

# "Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond W.E.I.R.D

Sheza Naveed

22100121@lums.edu.pk

Lahore University of Management Sciences  
Pakistan

Mobin Javed

mobin.javed@lums.edu.pk

Lahore University of Management Sciences  
Pakistan

Hamza Naveed

22100151@lums.edu.pk

Lahore University of Management Sciences  
Pakistan

Maryam Mustafa

maryam\_mustafa@lums.edu.pk

Lahore University of Management Sciences  
Pakistan

## ABSTRACT

We explore privacy perceptions, beliefs and practices of low-literate, low-income users in Pakistan, a patriarchal and religious context with a literacy rate of approx. 68% and where 59% of mobile users have less than 6 years of formal education. Through a qualitative study with 40 participants (17 male and 23 female) we examine the cultural, religious, and familial structures that impact users perceptions, management, and control of their personal privacy. We reveal significant gendered differences in privacy understandings, privacy preserving practices and the access to privacy related knowledge. Our work also highlights the seminal impact religious beliefs have on men and women's understandings and management of privacy and the prolific use of after-market modified apps to support users specific privacy needs. The privacy concerns raised by our participants provide HCI researchers with valuable insights into designing privacy affordances for vulnerable and diverse populations beyond Western, educated, industrialized, rich and democratic contexts.

## CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**.

## KEYWORDS

privacy, South Asia, patriarchy, religion, gender

### ACM Reference Format:

Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. "Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond W.E.I.R.D. In *CHI Conference on Human Factors in Computing Systems (CHI '22)*, April 29-May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 17 pages. <https://doi.org/10.1145/3491102.3501883>

---

The first two authors contributed equally to this paper.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9157-3/22/04...\$15.00

<https://doi.org/10.1145/3491102.3501883>

## 1 INTRODUCTION

This paper explores the privacy perceptions, mechanisms and behaviours of low-literate, low-income populations in Pakistan. Mobile device ownership along with access to an Internet connection has significantly grown in the last five years [19]. The year 2020 was extraordinary in which the significance of universal connectivity and access to critical information and opportunities was highlighted because of a worldwide pandemic. In much of the Global South, the mobile is the primary means for people to access the Internet, accounting for 85% of total broadband connections [29]. Additionally, South Asia has one of the world's largest populations with India, Pakistan, and Bangladesh alone home to more than approx. 26% of all people [57]. The pandemic has accelerated not only the rate of mobile phone adoption but also the adoption of digital services, online social networking sites for social commerce and digital financial services [35]. As more and more people come online and gain access to devices and the Internet in contexts beyond Western, educated, industrialized, rich and democratic (WEIRD) populations, it is vital to understand privacy perceptions, mechanisms, behaviours and beliefs of diverse populations in non-Western contexts.

There has been a great deal of focus in the last several years on understanding privacy behaviours and perceptions of users in the Global South [23, 48, 61, 62]. Much of this work has focused on the intersection of privacy and gender revealing the privacy practices of women in patriarchal and restrictive contexts India like Bangladesh and India. We build on and expand this work seeking to understand the privacy mental models, behaviours and privacy-preserving mechanisms amongst low-literate men and women in Pakistan. A recent report reveals Pakistan to have the lowest ICT skill levels across South Asia [35]. Unlike prior work, in addition to focusing on privacy behaviours we also explore the *norms*, *beliefs* and *value* systems that dictate privacy perceptions and practices in patriarchal, non-secular contexts like Pakistan. Johnson describes the patriarchal system as an "arrangement of shared understandings and relationships that connect people to one another", defining certain values and behaviours as expected and appropriate [36]. We explore how these pre-defined norms of appropriateness impact the privacy perceptions and behaviours of not just women but also men (whose values are also embedded within the patriarchal structure).

Prior work in HCI has also revealed the significant impact the Islamic faith has on the specific ways technologies are understood,

adopted and leveraged in Islamic communities [33, 51, 52]. In particular, the belief in *Purdah* (covering), which extends beyond just a physical covering but also implies a modesty in thought and act. Our work then, is situated across across multiple overlapping intersections; low-literacy, patriarchy, gender and religion. Our work adds to the existing privacy understandings for designing with diverse values and vulnerabilities (poverty, low-literacy, low digital skills) in non-WEIRD contexts.

In this paper, we draw on qualitative data from 40 interviews to reveal the understandings of privacy amongst low-literate men and women in Pakistan, how privacy is defined in this context and the mechanisms employed to maintain privacy on smartphones and different applications. While we situate our work using existing privacy frameworks [45, 54] we also reveal the challenges of using any one framework to analyse the privacy norms in a context deeply rooted in power imbalances. These imbalances (e.g. gender) create vulnerabilities which if not accounted for in privacy design might lead to the further marginalization of an already vulnerable population. Our work makes three unique contributions: 1) reveals the patriarchal norms and religious values that determine how boundaries are enacted and how privacy is defined, 2) within this understanding of appropriate behaviours explores how privacy is enacted and what strategies are employed by low-literate men and women to navigate the norms and perform privacy, and 3) presents design implications to include non-secular values, to help vulnerable groups in navigating pre-determined norms and empowering low-literate users to leverage privacy affordances.

## 2 RELATED WORK

Our work builds on existing privacy frameworks and previous research on user's privacy perceptions, mental models and privacy-preserving behaviours and practices. Although much of this prior research has focused on privacy from the perspective of Western, educated, industrialized, rich and democratic populations [9, 41], research in recent years has also explored privacy behaviours in the Global South [40, 62]. As researchers and designers work to understand the beliefs and values that determine privacy expectations and subsequent behaviours there is risk that privacy frameworks and methodologies omit alternative and diverse perspectives toward privacy. An essential first step in designing for privacy must inherently begin with an understanding of what privacy means to those who will use and be impacted by the use of the technology [27]. Our work builds on a growing body of work that explores privacy perceptions beyond the Global North, and presents the first data from Pakistan

### 2.1 Privacy Understanding and Frameworks in the Global North

Privacy is a significant concern for most people in the Global North [3, 53] and is not seen as static but an evolving concept where people assign different levels of importance and need for privacy to different applications and data [13]. For example, photos, videos and contacts are considered particularly valuable and private [49]. Additionally, users are more concerned about privacy leaks and unauthorized access of devices by insiders as compared

to strangers [50] and frequently block family members from viewing their photos and personal data [14]. Some of the most significant challenges to enacting boundaries and preserving privacy are shared devices and passwords within households which lead to complex privacy-preserving strategies, privacy expectations and behaviours. Research reveals that device sharing behaviours can be categorized into two main types; conspicuously i.e., using someone's phone with permission and stealthily, using someone's phone without permission [68]. A study across 99 English speaking households in the US reveals that what users often think of as "personal" devices or accounts might not be personal in practice. The study in particular highlights the 'invisibility' of sharing behaviours due to the unplanned nature of certain practices like borrowing or helping [44]. Such behaviours then require additional measures to be taken in order to preserve privacy.

Studies also reveal the specific types of privacy features most frequently used and their efficacy in users' perceptions of the safety of their data. In Germany, for example, a study revealed that people who used a screen lock found it unnecessary in 24.1% of the situations [32] and did not feel that pins provide adequate security [13]. Other studies, such as the one done in Canada revealed that people did not use a screen lock because of the social discomfort of using a lock in situations where trust was implied, such as in front of friends, [50], remembering a pin and typing it every time to unlock their phones was burdensome, and there was a lack of "motivation, convenience and concern" [25]. Such factors that hinder people from adopting privacy-preserving measures, regardless of the fact that they wish to, require modifications in the existing technologies to ensure inclusivity.

Lists and groups on social media such as Facebook also affect privacy behaviours. A study in UK showed that people prefer automatic grouping because manual grouping would be tiresome, despite realizing that it won't be very accurate [37]. Focus group findings in Germany showed that highly granular levels of privacy is preferred with control i.e., allowing and restricting particular phone functionalities [31]. As HCI researchers and designers, we need to be cognizant of such needs as these require highly personalize-able features. Attempts have been made to design interventions such as "PhoneLock" to avoid shoulder surfing by limiting input to solely auditory and tactile stimuli [15], however, these are not widely used. Focus groups, experiments and surveys in Berlin showed that women perceive systems or methods to be more secure than men [67] and a study of Australian users showed that females exhibit significantly less privacy-preserving behaviours than males [46]. These gender differences in privacy perception and behaviors reveal the need to explore the reasons behind these.

### 2.2 Privacy in the Global South

The learnings from prior research on disclosure and privacy practices in Western contexts [4, 14, 20, 22, 38, 43, 65, 69-71] can not be used to design for users in South Asia as this region represents a different context with high gender inequality [63], unique regional cultural norms and expectations [62] and emerging technology adoption [21, 47]. Privacy researchers emphasize the importance of community norms in boundary regulation [42], and that expectations for privacy are tied to the norms and data flows of a

given context [54]. This need for a contextualized understanding of privacy highlights the importance of exploring a diverse range of contexts, norms and value systems that underpin the privacy practices outside of the Global North. Although, an understanding of the norms is essential to designing for privacy, McDonald and Forte highlight the limitations of relying only on norms as an analytic tool [45]. Focusing on the norms ignores the unique privacy concerns of vulnerable populations who do not *determine the norms* but are often forced to visibly perform them in online spaces. This is particularly true in contexts with significant power differentials. Pakistan is one such context where patriarchal norms and expectations create specific vulnerabilities for both men and women. Our work explores these vulnerabilities and builds on earlier work in the Global South to expand our understanding of how privacy is performed in diverse contexts.

There is a growing body of knowledge studying the perceptions of digital privacy in the Global South. For example, a study on privacy challenges in the Global South highlights cultural differences, knowledge gaps and unintended use as key factors in determining privacy behaviours [66]. Similarly, prior work has also revealed low-literate users are unable to respond appropriately to security and privacy threats using available phone affordances [24]. Designers have also sought to leverage some cultural differences in how technology is used in a shared way to create interfaces that support collaborative learning by receiving remote help from higher literacy members of their community [8].

