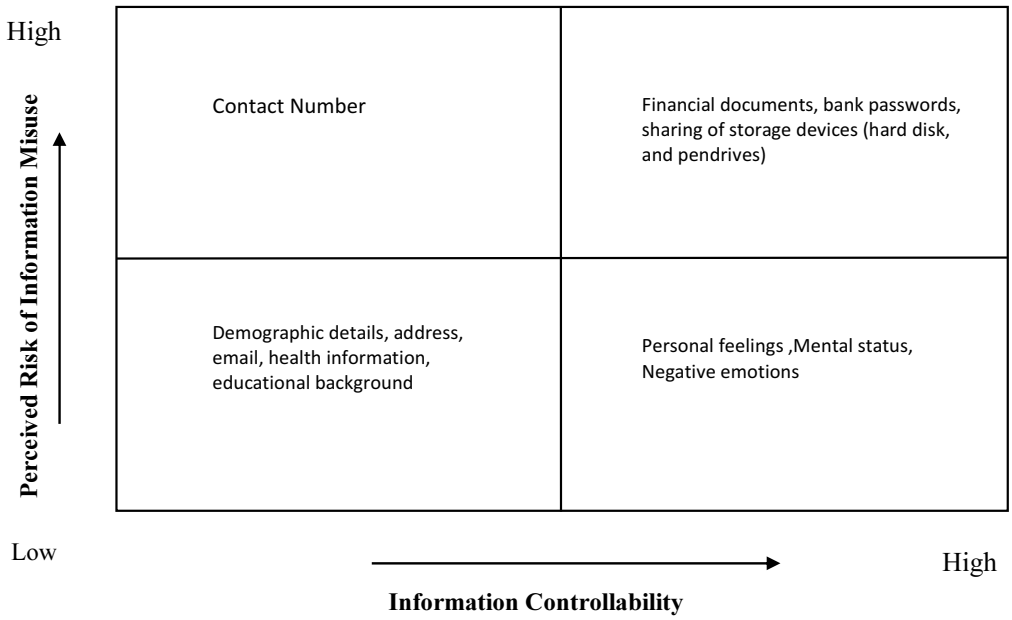
<Figure 1> Hierarchical Model of Privacy Concern Among Individuals

his office colleague he always locks his computer system before going for a break even as short as five minutes. The same individual agreed that he prefer revealing his personal system passwords to friends and family if required. This suggest that social role as an influence on individual's privacy.

As per social penetration theory we have presented the model of privacy preferences in five step hierarchal form. Of which people have higher concern in revealing the stuff occupying the peak position, that is, it requires more effort from an individual to conceal them. The items occupying top positions describe the core of an individual's personality. While the one at the footstep requires lesser effort in terms of concealing.

Based on the interpretations and open coding, we identified two parameters, *information controllability* and *perceived risk of information misuse* (<Figure 2> presents the privacy model). These two parameters are also consonant with SPT and privacy definition. Information controllability means the effort one puts in to conceal the information. While perceived risk of information misuse can be defined as the risk one believes one has in information being misused by others if revealed.

Information occupying low information controllability and low perceived risk of information misuse quadrant implies people easily reveal this information assuming lower risk of getting information being misused. On the other hand, people try hard to conceal the information regarding personal feelings (what one is thinking about) but perceive it to have lesser risk of being misused. Moreover, despite the higher perceived risk of information misuse, individuals put less effort in concealing their contact number. A mobile application which enjoys the priv-



<Figure 2> Privacy Model

ilege of accessing one's contact list increases the risk of contact number being misused by third parties. Financial documents and transactions fall in the quadrant where both perceived risk of information misuse and information controllability is high.

Ⅴ. Discussion and Implication

The objective of the study was to understand the notion of privacy and to examine if the notion varies with the different social roles undertaken by an individual. Studies on self-disclosure have previously focused on understanding what leads people to share knowledge in online communities (Chiu et al., 2006), and how to foster trust among customers who discloses their information in online platforms (Porter and Donthu, 2008). The studies on privacy in IS have focussed primarily on regulation (Bennett and Raab, 1997; Milberg et al., 2000; Smith, 2001). Milberg et al. (2000) found that if consumers are not satisfied with the way firm is protecting their privacy well, they then distrust self-regulation and prefer government regulation. On the cultural level, some studies have compared privacy laws of United States (U.S.) and Europe with the view to understand the notion of privacy *as a right* versus *as a commodity* (Jentzsch, 2001; Smith, 2001). It was found that European privacy laws are more inclined towards right view as compared to U.S. However, these studies have larger focus on the countries laws over the individual's privacy notion. Therefore, we in this study tried to focus on individual's privacy notion. We find that individuals have mixed notion of privacy, that is, their view towards privacy is both of commodity and control. One view dominates at a time, although, it fluctuates as per human needs. Next, we examined the influence of social role in the notion of privacy. The results reveal that the privacy notion of an individual is a function of an individual's role in the

society and their privacy preferences. Our hierarchical and privacy model enhances understanding on privacy spectrum of an individual. In summary, our results suggest that individual's self-disclosure and privacy notion is a function of social role and privacy preferences and they view privacy either as a right or as a commodity as per their privacy preferences.

The study has a few interesting implications for theory as well as practice. Theoretically, we contribute to the literature by enhancing the understanding of the privacy spectrum as a function of individual self-disclosure and privacy preferences, practices, and concerns. Further, we contribute by enhancing our understanding about the notion of individual's privacy and explaining the role of social role in shaping attitude towards privacy in general thus adding to the IS literature explain privacy paradox. Practically, we contribute by providing the marketers and e-commerce players an understanding of their customer's privacy concerns and preferences. E-commerce websites can create marketing strategies to target customers based on their social roles. For instance, during office hours individual is a employee and might have privacy reservations but after office hours when individual is with family might relax those reservations. Thus, targeting and recommending products as per the browsing hours of an individual might help e-commerce websites to churn more customers.

