"Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia

Nithya Sambasivan, Garen Checkley, Amna Batool[#], Nova Ahmed[*], David Nemer[+], Laura Sanely Gaytán-Lugo[Ω], Tara Matthews[Ψ], Sunny Consolvo, and Elizabeth Churchill

Google Inc., Mountain View, CA, USA,
{nithyasamba, garen, sconsolvo}@google.com, churchill@acm.org
[#] Information Technology University, Pakistan
batool.amna@itu.edu.pk
[*] North South University, Bangladesh
nova.ahmed@northsouth.edu
[+] University of Kentucky, USA
david.nemer@uky.edu
[Ω] Universidad de Colima, Mexico
laura@ucol.mx
[Ψ] Independent Researcher
taramatthews@gmail.com

ABSTRACT

Women in South Asian own fewer personal devices like laptops and phones than women elsewhere in the world. Further, cultural expectations dictate that they should share mobile phones with family members and that their digital activities be open to scrutiny by family members. In this paper, we report on a qualitative study conducted in India, Pakistan, and Bangladesh about how women perceive, manage, and control their personal privacy on shared phones. We describe a set of five performative practices our participants employed to maintain individuality and privacy, despite frequent borrowing and monitoring of their devices by family and social relations. These practices involved management of phone and app locks, content deletion, technology avoidance, and use of private modes. We present design opportunities for maintaining privacy on shared devices that are mindful of the social norms and values in the South Asian countries studied, including to improve discovery of privacy controls, offer content hiding, and provide algorithmic understanding of multiple-user use cases. Our suggestions have implications for enhancing the agency of user populations whose social norms shape their phone use.

1. INTRODUCTION

A large and growing population of nearly 760 million women live in India, Bangladesh, and Pakistan [55–57]. One of the highest worldwide gaps in phone ownership is among women in South Asia (that is, the sub-Himalayan region of eight southern Asian countries including India, Pakistan and Bangladesh). Here, women are 26% less likely to own a mobile phone compared to men [17]. Twenty-nine percent of South Asian women regularly borrow a phone [16]. Even when phones are individually owned—*i.e.*, in the possession of a user for a majority of the time—women in many South Asian contexts face cultural expectations to share their devices and digital activities. For example, in a survey conducted by GSMA, men, and sometimes women too, found it acceptable for a husband to check his wife's digital activity on her phone [16].

However, in the design and development of mobile devices and services, user privacy is predominantly modeled on the "one account, one user" paradigm, despite the fact that shared device usage of devices challenges the definition, architecture, and presentation of privacy controls developed on this assumption [3,7,23,36,37,40,44].

Prior work in various cultural contexts has focused on shared device practices among families, co-workers, friends and strangers, identifying factors such as economic constraints and social values that drive shared use [7,23,36,37,40,44]. Fewer studies have focused on social power relations as drivers for shared use and the resulting privacy practices and challenges, for example in settings where cultural expectations shape mobile phones that are shared and digital activities that are scrutinized by family relations.

In this paper, we examine the ways in which current technology designs could better support the privacy challenges of women in South Asia We explore two main questions:

- How do women in South Asia perceive, manage and control their privacy on shared mobile phones?
- How are social expectations of women fulfilled through technological and social affordances?

We report results from a study with 199 women in India, Pakistan, and Bangladesh who were owners of phones (167 of them owned smart phones, 22 had feature phones). Among our key findings

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018. August 12 -- 14, 2018, Baltimore, MD, USA.

were that our participants' digital activities on their phones were carefully monitored by close social relations, and participants' mobile phones were highly shared between people in their household.

In addition to describing the social context in which women's phones were shared and their use was monitored, we describe five performative practices used by our participants that allowed them to maintain some individual privacy on their mobile phones while adhering to cultural values of transparency and sharing that were expected of women's gender roles. These practices were: *phone locks* for prevention of misuse by strangers; *app locks* for securing content and applications from weak ties and children; *aggregate* and *entity deletions* of content, queries, recommendations, and history to remove content traces from everyone's view; *private modes* to enter private experiences; and *avoidance* of certain digital activities situationally or permanently. These ordinary privacy practices became performative when they enabled the women in our study to balance their gender role expectations of openness, manifested in openly shared phones and apps, with their own desire for privacy on devices. The repertoire of mostly covert and sometimes overt privacy practices was employed as needed in various social situations. For example, by selectively deleting search queries, our participants maintained covert privacy while not signaling that they were hiding anything from those who shared or monitored their devices. We also recommend several design suggestions that we hope will better support the needs of user groups that face cultural expectations to share mobile phones, such as offering content hiding, transience, and improved algorithmic feedback for shared use.

The paper is structured as follows. We begin by situating our research in related work. We then describe our study methodology and follow with our results. Finally, we make recommendations for designing technology for contexts in which device sharing is common and expected.

2. RELATED WORK

To situate our research contributions, we discuss related work on device sharing and access controls with social relations, device monitoring by social relations, and research at the intersection of gender and privacy.

2.1 Device sharing & access controls

Several research studies document the social practices around device sharing. We focus primarily on the literature on device sharing in South Asia, because of cultural similarities with our study. Definitionally, Matthews *et al.* define 'device sharing' as the action of using a device or an account by two or more people, simultaneously or one after another [29]. Studies in the West have documented a range of concerns with shared devices: for example fears of data being deleted [23]; desire to use profiles to personalize content instead of achieving privacy over content [7]; and how children act as trusted adversaries in households [41].

Prior work from South Asia has focused on the prevalence of shared phone use, exploring both economic constraints and cultural values. Cultures of shared technologies are so prevalent in these regions that James and Versteeg argue that subscriptions and accounts are not a reliable measure of mobile phone access; rather phone usage remains the best measure [21].