Studies in Muslim dominant countries, such as Saudi Arabia and Qatar highlight the role of Islam in shaping the privacy beliefs of citizens [2, 7]. These studies highlight privacy as a key value in the Islamic societies in the Gulf region, with women afforded both higher degrees of privacy in the home and society, as well as being responsible for the family honor. Abokhodair et al. draw upon a dataset of 18K Twitter posts of Qatar users and study the prominent keywords used to describe privacy, finding that men use paternalistic language in discussing women's privacy [1]. Another study also based in the Gulf region drawing on qualitative interviews with users in Saudi Arabia and Qatar, highlight the role of cultural and religious beliefs in boundary regulation leading to the creation of multiple accounts on social media for different audiences (for example, women preferring to only share certain photos with female friends) [2]. Their work recommends culturally sensitive design practices, in particular highlighting the need for flexibility of maintaining multiple accounts for multiple audiences as well as gender-sensitive friend recommendation systems. In contrast, our work is based in a patriarchal Islamic context where privacy is not understood as an individual right, and where the majority of users are low-literate and do not have the technical ability to enact advanced privacy practices like using and managing multiple accounts.

Several studies have also explored the privacy management challenges arising in developing countries, particularly for the lower-literate users [58, 68]. Reichel et al. study privacy management practices of low income mobile social media users in South Africa, finding blocking as a primary method of managing privacy as opposed to finer granularity privacy controls as well as self-censorship on social media based on the local crime rate [58]. Similarly, Wyche examining the experiences of Kenyan women in using mobile phones

highlight challenges in navigating privacy settings, online harassment from strangers, and dependency on younger family members and friends for resolving account related issues [72]. A recent study from Pakistan also reveals that women learn and are introduced to new technology in two ways: either through their male relatives or other women in their network who previously learnt about these technologies [34].

Privacy studies aimed at understanding user needs in Bangladesh reveal the privacy challenges arising due to shared mobile phone use [6], privacy risks associated while handing over devices to repair shops [5] and the awareness amongst Bangladeshi users of information leakage through different apps [9]. To address the privacy challenges arising from shared mobile use, one study proposes a "tiered" privacy model for authentication, where the user can log into a secret or a shared account depending on the context [7]. Similar work in India explores the role of patriarchy in shaping the privacy experiences of women in India, regulating social media use of daughters [39]. Karusala's work also highlights the willingness of young women in India to explore and go beyond cultural norms, motivating them to take charge of their privacy literacy. A particularly relevant and important study exploring gendered privacy practices amongst women in India, Bangladesh and Pakistan reveals the importance placed on sharing mobile phones with family members and that digital activities be open to scrutiny [62]. The study also describes the use of private modes, content deletion and applocks as some of the practices employed to preserve privacy on shared phones. Other work in South Asia has also revealed the significance of the sharing of passwords with family members which is considered as a sign of trust [10] and transparency [6]. In patriarchal contexts, damage to family honor and defamation are a significant concern [60] and the consequences of privacy violations, and online behaviours that are non-normative can be extreme. In 2016 Qandeel Baloch, a Pakistani social media celebrity whose real identity and name was leaked online, was murdered by her brother as a consequence of posting risqué content online [28].

Our work builds upon this understanding of how privacy is performed in the Global South and expands it to include an understanding of the vulnerabilities of both male and female users, the role of Islamic values in determining privacy practices, and the impact patriarchal norms have on not just determining female users privacy practices but also male users.

### 3 METHODOLOGY

This study explores the privacy perceptions, behaviours and understanding of digital privacy amongst low-literate populations in Pakistan. We interviewed 40 participants, of which 17 were men and 23 were women.

#### 3.1 Study Context

Cultural values and religious beliefs play a vital role in user's privacy perceptions and behaviours. Pakistan is a patriarchal context where Islam is the predominant religion [30]. It also ranks 153rd out of 156 countries on the gender parity index [26]. Pakistan also ranked seventh among eight countries in South Asia, only better than Afghanistan. Additionally, the literacy rate in Pakistan is approx. 59%, which has a significant impact on the ability to use

digital technologies. A recent survey by the World Bank exploring mobile Internet adoption in the Global South revealed a lack of digital literacy to be one of the most significant reasons for a lack of adoption of mobile Internet services and technologies. This is a gap in access but also digital literacy and understanding of technologies is further exacerbated for women in the Pakistani context [12].

A GSMA report on mobile gender gap reveals 29% of female mobile phone users see a lack of family approval to be the top barrier to their adoption of mobile Internet services as compared to only 2% men [59]. The report also reveals that reading and writing difficulties are also a significant barrier to mobile ownership among Pakistani women [59]. Women also have restricted access to public spaces and especially spaces traditionally considered 'male', in particular technology related marketplaces and spaces [11]. Studies reveal 90% male smartphone users purchased their own device, while only 42% women purchased their own smartphones [59].

The patriarchal and restrictive nature of Pakistani society directly impacts women and men's privacy perceptions, risks, concerns and privacy-preserving behaviours. Our work explores these perceptions and the impact underlying beliefs have on gendered privacy behaviours and practices.

### 3.2 Study Design

The study was conducted in Lahore, Pakistan from January 2021 to July 2021. We conducted one on one semi-structured interviews in Urdu with low literate participants. The semi-structured interviews explored the privacy perceptions, privacy-preserving mechanisms, the application specific privacy practices and the motivations for implementation of such practices. Moreover, each session also focused on the participant's mental models regarding privacy features, the sources of learning about these features and their perspective on how privacy should co-exist across gender, social and cultural norms. The interview protocol also probed about the granularity of what should be considered 'private' and what should be open for sharing.

All interviews, except one, were conducted in person. One interview was conducted over zoom due to the Covid-19 lockdown. In person interviews were arranged at safe spaces where participant's family members were not present. Participants were interviewed individually in a separate room to help them be more comfortable in sharing their privacy practices. Same gendered and same ethnicity facilitators helped build trust with the participants, which encouraged them to share intimate details. At the start of the interview participants were familiarized with the purpose of the research and briefed about the concept of privacy in case they didn't readily understand the term. Interviews were conducted in local languages i.e Punjabi and Urdu. Some application specific English terms such as "delete for everyone", "incognito mode", "status" etc were used as it is, however, their meaning was explained to the participants to ensure that they were not confused. We collected participant demographics in the first phase of the interview, to find common ground with the participant. The interview protocol comprised of sections about phone usage, password sharing, WhatsApp, Facebook, Instagram and YouTube. At certain points where participants struggled to explain a feature, the facilitator would hand them their phone so they may demonstrate it. Belief and practices related

Gender	Male	17
	Female	23
Age (years old)	below 18	2
	18-28	25
	29-38	8
	39-48	3
	48+	2
Education	Below Matriculation	15
	Matriculation and above	25
Marital status	Married	22
	Unmarried	18
Occupation	Works	25
	Housewife	8
	Studies	4
	None	3
Phone type	Smartphone	40
	Feature phone	0
App usage	WhatsApp	40
	Facebook	28
	YouTube	29
	Instagram	9
Shared phone	Male	12
	Female	21

**Table 1: Demographics of 40 participants interviewed for the study.**

questions were semi structured and focused on specific experiences of the participant. The questions encouraged them to share their sentiments and reactions to Western models of privacy.

### 3.3 Participant Recruitment

Participants were recruited using snowball sampling through personal contacts. Participants belonged to low-income areas of Lahore. Sessions were held every week until saturation was reached in the data i.e. no new insights or behaviours were revealed. We interviewed both both male and female participants to maintain gender balance and understand how each impacted the privacy practices of the other. There were 17 males and 23 females aged between 18 and 60 (Table. 1). The majority of our participants had less than 12 years of schooling with a small number who had completed 12 years of education. There was a mix of married and unmarried participants, the majority of them living in joint family systems. Participants belonged to different unskilled and semi-skilled professions, with females being housewives, students, factory workers, beauticians and tailors, while males being barbers, sweepers, drivers and gardeners (Table. 1). As per the government of Punjab, the minimum wage for unskilled adult and adolescent workers in Punjab is PKR 96.15 (0.6 USD) per hour whereas for semi-skilled and skilled labour the minimum wage ranges from PKR 99.65 (USD 0.62) to PKR 115.72 (0.72 USD) per hour [55]. All participants were compensated for their time with PKR 500 (approx. 3.12 USD) and interviews took approx 45 to 60 minutes, All participants owned a smartphone. However, some possessed a personal phone whereas others had shared phones with spouse or the whole family.

### 3.4 Ethical Considerations

Participants were informed about the intention of the study, the name of the institution the researchers belonged to and ensured the anonymity of their data. In the beginning of each interview, verbal consent was taken to record the interview and participants were informed about the option to opt out of the interview at any point without any impact on the compensation. Participants' anonymity was protected and interviews were conducted in safe spaces (researchers home or local school) to ensure they did not feel uncomfortable discussing their privacy practices in the presence of family members. This study was conducted during the Covid-19 pandemic but after lock-downs had eased, at a time when nationwide cases were low and small gatherings were allowed. All facilitators were partially or fully vaccinated and wore masks during the interviews. Participants were provided masks and seated at a safe distance from the researcher. The interviews took place in well ventilated spaces and all supporting material and surfaces were disinfected pre and post interview. All participants except for 2 were over 18 years old. Parental consent was obtained for participants under 18. Additionally, the interview was conducted in the presence of their parent. Although the participants were not able to share intimate details in the presence of their parent, the parent's frequent interruption as their child spoke provided us with interesting insights about the dynamics of phone usage. The parent's comments regarding the restrictions they had set on their child's phone usage provided us with data about controlled phone usage. For most interviews we ensured that the gender of the facilitator and the participant was the same, as social and cultural norms do not allow sharing of private and intimate information with the opposite gender. The names, addresses and all identifying information of the participants was removed from the data when shared with the extended research team.

### 3.5 Data Analysis

All interviews were first transcribed from audio recordings. The transcripts were then coded using open coding by two researchers. The codes were then combined and themes identified using thematic analysis [17]. The main themes that emerged were (1) commonly used phone features, (2) shared phone usage, (3) common privacy practices, (4) religious and cultural factors impacting privacy practices, (5) beliefs regarding ideal social media usage and (6) sources of learning privacy features. Two researchers worked together on data analysis that led to the generation of over 200 codes and sub-codes through open coding. Repetitive codes were merged into one code. The quantitative figures represented throughout the paper were derived from manually counting the occurrences in all interview transcripts. We also used affinity mapping to analyse particular privacy behaviours of both genders. We combined answers to questions about privacy settings and situations separately for male and female participants. Codes were grouped together in similar categories to create themes.