Ⅵ. Conclusion

In this paper, we have tried to present the various notion of privacy amongst the individuals. Till date not much focus has been given to an individual's social role and individual's self-regulation behaviour towards privacy. We in this study tried to expand the horizon of understanding on privacy by focussing on people's self-disclosure, privacy preferences, concerns, and practices using the theoretical lens of social penetration theory. The research can be further extended by implementing the symbolism framework identifying the magic, metaphor and myths related to privacy.

<References>

[1] Altman, I., and Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Holt, Rinehart & Winston.

[2] Bansal, G., and Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

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

[4] Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

[5] Bennett, C. J. (1995). *The political economy of privacy: a review of the literature*. Hackensack, NJ: Center for Social and Legal Research.

[6] Bennett, C. J., and Raab, C. D. (1997). The adequacy of privacy: The European Union data protection directive and the North American response. *The Information Society, 13*(3), 245-264.

[7] Bowie, N. E., and Jamal, K. (2006). Privacy rights on the internet: self-regulation or government regulation? *Business Ethics Quarterly, 16*(3), 323-342.

[8] Buchmann, J. (2014). *Internet Privacy: Options for adequate realisation*. Springer Science & Business Media.

[9] Cao, J., and Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

[10] Chellappa, R. K., and 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.

[11] Chiu, C.-M., Hsu, M.-H., and Wang, E. T. G. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems, 42*(3), 1872-1888.

[12] Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM, 42*(2), 60-67.

[13] Culnan, M. J. (1985). The dimensions of perceived accessibility to information: Implications for the delivery of information systems and services. *Journal of the American Society for Information Science, 36*(5), 302-308.

[14] Culnan, M. J., and Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

[15] Deutsch, M., and Gerard, H. B. (1955). A study of normative and informational social influences upon individual judgment. *The Journal of Abnormal and Social Psychology, 51*(3), 629-636. https://doi.org/10.1037/h0046408

[16] Dinev, T., and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

[17] Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., and Carter, C. (2000). Trust and privacy online: Why americans want to rewrite the rules. pew internet & american life project, washington. *The Pew Internet and American Life Project, 2*, 1-29.

[18] Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 149-166.

[19] Hichang, C. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security, 6*(1), 3-27.

[20] Jentzsch, N. (2001). The economics and regulation of financial privacy: A comparative analysis of the United States and Europe. *John F. Kennedy Institute For North American Studies. Working Paper*, (128).

[21] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

[22] Lewis, K., Kaufman, J., and Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1), 79-100.

[23] Lwin, M. O., and Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters, 14*(4), 257-272.

[24] Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

[25] Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*(2), 243-261.

[26] Mason, R. O. (1986). Four ethical issues of the information age. *Mis Quarterly*, 5-12.

[27] Milberg, S. J., Smith, H. J., and Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

[28] Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977-988.

[29] Porter, C. E., and Donthu, N. (2008). Cultivating trust and harvesting value in virtual communities. *Management Science, 54*(1), 113-128.

[30] Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

[31] Posey, C., Roberts, T., Lowry, P., Bennett, B., and Courtney, J. (2013). *Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors*.

[32] Sheehan, K. B., and Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

[33] Smith, H. J. (2001). Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review, 43*(2), 8-33.

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

[35] Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.

[36] Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NY, US: NYU Press.

[37] Solove, D. J. (2008). *Understanding privacy*. Cambrige, US: Harvard University Press.

[38] 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.

[39] Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Associate for Information Systems, 7*(6), 415-444.

[40] Vladlena, B., Saridakis, G., Tennakoon, H., and Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies, 80*, 36-44.

[41] Wang, H., Lee, M. K. O., and Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70.

[42] Westin, A. F. (1967). *Privacy and freedom*. New York: Athenaeum.

[43] Whitty, M. T. (2008). Revealing the "real"me, searching for the "actual"you: Presentations of self on an internet dating site. *Computers in Human Behavior, 24*(4), 1707-1723.

<Appendix A> Interview Questions

1. Which the most frequently e-commerce site used by you?
2. What does the above mentioned site know about you?
3. How do you go make transactions on this site?
4. If using credit/debit card? Do you prefer to save cards for future ease of transaction ?
5. What all your family knows about you?
6. What does government know about you?
7. What type of information are you willing to share with the government?
8. What does your employer know about you?
9. What are the stuffs you prefer to keep it to yourself?
10. Do you have fear of getting your personal information being misused by the government/ e-commerce sites?
11. How do you manage your personal documents?
12. Do you share your laptop with others?
13. If no, then why?

◆ About the Authors ◆

Sana Ansari

Sana Ansari is a doctoral scholar in the area of Management Information Systems at the Indian Institute of Management Raipur. Her areas of interest are e-commerce, social media usage for collective action, and online reviews manipulation. Her work has been published in the proceedings of 22nd Pacific Asia Conference on Information Systems (PACIS) 2018.

Sumeet Gupta

Sumeet Gupta is currently affiliated with the Indian Institute of Management Raipur as Associate Professor and Chairman (Research). He received his PhD (Information Systems) as well as MBA from the National University of Singapore. His research interests include electronic governance, e-commerce and business analytics. He has worked on several high profile national and international consultancy assignments such as with SAP A.G., DFS Gallerias, ASEAN secretariat and EDB Singapore. His work has been published in top tier international journals such as Journal of Management Information Systems, Decision Support Systems, European Journal of Operations Research, Omega and at international conferences. He is also a reviewer for top tier international journals in the field of information systems.

Submitted: March 8, 2018; 1st Revision: July 15, 2018; Accepted: October 8, 2018