### 3.6 Positionality

All authors of this paper are researchers living and working in Pakistan. To adopt and practice intersectionality it is important to recognize our own positionality. Three of the authors are women

and one author is a male. None of the authors belong to low-income groups. All authors grew up as Muslims in Pakistan, practice the religion to varying degrees and understand intuitively the religious terminology used by our participants. Our own understanding of Islam and how it is practiced in Pakistan has informed this work. As women raised in Pakistan but who has spent significant time in the West, our understandings and experiences of the existing patriarchal structures have also informed this work. Due to the religious reservations and cultural norms of the population being interviewed, male facilitator interviewed male participants and female facilitator interviewed female participants.

## 4 FINDINGS

Our findings reveal privacy perceptions and practices amongst low-literate, low-income Pakistani users. We reveal significant difference in how female participants understood and performed privacy versus male participants. We also found religion to play an important role in determining users privacy perceptions and behaviours. Pakistan is a predominantly Muslim country and participants relied heavily on their interpretations of Islamic beliefs to conceptualize and enact digital privacy. As also revealed by earlier work [62] cultural expectations of a patriarchal context also played a significant role in determining privacy beliefs. We organize our findings along these three main themes that we found to have the greatest impact on user's privacy perceptions and behaviours; religious norms, patriarchal norms and access to sources privacy knowledge.

### 4.1 Religion and Privacy

Islamic values and beliefs form the foundations on which much of what our male and female participants considered private. 'Purdah' and 'Haya' were the two predominant beliefs influencing men's and women's understandings of the private. Purdah is understood as a covering [56] and in Muslim communities it is predominantly linked with women's bodies and protecting them from immodest eyes and men's gaze [64]. Although the term refers to a physical covering, it also implies a covering in terms of the language used and often in terms of women's presence in physical and digital spaces. Segregation of genders is one performative form which Purdah takes in public and private spaces in many Muslim countries. Our work reveals this segregation to also be enacted in the digital space as a form of 'Digital Purdah', keeping digital spaces 'private' and secluded from men. One way participants enact (discussed in detail below) Digital Purdah on social media sites is by posting in spaces where they can segregate the audience. Participants reported making viewer lists for who can see their statuses on WhatsApp (11.7% male and 21.7% female participants), monitoring viewership of their stories (17.6% male and 21.7% female participants) and adding only specific contacts and changing display picture settings (29.4% male and 65.2% female participants). The ability to enact Digital Purdah also determines which applications are predominantly used by men and women.

Similarly, 'haya', which loosely relates to honor, is understood as a natural or inherent shyness, and a sense of modesty [16]. In Islamic terminology, it is mainly used in the context of modesty [18]. Haya encourages Muslims to avoid anything considered distasteful or abominable and plays an essential role in Islam, as it is one of the

most important parts of faith [16]. Both these concepts of Haya and Purdah largely determine the privacy behaviours and perceptions of Muslim users:

"From Islamic point of view we should cover ourselves. Our culture is different from the foreign culture." -FP7

In performing 'Haya' or modesty in the digital space FP7 further explains:

"Sometimes I upload my picture wearing jeans with no scarf so they (male relatives) say that I'm very modern. So I hide those from them (male relatives). Only my friends and people from my family can see my status."

There are significant differences in who enacts Purdah in the digital space. For example, 52.2% of our female participants reported not uploading pictures of themselves as their WhatsApp display picture and instead used pictures of their father, brother, husband and children as their display picture. In contrast only one male participant did not use his own picture as the WhatsApp display picture. Some of our participants navigated digital modesty by uploading parts of their face as opposed to the whole; i.e. cropping the face out of picture, and uploading pictures of hands, eyes, lips, etc. This allowed them to keep their images private but also feel ownership of their display pictures.

Much of the literature on privacy based in the Global South is gendered in nature and focuses exclusively on the female perspective [34, 39, 61, 62], in contrast, we explicitly sought to understand the male perspective on women's digital presence and privacy. Without a complete, holistic understanding of women's privacy practices which are determined by the cultural context and established norms, any design aimed at inclusion and safety would fall short.

We find these norms to be heavily influenced by religious beliefs and are reflected in subsequent privacy practices and strategies that female users adopt to 'hide' their presence. In particular, male participants link women's presence in digital spaces with sinning and corruption of communities:

"Women create immodest videos on Tiktok and in this way it makes us all guilty of doing a sin." -MP4

Out of the 47% male participants who commented on female representation on social media, 75% believed that women's access to social media should be restricted based on their religious beliefs. Participant M10 discusses the types of content that he thinks women should be 'allowed' to post and believes women's online behaviour should be in line with Islamic understanding of modesty:

"They (women) should be allowed to post good pictures only. They must not post inappropriate or immodest pictures because others can also view those pictures." -M10

The two major concerns shared by male participants were women uploading pictures that they did not consider religiously or socially acceptable and other men viewing these pictures online. These concerns directly result in men establishing boundaries or norms of technology usages in their own families and feed into the perceptions of the ways in which it is acceptable for women to exist in

these digital spaces. MP11, who was a 20 years old married labourer further explains:

"Everyone has their own opinion but I think women shouldn't excel this much. As in she should stay in Purdah, not on Facebook. Women at my home don't know about Facebook. They use simple button phones."

In addition to Purdah being a religious obligation, men also influence women in their families to observe Purdah and practice segregation. MP12 discusses his thoughts about strangers (men) messaging women:

"Yes, they (women) should also use WhatsApp but the problem begins when they start talking to strangers or when a stranger (man) starts sending messages to them."

In contrast, our data reveals no female perspective on what men should do online. When faced with unwanted messages, they, instead of deleting the person messaging, delete their own account. One participant explained:

"Your izzat (respect/honour) is in your own hands."

Female participants believed "*men will do this, they always do this*. and take up defensive roles where they are protecting themselves from men. A consistent theme in what women choose to keep private (as illustrated by the comments of female participants) is linked with not just what they themselves consider private but what their families decide is private *for them*. And this distinction is made on the basis of family honour and respect, which in Pakistan is almost exclusively linked with a woman's body.

## 4.2 Patriarchal Norms: Gendered Differences

Both male and female participants employed different measures to preserve their phone privacy as well as privacy over different applications (Table 2). 78.2 % female and 100% male participants used pin/password lock on their phones. However, we observed a significant disparity in the number of men and women who used the fingerprint lock. Only 13% of female participants used fingerprint lock, whereas 58.8 % of the male participants used fingerprint lock.

All the participants were smartphone users and had access to the Internet through Wifi or mobile data. Although all participants claimed to have a personal phone, upon further discussion we learnt only 8.7% female participants versus 30% of the male participants did **not** share their phones and passwords with others. The rest of the participants had open access to their physical phones, i.e., their phones were being used by family members and their passwords were known to them.

We observed a correlation between the literacy level of the participants and their ability to understand various app functions. We observed that the participants who had received education below Matriculation (approx. grade 10) (17.4% female and 64.7% male participants) did not report much self-exploration of features in their phones and apps and did not know details about certain features such as the difference between 'delete for me' and 'delete for everyone' (in WhatsApp) as compared to the participants who had completed Matriculation. Similarly, we also found that although on average female participants had a higher education level than male participants, 60.1% female participants reported that their phone

Privacy Practices	Male Participants	Female Participants
Phone and password sharing	70%	91.3%
Parental surveillance	29.4%	78.2%
Family influence	0%	69.6%
Access to knowledge because of social circles	100%	0%
Applocks	60%	8.7%
Modded apps	35.3%	17.4%

**Table 2: A comparison of the adoption of certain privacy practices between male and female participants.**

and app privacy settings had been set up by male members of the family such as sons, brothers, fathers and husbands. While this practice amongst women has also been reported by earlier work [34], we additionally reveal that because male participants have greater access to public spaces, they are able to leverage mobile shop owners to set up their phones (discussed further in Section 4.4) and as a consequence had more information about digital devices than female participants. Female participants also reported a lack of involvement in the process of setting up the privacy settings on their phones and applications – male family members did not discuss or ask for their preferences. Only one of our female participants was asked by her son about her preferences regarding privacy whereas others were handed over the phone after setting up the privacy settings however the men wished. Conversations with female participants hinted that they were satisfied with this mechanism as they repeatedly mentioned in various ways that

"Husband/son/brother (in different cases) knows it all, he set it all up well."

For each of the most commonly used applications amongst our participants we explored specific privacy practices and features that helped them secure their digital identities and data. We discuss these below based on the platform, the purpose of use for each application and the intended audience.

**4.2.1 Phone Sharing.** As noted in earlier research exploring women’s privacy practices in South Asia, there is a cultural expectation on women to share their phones with family, relatives and often friends [62]. Our findings also reveal similar expectations on women to share their phones and passwords. Additionally, our work also reveals the absence of any such expectations felt by male users. Our data reveals that 70.9 % male participants and 91.3 % female participants had shared phones. As MP12 discusses, he is not bound by expectations, rather he willingly allows if someone wishes to use his phone

"No, I’m the only one who uses it (phone) but if someone needs to use my phone I allow them."

Participants revealed the sharing of phone and passwords as a form of courtesy so as not to offend other people. This form of courtesy and expectation was exclusively felt by all female participants except two, but none of the male participants. FP23, an 18 years old newly married female participant, who lived in a joint family with her cousins and her brother-in-laws, said that she did not need a password:

"I’ve thought about it but I have never used this feature. Others also use my phone and it’s inappropriate

to secure it with a password. In this way, others will think that I’ve secured my phone from them."

She felt that because her family ‘took care of her’ and her cousins, it would be inappropriate to secure her phone from them.

In contrast, male participants had different reasons for password and phone sharing such as: 1) friends and family members needing to make frequent calls 2) as a symbol of trust with close friends, and 3) spouse needing to use their phone as they did not have a separate one.

Participants further revealed the reason for having a password at all was to protect the phone from outsiders at work and not from people in the household. Female participants also employed multiple techniques in order to not be forced into sharing phones out of courtesy with outsiders. FP17 explained that her father had recommended she hide her phones whenever guests came over so they could not ask her to see her phone and view the content in it.

This expectation of sharing devices and passwords is also enforced by mothers with respect to their daughters as illustrated by FP11 a 20 year old student:

"My mother has strictly told me to share my password with her. If I change my password or put a lock on my apps my mother says that I must have been hiding something from her." -FP11

Our code book reveals that while there were 18 incidents where parents influenced the privacy practices of their daughters, there were only 5 such incidents for sons reported directly by interviewee or indirectly by their parents. FP6’s (aged 19) mother accompanied her to the interview and revealed her daughter was only allowed a phone because it had been a gift from her fiancé. The mother also described in detail how she regulated her daughter’s phone usage, such as allowing her to have a limited contacts list only and listening to any calls she made on the phone by sitting with her during the conversation. In contrast the mother did not check her son’s phone because she thought boys sensible enough to use phones in a "proper manner". Another female participant, FP10, aged 20 who lived with her mother said that her mother monitored who her friends were and with whom she shared her number:

"Because my mother told me to only give my number to my special friends, and my contacts have 19 numbers."

This surveillance is not only performed by parents but brothers and husbands also monitor women’s devices. However, some of our female participants have found ways to navigate this surveillance as participant FP10 reported hiding her online status using GB WhatsApp (a modded version of WhatsApp which has extra

features, discussed in Section 4.3) because her brother would scold her if he saw her online at night:

"You know I talk to my friends in groups, they stay online at night and then my mother and my brother keep an eye on me. If my brother gets to know that I am online then he comes to my room and scolds me so I hide online status on GB WhatsApp."

Similarly, participant FP7, an unmarried woman, aged 19, discussed being suspected by her brother if she used her phone after 12 midnight. Her brother raised concerns regarding who was she talking to. On many occasions, such restrictive measures of surveillance and control lead to women coming up with novel and unconventional practices to keep their content and conversations private.

However, regardless of cultural expectations and the perception of sharing all our participants had created mechanisms for maintaining privacy whether on shared or monitored phones. Given the difference in cultural expectations between genders, these mechanisms greatly differed.

**4.2.2 Privacy as Scandal for Women.** A common theme across the interviews with female participants was the association of privacy and the desire for privacy with 'scandalous' and inappropriate content. This again is grounded in the Islamic belief in 'modesty' and *purdah*. However, in contrast to our female users this was not a common theme amongst male participants. Male participants did not report sharing passwords because they had nothing to hide, instead, they had reasons where their friends or family needed to use their phones for making calls etc.

Our female participants were particularly concerned with the negative connotation of *privacy* - i.e. if you have not done anything 'wrong', you do not need privacy:

"I think when you have done something mysterious or wrong only then you will feel the need to hide it from your family members. My kids are very good and my husband and I have nothing to keep from one another. We have everything in the open." - FP8

This is highlighted by FP1, a 24 years old female participant with a 2 year old child, who felt that as long as she is not doing anything 'wrong' she does not need a phone lock. She notes that her phone has nothing private and is left unlocked on a table when she is busy with household chores:

"I do not need phone lock and I never will."

She further explained that a phone lock would be synonymous with hiding things from her husband and it is important for her to ensure he has ready access to her phone.

In exploring women's privacy practices we find them to be leveraging specific mechanisms to ensure privacy on digital devices without obviously appearing to be enacting privacy. In contrast, most of our male participants privacy practices are more open, obvious and deliberate. Below we discuss the ways men and women practice privacy with respect to the cultural and religious constraints.

**4.2.3 Applocks Predominantly used by Men.** Another important privacy-preserving mechanism employed by a few female participants (8.7%) and most of our male participants (60%) was the use of applocks. Applocks enable users to password protect specific

applications, images and folders. Applocks are used as an additional measure on top of the standard phone lock because phones are often shared with friends and family. Although all the male participants who were using applocks (on top of phone locks) also claimed their phone was their personal device, still they were concerned about their content being viewed by someone when they give their phone to make a call or view content.

Participants reported using applocks to hide social media applications like WhatsApp, Tiktok and Facebook. The participants who used applocks wanted to keep their conversation private from family members. MP1, a 21 years old male participant who had a good understanding of phones, noted that because his father and younger brother often used his phone, he used an applock on WhatsApp to prevent his father and brother from viewing his conversations with his female friends. MP3, another male participant, speculated that most men would hide conversations with their girlfriend in the applock. He also elaborated his own use of applock,

"I have applock on my gallery so when my friends take my phone they can be mischievous and they can do anything and I have family pics in the gallery."

For MP3, his friends are the outsiders, and he wants to prevent them from accessing his gallery even when they are given the phone. Applocks were also used to hide family pictures, pictures of partners and wedding photos. The few female participants who used applocks learnt of them from other family members and often indirectly hinting at using them to hide their personal photos.

In contrast, all the male participants learnt of applocks and other phone features from male friends in their social circle. Built-in gallery locks have become increasingly common on Android phones and participants (4.3 % females and 11.7% male participants) were also seen using them. 58.8% male participants and 13% female participants also reported using fingerprints as phone locks as well and some (26.6 % males) used WhatsApp's built-in fingerprint lock, which only lets registered users access WhatsApp through a fingerprint. Gallery locks and WhatsApp fingerprint identification both don't require any additional app to be installed, which is an easier way for our target population as all of them were low-literate. This does not require them to navigate the Play store to download an app or depend on someone else to download it for them.

Applocks have existed on app stores for a significant amount of time with almost all of them providing a similar user experience, but most applocks have recognize-able icons often showing some type of lock and a discrete password screen pops up while accessing applications. This leads to others questioning if they are hiding something suspicious or scandalous. 21.7% of female participants had heard about applocks but only 8.69% were actively using them, most of them were open (with the researchers) about what they were hiding i.e photos of themselves or family members. While the use of conventional applocks (with lock screens and recognizable icons) has previously been documented in South Asian population [62], in addition to the conventional applocks, 17.65% male participants were also using hidden/disguised applocks to remove the element of suspicion that comes along with conventional applocks. Such applocks are disguised as other phone utility applications until the user selects certain options. In our sample group, two types of hidden applocks were mainly found: 1) calculator and



2) clock lock. MP1, a participant who already uses a phone lock and a standard applock, summarizes the functionality of calculator applock,

"So the first time I saw this was on someone else's phone, when you open it has gallery, numbers, pictures and person will only be able to see calculator until you enter pin. Let me show you. You have option to save apps, numbers, video, gallery, pictures etc. Any outside person can use calculator, until you enter pin."

The Calculator applock is an app that looks similar to the built-in calculator app and performed the regular operations of a calculator, until the participant entered their PIN and pressed '=', that would lead to opening of the applock interface. Similarly, to the untrained eye, the Clock lock application seemed like a regular alarm clock app until you open and configure it to a certain time, which unlocks the applock interface. These hidden applocks add a hidden layer to the multi-layered privacy model used by the participants when sharing phones. This means users are restricting the amount of control they want to give up at different stages (phonelock, applocks, gallery locks) but are also adding an incognito layer, whose control can't be requested because no outsider knows about its existence. This granularity of control was only demonstrated by male participants, they defined boundaries of access differently for strangers, friends, close friends, family and finally a boundary which only they knew of.

Male participants learnt about hidden applocks from their friends or informal work gatherings (for example, a group of chauffeurs waiting outside a venue). The secrecy aspect of hidden applocks was further reinforced by the reluctance of the participants to share information about the app's existence with the researchers. One male participant was very hesitant to tell us the name of a 'secret' application he got to know from a friend, when asked to describe some of the features of the app, they matched the description of some of the hidden applocks we had seen earlier.

### 4.3 Patriarchal Norms: Controlling Other Users Privacy

Many participants used after market applications to supplement their privacy needs. WhatsApp is one of the applications which was used by all our participants on a regular basis. Although WhatsApp provides many built-in privacy features, 17.4% female and 35.3% male participants reported the use of after market/modded versions of WhatsApp known as GB WhatsApp and FM WhatsApp. These applications provide additional features over standard WhatsApp, some of these include: 1) the ability to customize user interface with themes, 2) viewing status (24 hours story) without notifying the other person, 3) reading messages without them being marked as read (for specific participants), 4) being able to view deleted stories and messages, and 5) being able to freeze your last seen online time stamp. The contacts of a person using a modded version of WhatsApp are unaware of its use - on their end the application looks and functions exactly like the official application. These modded applications are unavailable on the Android Play store and participants installed GB and FM WhatsApp through APK (Android

Package Files), a process which requires the sharing of the installation file (apk file) with the user. Other ways to get GB and FM WhatsApp include directly downloading them from the website. Female participants who used GB WhatsApp did so to hide their online presence after hours, and their presence online:

"GB WhatsApp allows you to hide your activity status. You can hide if you want to stay online at night. You can also hide if you have read the other person's message or not. The sender will never get to know if you are online or not...I activate these features sometimes at night...you know I talk to my friends in groups, they stay online at night and then my mother and my brother keep an eye on me. If my brother gets to know that I am online then he comes to my room and scolds me."- FP11

Participants who used these modded versions of WhatsApp believed these ensured extra privacy with more control. However it is arguable if it improved their privacy or compromised the privacy of others by being able to view their deleted messages and stories. GB and FM WhatsApp features that grant them preference over the standard WhatsApp, are features that allow users to maintain a stealthy approach while interacting with their contacts, whether it be viewing their message secretly or to appear offline to them. MP3, who frequently uploads videos and pictures on GB WhatsApp status, explains,

"There is a sort of privacy where even when you see their story (referring to WhatsApp status) they don't get to know about it (referring to GB and FM WhatsApp). Similarly status can be hidden from specific people as well."

He perceives the ability to view his contact's story, without them knowing, as a form of privacy. Moreover, his use for GB WhatsApp has been focused around the ability to secretly view the content of others and control who can view his content, although standard WhatsApp allows some control over content as well (discussed in Section 4.5). Most participants learnt about GB and FM WhatsApp from their friends or work circles.

### 4.4 Sources of Privacy Knowledge

One significant difference in smartphone privacy practices between male and female participants is the sources of knowledge about privacy features. Women in Pakistan are excluded from the public spaces in general and in particular from tech marketplaces (mobile purchase and repair shops). As a result they are almost never part of the initial on boarding while buying the mobile phone and thus miss out on the opportunity of setting up the phone as well as informal tech conversations at the mobile shop. Women who are housewives or do not do work/study that requires them to go outside their house, have even more limited circles often restricted to their immediate families and relatives. Amongst our female participants who were housewives or had no occupation (43.5%), none of them reported going out often to meet their friends or interacting with a larger social circle. FP24's, a newly married girl, discusses her routine and social interaction:

"I do not have any friends. I am so busy with household chores the whole day that when I get free I spend that time with my in laws."

In such limited social circles, the only sources of information about privacy features and mechanism that women have are the men who are related to them (husband, father, brother, son) or other women in the family. Such limited social circles lead to limited tech knowledge.

The literacy level of our female participants was more than male participants overall; 82.6% of our female participants had done Matriculation or above while only 35.3% of our male population had received education to the Matriculation level or above. It was surprising that despite this significant gap in literacy level, 58.8% of female participants reported learning phone use from a male family member and 60.1% female participants reported that their phone and app settings were set up by male members. MP4's comments regarding learning about phone features despite not being educated further highlight the reason behind men being more aware of features

"I'm not well educated. But now I understand everything if someone tries to make me learn."

Moreover, upon inquiring further, we discovered that none of our female participants except one were asked about their preferences when men set up their privacy settings. Upon asking if her husband asked her for her preferences when setting up the phone, FP9 reported

"No. He did it all by himself. He taught me as well how to use WhatsApp, YouTube etc."

On the other hand, our female participants were not aware of their husband's phone and privacy settings as FP15 reported

"When I had a Facebook account my posts were visible to friends only. I am not sure about my husband's privacy settings."

As compared to female participants, our male participants reported having significantly larger social circles. The culture of Pakistan makes it easier for men to sit at shops over tea, lunch or meet in public for discussions. Some of the common informal social circles reported by our male participants were 1) drivers waiting outside a school or office for their passengers, 2) groups of people in a workplace, 3) friend gatherings in public spaces, and 4) shopkeepers with regular customers. This leads to an exchange of knowledge where men educate each other about different phone features and applications such as hidden applocks and modded applications such as GB WhatsApp. As MP3 reported

"So the first time I saw this was on someone else's phone (in a social gathering)."

100% of male participants reported having learnt about a new feature from their friends or people in their informal social circles. Men also have access to their male employers who are often more informal with their male employees than female employees:

"I used to work at a madam's house and I used to take help from her sons." -M15

Even though 26.1 % of our female participants had jobs where they had an employer (others worked as a tailor etc. so they did not have an employer), none of them reported taking help from

their employer or anyone related to the employer. Most of these participants worked as domestic workers in homes and one possible reason for not getting technical assistance from employer could be the restrictions female participants face on phone usage during work (either submit it at work before beginning work or not being allowed to use it or bring it to work), whereas, none of our male participants reported such restrictions (not domestic workers).

Furthermore, men in Pakistan have more access to shops and repair centres where they can visit people who specialize in mobile phones and other digital devices as opposed to women as these spaces are dominated by men. MP14's comments show the easy access of facilitators at men's disposal

"Initially when I bought my phone I had no idea how to create an account on Facebook. I paid shopkeeper for creating my account. Later my friends taught me how to create an account on Facebook."

#### 4.5 Navigating Religious and Patriarchal Norms

All our participants were active WhatsApp users where WhatsApp was being used for a variety of purposes including talking to people at work, connecting with family as well as friends. In our context, WhatsApp is particularly ubiquitous because it allows non-textual ways to communicate through voice messages. Additionally, Facebook was amongst the most widely used applications by our participants after WhatsApp. 65.2% female and 76.5% male participants reported using Facebook.

Our interviews explored the specific WhatsApp and Facebook privacy features that were used most frequently and the differences in how men and women employed these features.

**4.5.1 Delete Feature in WhatsApp.** 58.8% of male and 73.9% female participants reported knowing the difference between 'delete for me' (removes messages on the sender's end) and 'delete for everyone' (which removes the message from both the sender's and receiver's end) on WhatsApp. Both the options are presented when a user clicks on the delete button, but the delete for everyone option disappears after an hour of sending the message. Even the female participants who were not aware of the difference between the two options (21.7%), used the feature to enhance their privacy on shared phones by deleting messages after sending them so no one could access them. We asked participants to explain which option they chose and when (delete for me or delete for all), and in some cases participants were unable to explain the difference between the two options. The research team then showed both options on their (researcher's) phone and asked which one they chose. All female participants who used this measure chose the "delete for everyone" option so "there is nothing left", they reported. 52.2% of the female participants reported deleting conversations on WhatsApp on shared phones that they wished to keep confidential. However, this practice was only found in female participants who had shared phones but not amongst users who did not share their passwords with others, or amongst male users. Examples of confidential information included discussions with other women regarding intimate health issues as well as discussions participants did not want family

members to see. FP18 described deleting messages so her brothers, who also used her phone, did not see her chats:

"Yes, I delete them[chats] because we share personal stuff sometimes."

Female participants with shared phones initially insisted they did not have anything to hide in their WhatsApp chats and did not use the delete function. However, upon further probing, many disclosed that they delete the WhatsApp chats that they wish to keep private from other individuals sharing their phone. One participant mentioned deleting conversations with her friends on WhatsApp because she shared the phone with her mother. FP23, whose phone was shared with her younger brother-in-laws (who mainly used it for gaming), discusses the mechanisms she used to ensure privacy on her chats:

"I am 4 months pregnant and whenever I experience pains or discomfort I talk to my elder sister about it. Later I delete those conversations because my younger brother-in-laws use my phone for gaming and it does not look nice if they come across this conversation in case they open WhatsApp."

The participant felt that her conversation about pregnancy related issues should not be accessible to other users of her phone. She does not employ the use of a password on her phone to restrict access to her family members to prevent unease or suspicion. For her, the privacy-preserving mechanism is to delete the conversation to make the content inaccessible, even if it meant that she would be unable to access it later.

However female participants raised a concern regarding the delete feature on WhatsApp. When a user selects the *delete for me* option on WhatsApp, the message is removed from the sender's end without any traces or residue messages. However, when using *delete for everyone*, the message body is replaced with a text saying 'this message was deleted' on both the sender's and receiver's end. Our female participants reveal this to be a potential hazard for them, raising suspicions as to what needed to be deleted/ kept hidden. 13% of the female participants reported not deleting messages for everyone as they did not want to be a source of stress for the receiver or a cause of conflict. This was not felt by any of our male participants except one who said that it was "embarrassing" to delete a message like that. Similarly, one participant, FP8 a GB WhatsApp user (a modified version of WhatsApp discussed in Section 4.3) noted that being able to see deleted messages sent by someone else, a salient feature of this modded version of WhatsApp, can cause fights so she prefers using the official version of WhatsApp.

Our data analysis reveals that while female participants made extensive use of the delete feature, none of the males resorted to this feature in order to preserve their privacy. The only usage of delete feature by males was when male participant sent something by mistake to someone and they wanted to delete it. As noted in Section 4.2.3, male participants predominantly used applocks and gallery locks to ensure multilevel privacy where other user(s) had access to their phone.

**4.5.2 Owning Facebook Accounts.** Female participants were also fearful of owning private Facebook accounts. 17% female participants who used Facebook had a shared account with male members

of their family. Whereas, all male participants who used Facebook had their own accounts. Fear of the negative connotation and perception of owning a Facebook account was a primary reason for women not having a private account. FP21, a 20 years old unmarried female participant said she uses Facebook to follow famous personalities but the account she uses belongs to her brother:

"I never felt the need to create my personal ID."

FP21 discussed fear as the primary reason for not opening her own private Facebook account. She believed that carrying a phone might invite male users to ask for her number and so chooses not to carry one. This fear also translates to social media as well so she does not have an account linked to her, as men might message her there (an occurrence other female participants have reported). The participant's usage is mostly following famous personalities and not communicating or uploading content so she is unaffected by the fact that it is her brother's account.

**4.5.3 Display Pictures.** Display picture is the profile picture that is used on WhatsApp. It's visibility can be set to 1) 'Everyone', 2) 'Contacts', 3) 'Only me'. Both WhatsApp about information and the 24 hours duration story are known as status. We will be referring to the 24 hours status in the following sections. Status allows more detailed privacy settings as compared to display picture as it allows making viewer lists to share status with 1) 'My contacts', 2) 'My contacts except' and 3) 'Only share with'. Only 13% of our female participants reported using their own picture as the WhatsApp display picture, whereas 76.5% males reported using their own display picture. Female participants used pictures of their fathers, brothers, children, husbands and random pictures from the Internet as their display picture. All the females who did not use their own picture as display picture reported not being allowed to do so by either male members of the family or parents. Similar to WhatsApp, 43.5% of the female participants who used Facebook reported not using their own display picture whereas only 11.8% of male participants did not use their own picture as their display picture. In addition to the reasons discussed earlier, female participants who did not use their own picture reported being afraid of someone taking a screenshot of their picture and making it viral. They discussed the significance of family honor and the importance of preserving it. FP18, a 22 years old female participant reported that men on Facebook might take a screenshot of her pictures so she does not use her own picture

"They [unknown men messaging on messenger] ask for selfie, then if one does not provide them with selfie they can take screenshot of display picture."

This disparity and restriction on using profile pictures on Facebook has also been reported in other work in South Asia [62].

The female participants who did use their own pictures as display picture on WhatsApp mentioned WhatsApp as being only for close friends and relatives who they trusted, therefore, they were not afraid to use their picture. FP7, who had talked to close friends and relatives on WhatsApp discussed this:

"I found out that nothing is wrong with this[using own picture as display picture] and no one will misuse it. Even if someone screenshots it I know they won't do anything."

On the other hand, male participants associated no such concern with uploading pictures as display pictures and simply mentioned uploading their own pictures as display picture

In contrast our participants were more comfortable with setting their personal pictures as a WhatsApp status. All male and female participants reported using this status feature on WhatsApp where users can upload pictures and videos that can be seen their contacts for up to 24 hours. WhatsApp is unique in the apps being used in that it seen as less public and most intimate allowing communication amongst people who are known in real life and are considered as part of the family's inner circle:

"Only my contacts can see it."

and

"People who have my number can see it."

Although male participants were aware of the viewer lists facilitated by WhatsApp as illustrated by MP11

"If I'll hide my status from some people, they will not be able to view it. It'll be visible to others."

they did not hide their status from members of the opposite gender or relatives like our female participants did.

However, participants misunderstand the privacy settings of WhatsApp's status visibility. Only the user's contacts can see the WhatsApp status if the status visibility is set to 'My contacts'. Our participants mentioned their status being visible to everyone, even though WhatsApp does not provide any such option. FP14, who owned the same phone as her husband, initially mentioned that only her contacts will be able to view her WhatsApp status, however, upon further probing, she explained

"If you have my number saved then you will be able to view my status and if I have your number saved I will be able to view your status."

21.7% of female participants reported uploading their pictures on WhatsApp status but not on display picture as WhatsApp status allowed them to make viewer lists where they could choose who they wished to share their status with. Some of the common viewer lists used by our female participants included: 1) only females, 2) only friends, 3) hiding from relatives, 4) hiding from employers, and 5) hiding from teachers in cases where children were using their mother's phone to contact teachers due to the pandemic situation.

**4.5.4 Facebook Limiting Access.** While most of our participants were aware of the Facebook privacy settings to limit access of pictures to everyone, friends, only me etc, unlike WhatsApp status content, women still did not trust Facebook limited lists enough to post their own pictures. Only 23.5% of male and 17.4% of female participants explicitly stated not being aware of limiting access to pictures and status updates. Although both WhatsApp and Facebook facilitate to limit visibility to pictures on granular levels, none of our participants were aware of these custom visibility lists offered by Facebook. When asked, all participants who knew about privacy settings of Facebook mentioned the main lists i.e., visible to everyone, friends, only me. None of the participants were aware of the 1) friends except 2) specific friends and 3) acquaintances lists.

Most common content that participants wanted to keep private on Facebook included family pictures and pictures of females (female participants reported this themselves and male participants

reported that they wished to keep pictures of females in their family private) as MP2 reported:

"For the personal settings, like pictures of home (i.e. pictures of family members), I have restricted (the facebook audience) to me. If I want to share something I have written, I share with friends. When I am outside, I share (content) as public. Say if I am out of city, then I share (content) as public."

There were a few features where we found no difference was between male and female participants. Such as majority of both reported being in WhatsApp groups of friends, family, work etc. Only two male and female participants were unaware of read receipts on WhatsApp. The rest of them knew about it and appreciated it because it allowed them to see if their message had been seen. Similar was the case with online status. 50% of both male and female participants knew about it and appreciated it as they could see who is online.

There was a significant difference in the number of male and female participants who set up their accounts themselves. Only 27.3% of the female Facebook users set up their Facebook account themselves whereas approximately 50% of males set it up themselves. However, female participants had access to fewer people who could configure and set up their account due to limited informal tech circles (discussed in Section 4.4) as compared to males.

## 5 DISCUSSION

We analyse our participants privacy perceptions, vulnerabilities and mechanisms through Nisenbaums contextual integrity lens [54], in combination with the vulnerability-centric framework presented by McDonald and Forte [45]. The contextual integrity framework which proposes that community norms that guide the flow of information in any context are regulated and dependent upon contextual variables such as social roles, process of transmission and type of information, is insufficient in and of itself for our analysis. While hugely influential in HCI to understand privacy in the Global North, it falls short of capturing the privilege and power differentials that dictate who actually gets to establish the norms of information flow in our context. We find that the dominant norms which motivate privacy practices are determined and enforced by the dominant gender - men. This is not surprising given the deeply patriarchal nature of Pakistani society. These deep rooted structures of patriarchy do not just impact women's privacy practices but also impact the way our male participants perform privacy. We find male participants privacy needs extend beyond just ensuring the safety and privacy of their own data but the use of specialized applications (modded apps) to control other users data privacy as well (e.g. gaining access to data 'deleted for everyone' on WhatsApp). Patriarchy encourages men to seek security, status, and other rewards through control and to identify being *in control* and having *power over* (the ability to control others, events and resources) as a continued goal of great importance [36]. We see this desire for control as central to how male participants perceive and perform privacy; controlling norms around how others should perceive privacy, and working to control other users privacy practices through modded apps. If we were to rely on only the contextual integrity framework to highlight the norms and in turn aim to design for them, we would perhaps

be further marginalizing an already vulnerable population (female users) whose privacy needs are often invisible. This is not to say our male participants do not experience their own vulnerabilities and marginalizations; most are low-literate and feel they carry the burden of ensuring the 'safety' of their families, even in digital spaces, using applocks and gallery locks to ensure pictures of their family are not accessible. While we emphasize the norms and we explore the perceptions and practices of the dominant class of people engaged in the setting of these norms we also augment the contextual integrity framework using McDonald and Forte's vulnerability-centric framework to explore the power dynamics at play in the setting of these 'norms', how these norms are visibly performed but secretly circumnavigated and the often invisible *vulnerabilities* of our participants that if not considered in the design of privacy affordances might further perpetuate existing inequalities.

Below we highlight two of the key vulnerabilities and norms that drive privacy behaviours and practices; 1. male-centered patriarchal structures which determine norms and, 2. religious beliefs and practices which determine 'appropriateness' of information flows and audiences. We then also present specific design implications based on our findings and this context.

### 5.1 Negotiating Patriarchal Norms

The privacy related norms we observe are determined and set by male beliefs of women's place in society, their beliefs of how women *should* be using technologies and how much access they should have to SNSs. One particularly relevant norm is belief in the need for privacy only when indulging in deviant behavior. In our context, privacy is not established or maintained within an individualistic framework but is understood as a collective, i.e. preserving the families privacy, honor and dignity. As a consequence our users strongly link the concept of privacy with scandal; the idea that if you have done nothing wrong you have nothing to 'hide'. Like prior work [34, 62] we find this is particularly true for female users who, even when they have their personal devices, share passwords with family members and want to give the impression of an 'open' device and digital space that family is free to monitor and see. This context of a sort of secret privacy, where users would like to enact specific boundaries but would like these boundaries to be invisible and untraceable has also been discussed by Sambasivan et al. when discussing women's privacy over shared phones [62]. However, we find this to be the norm even on personal devices and we find men also subscribe to this notion. Our male participants used specific applocks to differentiate between content that was 'open' and accessible to family and friends and content that they would like to keep private, but enact this privacy in a secret way using hidden applocks that look like innocuous applications (calculator or a clock). Privacy in general then in this context is seen as something to 'hide', by both genders and to be performed invisibly. Male participants however, have access to public spaces and are mobile unlike our female users. This means they have access to mobile repair shops and informal male circles for learning *how* to enact *invisible privacy*. In contrast, our female participants have no access to places, spaces or people who might be valuable sources of privacy related information. Their access to public spaces is limited, social connections are also restricted mostly to female family members [73] and most of

what they know about their phones and privacy affordances come from husbands, brothers or fathers, who are the dominant group here, setting the norms and determining the 'appropriateness' of which technologies and applications may be used, by whom and in what way. Our low-literate female participants can then only rely on those privacy features that are easily understood, provide tangible visual feedback in terms of the link between the setting used and the immediate feedback on boundary enacted such as deleting chats, using modded versions of WhatsApp to disappear (appear offline) or use male family members Facebook accounts. In all of this the key goal is to give the appearance of following the norms of content and information sharing and the right 'audience' with which it is being shared to uphold established patriarchal structures and existing power inequities.

### 5.2 Negotiating Religious Norms

Religion, modesty and the performance of piety are a second integral factor in how users decide what kind of content can be shared and with whom and what kind of contacts and relationships are 'appropriate'. We would go so far as to argue that in our context, privacy can not be conceptualized as a secular concept but must be (re-)imagined within a religious framework drawing from Islamic beliefs and understanding of what is appropriate, what are the boundaries that must be enacted and for whom. The central theme that drives an Islamic understanding of digital privacy is the belief in Purdah, for men and women both. While prior work has revealed the importance of religion and in particular, the belief in Purdah to have great importance in women's privacy practices [2, 7], we further reveal the importance of enacting 'Digital Purdah' for male users who explicitly use applocks just for WhatsApp conversations with female friends. Most of their added privacy behaviours like using secret applocks are to hide content that would be considered impermissible under Islamic beliefs (porn etc.). Similarly, most of the actual privacy practices and strategies adopted by our female participants are tailored towards enacting digital purdah; not using their own pictures as profile pictures, posting specifically in spaces like WhatsApp status where they can segregating viewer lists based on gender and the Islamic principles of '*mehram*'. Women are not required to observe Purdah from other women or a Mahram male. A *mehram* is defined under Islam as a member of one's family with whom marriage would be considered illegal. Purdah or concealment of the body with hijab/covering, from these members is not obligatory and with whom, if he is an adult male, she may be escorted during a journey. It is this definition of Mahram and gender that helps guide women in our context on segregating audiences for pictures, personal statuses etc. However, most platforms do not allow for such designations; none of the existing SNS's allow for easy gender based segregation of audiences and while Mahram men are family, not all family males are considered Mahram. There is no easy, simple way to enact Digital Purdah for our participants.

### 5.3 Implications for Design

In this section we discuss potential opportunities for design along multiple intersections revealed by our qualitative data; low-literacy,

gendered privacy beliefs and practices and Islamic beliefs that determine privacy boundaries and norms. For our low-literate populations WhatsApp is the most ubiquitously used application because it allows for voice notes, the result of privacy settings are almost immediately visible and tangible and it allows for the granularity of privacy control that other applications do not. While many of our design guidelines use WhatsApp as a case study, they can also be generalized and adopted by privacy designers in general:

- (1) **Private Mode.** While WhatsApp has options like delete for everyone and disappearing messages, these options leave some sort of residue or indicator of use (e.g. "message has been deleted"). As we know this is a concern for female users who need to perform privacy *invisibly*. Instead a *private conversation mode* would mean that there is no trace of the conversation or media left on the device. A private mode will allow any shared content to be restricted to that session only and private interactions will be broken down into sessions. Any shared media and messages would not be accessible outside the session after it has lapsed and there would not be a log of the session. After the user has backed out/closed the session he or she will not be able to see the conversation that happened in the private mode. The private mode addresses two main challenges reported by our participants; 1. the desire to have closed conversations about sensitive topics without the fear of some one else accessing them and 2. traces being left behind of private conversations and the inability to remove these traces. While the Internet browsers typically allow for incognito mode (similar to a private session), none of our users were aware of this or had used it. We recommend then that privacy features (like the private mode) are not embedded in menus which lowers the chance of low-literate users discovering such features during their explorations. We found out participants easily explore features (such as delete for everyone) that have smaller exploration costs, and immediate feedback on what the setting actually did.
- (2) **Notification about after-market App.** Participants who use the standard version of WhatsApp rely on the information the app is providing them (i.e this message is deleted for everyone, the participant was last seen online at a certain time) for their privacy practices. If the recipient is using GB or FM WhatsApp (modded versions), then participant might unknowingly be sharing information that they think they can delete for everyone later on, or the GB or FM WhatsApp user might be viewing their content, like WhatsApp Status, without the users knowing about it. It is important that users in conversation with modded apps be notified if a contact is using a modified version of WhatsApp. User's should then have the option of either blocking the contact or agreeing to communicate over a modded version. This will caution users from sharing any content that might be sensitive with the modded WhatsApp user and not rely on read receipts, status views list (list of people who have viewed your WhatsApp status), delete for everyone etc for privacy purposes. Moreover, while these modded applications might use the source code of the official application, they have no guarantee about

the safety and security of the data that is being shared as they are not licensed applications.

- (3) **Enacting Digital Purdah.** A recurring concern for our participants is the desire to customize content and limit audiences based on the Islamic practices of Purdah and the understanding of who a *Mahram* is and what content is then suitable for them. While some social networking platforms like Facebook provide mechanisms for limiting audiences, these are based on secular values and do not easily allow for gender segregation or having a tiered mechanism where contacts maybe assigned a family role and then a subset of that as a *Mahram* with special privileges; a Mahram is always family but all male family members are not considered *Mahram*. This could mean multiple custom (status) lists on WhatsApp allowing users to upload their WhatsApp statuses (images and videos that expire in 24 hours) for specific lists of contacts. Currently, users only have the option to hide their status from specific participants but not generate custom audience lists. For women who are trying to enact Purdah in digital spaces, features like this would not only enable them to share their pictures with *Mahram men* and women only, but also give the appearance of them following cultural and religious norms to any outsider (discussed in Section 5.1) in their contact list by ensuring that women have control over limiting what broader circles can see. Similarly, because social networking sites like Facebook are based on a secular understanding of privacy women have to find workarounds to enact Purdah in online spaces i.e. gender segregated accounts. Easy gender segregation and assigning of specific roles to audiences based on Islamic values would perhaps allow Muslim users to engage more fully with online platforms.
- (4) **Content forwarding.** One major concerns our female participants highlighted was their pictures being forwarded or circulated without their consent as WhatsApp makes it easy to mass share pictures in groups. If these pictures of the participant themselves, then it can have severe consequences and backlash from male relatives or family members (Discussed in Section 4.1). We suggest that users should be able to flag certain media as personal before sharing, and if the recipient forwards that media then the sender should be informed or the media, if embedded with specific metadata not be forward-able. Accompanying meta data can be added along with the pictures/videos flagged as private to separate them from mainstream content and track or block their forwarding. WhatsApp already tracks the forwarding of media that has been frequently forwarded and flags them as 'forwarded' and 'forwarded many times' but this feature doesn't inform the user if their personal content is forwarded.
- (5) **Privacy Visualisation.** A significant challenge for our low literate participants was to understand Facebook's multi-level privacy settings, in contrast to WhatsApp, which was readily understood. One of the reasons for this was that the exploration cost for privacy settings was lower on WhatsApp (Generalized menu, Larger grouping, lesser options), but more importantly WhatsApp shows immediate and tangible feedback of privacy preserving mechanisms that the

participants were using. For example, while our participants did not know the difference between the 'delete for me' and 'delete for everyone' options, they understood their function because selecting an option provided immediate visual feedback i.e message disappears and instead a different lighter coloured text appears ('You deleted this message') and when it is 'deleted for me' the message body disappears. This is unlike most social networking sites, where you may add people to a custom viewer list, but you do not immediately see how each audience list or group interacts with your content, there is no feedback to show *how* the setting would work. We recommend applications and social networking sites consider providing some form of visual feedback for allowing immediate recognition of a privacy affordance. For example, Facebook could provide the option to view as particular audience member (women, family etc). Similarly, a significant concern for all our participants (and in particular women) was the possibility of screenshots of their private conversations being leaked and their pictures being used to blackmail through screenshots. Currently, there is no mechanism that disallows this on the most ubiquitously used applications like WhatsApp and Facebook. One mechanism to counter this would be to either dis-allow screenshots of the conversation or send feedback to users if a screenshot is taken.

## 6 LIMITATIONS

Although our research included a diverse sample, it may be subject to common limitations of qualitative studies including self-censorship of participants, recall and observer bias. It is in particular difficult to get at inherent power differentials in patriarchal communities and our data often depended on what the participants wished to share with us. Furthermore, parents were present in the interviews of participants aged under 18 which might have led participants censoring information. Moreover, the sample is limited to Pakistan only, however, the findings that we discuss are reflective of a larger South Asian and Muslim populations.

## 7 FUTURE WORK

This study is a first step in understanding privacy behaviours and perceptions of low-literate users in a patriarchal context. Future directions of work could include exploring mechanisms for privacy prompts that would be most meaningful in this context, given that existing prompts are wholly unsuited. In particular exploring vulnerability-centered privacy prompts and protections. As our work reveals, men and women in our population have unique privacy concerns and experience different harms. Therefore, it might be useful to explore designing individualized privacy prompts, warnings and privacy protections targeting specific user vulnerabilities.

## 8 CONCLUSION

Our study of low-income, low-literate users privacy perceptions, beliefs and behaviours makes several contributions to HCI. We deepen the understanding of privacy from a cultural and religious perspective for both male and female participants. We also extend conversations on the impact of patriarchal norms on male privacy practices in HCI, the mechanisms women in these contexts use to

circumnavigate *norms* that they are expected to uphold and the specific privacy-related vulnerabilities arising from low-literacy. In particular, we highlight the non-secular nature of privacy as perceived and practiced in our context and the lack of affordances that allow for friction-less performance of these practices in digital spaces. Our work highlights the potential pitfalls of privacy designs which focus on *community norms* without an exploration into who is setting the norms, who benefits from them and who is excluded, raising the very real risk of reinforcing privileged notions of privacy and territory.

## REFERENCES

- [1] Norah Abokhodair, Sofiane Abbar, Sarah Vieweg, and Yelena Mejova. 2016. Privacy and twitter in qatar: traditional values in the digital world. In *Proceedings of the 8th ACM Conference on Web Science*. Association for Computing Machinery, New York, NY, USA, 66–77.
- [2] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & social media in the context of the Arab Gulf. In *Proceedings of the 2016 ACM conference on designing interactive systems*. Association for Computing Machinery, New York, NY, USA, 672–683.
- [3] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce* (Denver, Colorado, USA) (*EC '99*). Association for Computing Machinery, New York, NY, USA, 1–8. <https://doi.org/10.1145/336992.336995>
- [4] Shane Ahern, Dean Eckles, Nathaniel S. Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) (*CHI '07*). Association for Computing Machinery, New York, NY, USA, 357–366. <https://doi.org/10.1145/1240624.1240683>
- [5] Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (Ann Arbor, MI, USA) (*ICTD '16*). Association for Computing Machinery, New York, NY, USA, Article 11, 10 pages. <https://doi.org/10.1145/2909609.2909661>
- [6] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–20.
- [7] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. "Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–13.
- [8] Syed Ishtiaque Ahmed, Maruf Hasan Zaber, Mehrab Bin Morshed, Md Habibullah Bin Ismail, Dan Cosley, and Steven J Jackson. 2015. Suhrid: A collaborative mobile phone interface for low literate people. In *Proceedings of the 2015 Annual Symposium on Computing for Development*. Association for Computing Machinery, New York, NY, USA, 95–103.
- [9] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies*. Association for Computing Machinery, New York, NY, USA, 32–43.
- [10] Deena Alghamdi, Ivan Flechais, and Marina Jirotko. 2015. Security practices for households bank customers in the Kingdom of Saudi Arabia. In *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015*. USENIX Association, USA, 297–308.
- [11] Kamran Asdar Ali. 2012. Women, work and public spaces: Conflict and coexistence in Karachi's poor neighborhoods. *International Journal of Urban and Regional Research* 36, 3 (2012), 585–605.
- [12] World Bank. 2019. Literacy rate, adult total (% of people ages 15 and above) - Pakistan. <https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?locations=PK>
- [13] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. 2011. On the Need for Different Security Methods on Mobile Phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (Stockholm, Sweden) (*MobileHCI '11*). Association for Computing Machinery, New York, NY, USA, 465–473. <https://doi.org/10.1145/2037373.2037442>

- [14] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond Untagging: Photo Privacy in a Tagged World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) (CHI '10). Association for Computing Machinery, New York, NY, USA, 1563–1572. <https://doi.org/10.1145/1753326.1753560>
- [15] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2010. The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction* (Funchal, Portugal) (TEI '11). Association for Computing Machinery, New York, NY, USA, 197–200. <https://doi.org/10.1145/1935701.1935740>
- [16] Aisha Wood Boulanour. 2006. The notion of modesty in Muslim women's clothing: An Islamic point of view. *New Zealand Journal of Asian Studies* 8, 2 (2006), 134.
- [17] Nela Brown and Tony Stockman. 2013. Examining the Use of Thematic Analysis as a Tool for Informing Design of New Family Communication Technologies. In *Proceedings of the 27th International BCS Human Computer Interaction Conference* (London, UK) (BCS-HCI '13). BCS Learning & Development Ltd., Swindon, GBR, Article 21, 6 pages.
- [18] M.I. Bukhārī. 2002. *Manners in Islam*. Darul Ishaat, ". <https://books.google.com.bd/books?id=wOvXAAAAMAAJ>
- [19] Rong Chen. 2021. *A Demand-Side View of Mobile Internet Adoption in the Global South*. The World Bank, World Bank, Washington, DC. <https://doi.org/10.1596/1813-9450-9590> arXiv:<https://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-9590>
- [20] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powladge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA) (CHI '05). Association for Computing Machinery, New York, NY, USA, 81–90. <https://doi.org/10.1145/1054972.1054985>
- [21] Arijit Datta, Vimal Bhatia, Josef Noll, and Sudhir Dixit. 2019. Bridging the Digital Divide: Challenges in Opening the Digital World to the Elderly, Poor, and Digitally Illiterate. *IEEE Consumer Electronics Magazine* 8, 1 (2019), 78–81. <https://doi.org/10.1109/MCE.2018.2867985>
- [22] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) (CHI '14). Association for Computing Machinery, New York, NY, USA, 2937–2946. <https://doi.org/10.1145/2556288.2557097>
- [23] Jayati Dev, Pablo Moriano, and L. Jean Camp. 2020. Lessons Learnt from Comparing WhatsApp Privacy Concerns across Saudi and Indian Populations. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, USA, Article 5, 17 pages.
- [24] Pankaj Doke and Anirudha Joshi. 2015. Mobile Phone Usage by Low Literate Users. In *Proceedings of the 7th International Conference on HCI, IndiaHCI 2015* (Guwahati, India) (IndiaHCI '15). Association for Computing Machinery, New York, NY, USA, 10–18. <https://doi.org/10.1145/2835966.2835968>
- [25] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) (CCS '14). Association for Computing Machinery, New York, NY, USA, 750–761. <https://doi.org/10.1145/2660267.2660273>
- [26] World Economic Forum. 2021. Global gender gap report 2021. <https://www.weforum.org/reports/global-gender-gap-report-2021>
- [27] Batya Friedman, Kristina Hook, Brian Gill, Lina Eidmar, Catherine Sallmander Prien, and Rachel Severson. 2008. Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges* (Lund, Sweden) (NordCHI '08). Association for Computing Machinery, New York, NY, USA, 142–151. <https://doi.org/10.1145/1463160.1463176>
- [28] Imran Gabol and Taser Subhani. 2016. Qandeel Baloch murdered by brother in Multan. *Dawn News* 1 (2016), 1–6.
- [29] GSMA. 2021. Addressing the Mobile Gender Gap in Pakistan. <https://www.gsma.com/mobilefordevelopment/resources/addressing-the-mobile-gender-gap-in-pakistan/>
- [30] Abdul Hadi et al. 2017. Patriarchy and gender-based violence in Pakistan. *European Journal of Social Sciences Education and Research* 10, 2 (2017), 297–304.
- [31] Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2012. Too Much Information! User Attitudes towards Smartphone Sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design* (Copenhagen, Denmark) (NordCHI '12). Association for Computing Machinery, New York, NY, USA, 284–287. <https://doi.org/10.1145/2399016.2399061>
- [32] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 213–230. <https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach>
- [33] Samia Ibtasam. 2021. For God's Sake! Considering Religious Beliefs in HCI Research: A Case of Islamic HCI. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 9, 8 pages. <https://doi.org/10.1145/3411763.3450383>
- [34] Samia Ibtasam, Lubna Razaq, Maryam Ayub, Jennifer R Webster, Syed Ishtiaque Ahmed, and Richard Anderson. 2019. "My cousin bought the phone for me. I never go to mobile shops." The Role of Family in Women's Technological Inclusion in Islamic Culture. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–33.
- [35] ITUPublications. 2021. Digital trends in Asia and the Pacific 2021.
- [36] Allan G Johnson. 2004. Patriarchy, the system. *Women's lives: Multicultural perspectives* 3 (2004), 25–32.
- [37] Simon Jones and Eamonn O'Neill. 2010. Feasibility of structural network clustering for group-based privacy control in social networks. In *proceedings of the sixth symposium on usable privacy and security*. Association for Computing Machinery, New York, NY, USA, 1–13.
- [38] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can i Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) (CHI '09). Association for Computing Machinery, New York, NY, USA, 1647–1650. <https://doi.org/10.1145/1518701.1518953>
- [39] Naveena Karusala, Apoorva Bhalla, and Neha Kumar. 2019. Privacy, Patriarchy, and Participation on Social Media. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) (DIS '19). Association for Computing Machinery, New York, NY, USA, 511–526. <https://doi.org/10.1145/3322276.3322355>
- [40] Naveena Karusala and Neha Kumar. 2017. Women's Safety in Public Spaces: Examining the Efficacy of Panic Buttons in New Delhi. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) (CHI '17). Association for Computing Machinery, New York, NY, USA, 3340–3351. <https://doi.org/10.1145/3025453.3025532>
- [41] Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Elaine Newton. 2005. Privacy Perceptions in India and the United States: An Interview Study. In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)* 1 (September 2005), 1–13. [http://precog.iitd.edu.in/Publications\\_files/tprc\\_2005\\_pk\\_lc\\_en.pdf](http://precog.iitd.edu.in/Publications_files/tprc_2005_pk_lc_en.pdf)
- [42] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) (CHI '11). Association for Computing Machinery, New York, NY, USA, 3217–3226. <https://doi.org/10.1145/1978942.1979420>
- [43] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luis Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 159–174. <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/marques>
- [44] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll Just Grab Any Device That's Closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) (CHI '16). Association for Computing Machinery, New York, NY, USA, 5921–5932. <https://doi.org/10.1145/2858036.2858051>
- [45] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–14. <https://doi.org/10.1145/3313831.3376167>
- [46] Tanya McGill and Nik Thompson. 2018. Gender differences in information security perceptions and behaviour. In *Australasian Conference on Information Systems 2018*. University of Technology, Sydney, Australia.
- [47] Mary Meeker. 2014. Internet trends 2014-code conference. Retrieved May 28 (2014), 2014.
- [48] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 138 (apr 2021), 24 pages. <https://doi.org/10.1145/3449212>
- [49] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2012. Understanding Users' Requirements for Data Protection in Smartphones. , 228–235 pages.
- [50] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Munich, Germany) (MobileHCI '13). Association for Computing Machinery, New York, NY, USA, 271–280. <https://doi.org/10.1145/2493190.2493223>



- [51] Maryam Mustafa, Amna Batool, Beenish Fatima, Fareeda Nawaz, Kentaro Toyama, and Agha Ali Raza. 2020. Patriarchy, Maternal Health and Spiritual Healing: Designing Maternal Health Interventions in Pakistan. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–13. <https://doi.org/10.1145/3313831.3376294>
- [52] Maryam Mustafa, Shaimaa Lazem, Ebtisam Alabdulqader, Kentaro Toyama, Sharifa Sultana, Samia Ibtasam, Richard Anderson, and Syed Ishtiaque Ahmed. 2020. IslamicHCI: Designing with and within Muslim Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–8. <https://doi.org/10.1145/3334480.3375151>
- [53] Jema David Ndibwile, Edith Talina Luhanga, Doudou Fall, Daisuke Miyamoto, and Youki Kadobayashi. 2018. A Comparative Study of Smartphone-User Security Perception and Preference towards Redesigned Security Notifications. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities* (Windhoek, Namibia) (AfriCHI '18). Association for Computing Machinery, New York, NY, USA, Article 17, 6 pages. <https://doi.org/10.1145/3283458.3283486>
- [54] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
- [55] Government of Punjab. 2021. The Punjab Minimum Wages Notification 2021. <https://labour.punjab.gov.pk/node/86>
- [56] Hanna Papanek. 1973. Purdah: Separate worlds and symbolic shelter. *Comparative studies in society and history* 15, 3 (1973), 289–325.
- [57] Southern Asia Population. 2021. Southern Asia Population 2021. <https://worldpopulationreview.com/continents/southern-asia-population>
- [58] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 2020. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, USA, 1949–1966. <https://www.usenix.org/conference/usenixsecurity20/presentation/reichel>
- [59] Oliver Rowntree and Matthew Shanahan. 2020. The Mobile Gender Gap Report 2020. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf>
- [60] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. 2019. What About My Privacy, Habibi?. In *IFIP Conference on Human-Computer Interaction*. Springer, Cham, 67–87.
- [61] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14. <https://doi.org/10.1145/3290605.3300232>
- [62] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 127–142. <https://www.usenix.org/conference/soups2018/presentation/sambasivan>
- [63] Klaus Schwab, Richard Samans, Saadia Zahidi, Till Alexander Leopold, Vesselina Ratcheva, Ricardo Hausmann, and Laura D Tyson. 2017. The Global Gender Gap report 2017.
- [64] Anna J Secor. 2002. The veil and urban space in Istanbul: women's dress, mobility and Islamic knowledge. *Gender, Place and Culture: A Journal of Feminist Geography* 9, 1 (2002), 5–22.
- [65] Julian Seifert, Alexander De Luca, Bettina Conradi, and Heinrich Hussmann. 2010. TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones. In *Proceedings of the 8th International Conference on Pervasive Computing* (Helsinki, Finland) (Pervasive'10). Springer-Verlag, Berlin, Heidelberg, 130–137. [https://doi.org/10.1007/978-3-642-12654-3\\_8](https://doi.org/10.1007/978-3-642-12654-3_8)
- [66] Aditya Vashistha Shrirang Mare and Richard Anderson. 2017. Security and privacy design considerations for low-literate users in developing regions. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 1–4. <https://www.usenix.org/conference/soups2017/workshop-program/wips2017/mare>
- [67] Hanul Sieger and Sebastian Möller. 2012. Gender Differences in the Perception of Security of Mobile Phones. In *Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services Companion* (San Francisco, California, USA) (MobileHCI '12). Association for Computing Machinery, New York, NY, USA, 107–112. <https://doi.org/10.1145/2371664.2371685>
- [68] Molly Steenson and Jonathan Donner. 2009. Beyond the Personal and Private: Modes of Mobile Phone Sharing in Urban India. *The Reconstruction of Space and Time: Mobile Communication Practices* 1 (01 2009), 231–250.
- [69] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-Based Authentication on Mobile Devices. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Munich, Germany) (MobileHCI '13). Association for Computing Machinery, New York, NY, USA, 261–270. <https://doi.org/10.1145/2493190.2493231>
- [70] Emanuel von Zezschwitz, Sigrid Ebbinghaus, Heinrich Hussmann, and Alexander De Luca. 2016. You Can't Watch This! Privacy-Respectful Photo Browsing on Smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) (CHI '16). Association for Computing Machinery, New York, NY, USA, 4320–4324. <https://doi.org/10.1145/2858036.2858120>
- [71] Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 1427–1441. <https://doi.org/10.1145/2675133.2675256>
- [72] Susan Wyche. 2017. Exploring women's everyday mobile phone experiences in Nairobi, Kenya. *Interacting with Computers* 29, 3 (2017), 391–402.
- [73] Fouzia Younas, Mustafa Naseem, and Maryam Mustafa. 2020. Patriarchy and Social Media: Women Only Facebook Groups as Safe Spaces for Support Seeking in Pakistan. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development* (Guayaquil, Ecuador) (ICTD2020). Association for Computing Machinery, New York, NY, USA, Article 11, 11 pages. <https://doi.org/10.1145/3392561.3394639>