Others have examined the motivations and practices around phone sharing in South Asia. Steenson and Donner describe how mobile phones were shared in Indian households along two dimensions: proximity and socio-spatial contexts [44]. They observed that phone sharing may occur informally due to co-presence or stealthily without the owner's knowledge. Phones were also shared when they were used to call someone known to be near the phone, or when the phone was used as a family landline. Sambasivan *et al.* describe how devices are shared in low-resource communities due to the presence of fewer devices, leading to 'intermediated usage,' where technologically aware members may use technologies on behalf of those with lower technical literacy; thus intermediation vastly expanded access to devices, especially for women [40]. Rangaswamy and Sambasivan describe how technologies were fluidly shared in slum communities in India, deriving more value out of less money [36]. They invoke a local term, *cutting chai*, used to share a cup of tea among many members, as a metaphor for how a device is divided among many users.

Access controls can help users cope with device sharing. Little has been said about access controls in shared device environments in South Asia, though. A notable exception is a study by Ahmed *et al.* [3] on privacy challenges with shared mobiles. They showed that device sharing is a cultural practice that can be affected by power relations. The authors briefly discuss gender dynamics, but this was not the study's focus.

The literature on access controls from the West is extensive; for example, user profiles, locks, and logins have been well-researched in Western contexts [6,7,11,12,18,19,23]. Across these studies, common themes include the importance of appropriate access controls, flexibility, and customization for various social contexts.

Family profiles have been reported to be a good middle ground between individual profiles and a single shared account for all users, in environments where privacy and security requirements across users is less stringent [11]. Guest profiles with discrete switching have been recommended to avoid misunderstanding [31]. Karlson *et al.* showed that the binary access models on phones do not address the social discomfort users experience when sharing phones [23]. Transparency of access controls to avoid social implications has been suggested by Harbach *et al.* and Mazurek *et al.* [18,31]. Logins [6] and locks [12,19] have been studied, for example, showing that all-or-nothing lock models do not fit the needs of users [19], and that users may not make a connection between sensitive data in apps and the need for locking [12].

Most prior studies on device sharing and access controls have been conducted in the West, where adult users are typically not socially obligated to share their phones to the same extent as women in the South Asian countries we studied. In contrast to prior studies in South Asia, which have focused on women as borrowers or recipients of sharing [36,40,44], all our participants owned their Internet-enabled phones but were still culturally obligated to share with others. We describe privacy techniques employed by our participants, showing how they fulfill cultural expectations of sharing and yet maintain some privacy on their devices. We further show how many of these practices are unanticipated workarounds due to poor app usability.

2.2 Device monitoring by social relations

Our study revealed that women's devices in South Asia are monitored by their social relations (including husbands, brothers,

parents, and children). While some device sharing research touches upon device monitoring by social relations, a series of other studies, with a range of specialized populations, focus on these issues. As an overview, Marques *et al*. [28] showed that snooping on other's phones is something that an estimated 1 in 5 U.S. adults had done in the year prior to their survey. Monitoring of device use by social relations has been studied in multiple more focused contexts, including (but not limited to) parents monitoring children (*e.g*., [8,15,51,52]), snooping in romantic relationships (*e.g*., [9,28]), and intimate partner abuse (*e.g*., [10,13,14,30,43,53]. Much of this monitoring research has occurred in Western contexts, barring the exception of a study of Bangladeshis' shared phone use [3] and a high level overview of this team's research on gender equity [39], which both allude to monitoring of women's phones.

A common theme in this literature is that monitoring *does* occur, but it is often *not* a socially desirable behavior in the West. Monitoring is generally more accepted in parent-child relationships, but it still not necessarily welcome by the person being monitored [15]. Another theme is that study subjects try to maintain privacy from social relations but face various challenges. For example, abusers go to great lengths to monitor and control survivors (such as coercing survivors into physically sharing a device, or covertly installing spyware on the survivor's device), leading some survivors to take drastic actions like deleting accounts or abandoning devices [13,14,30,43]. In studies with a general population, willing device sharers have expressed an obligation to give open access to close relations to communicate trust, which opened them up to snooping [29].

While our study also discusses monitoring by social relations, the cultural context—especially the acceptability of social monitoring—is very different from prior work. Our study explores an under-studied population and describes a variety of cultural factors that result in the commonplace and sometimes accepted practice of social relations regularly monitoring women's devices in South Asia, and how the women perceive and react to this reality.

2.3 Gender and privacy

A growing body of research observes that women's use of technology in South Asia is limited and controlled by cultural norms in a variety of ways. Privacy is sometimes discussed, but the focus is primarily on the ways in which women's use of technology is limited. For example, technology needs and perceptions are different depending on a person's gender [34]. An emerging area of research is concerned with women living in gender-unequal contexts [2,3,22,24,39,40,46–48]. Restrictive gender norms limit the impact of information technologies for women in practice [3,39,47]. For example, Abokhodair and Vieweg, in their research study in Saudi Arabia and Qatar, reported that women preferred to keep their online presence private and restricted to same-gender interactions [1]. Meanwhile, Sultana *et al*. detail how some women depended on their husbands, even in emergency situations, as they were required to wait until their husbands returned home in order to make phone calls [47]. Murphy and Priebe present a well-rounded literature review on how class, race and sex shape women's attitudes towards mobile phones, by discussing cases from India that reveal how gendered perceptions of modesty conflict with phone ownership [32]. Sambasivan *et al*. briefly describe device sharing and privacy practices employed by women in South Asia, in a broader research overview of gender and technology [39].

However, technology can be empowering to women. For example, research by Alghamdi *et al*. showed how online banking enabled Saudi women to perform banking transaction from home, giving them new financial autonomy. When the task had to be completed in public, their male family members had to transact on their behalf due to Islamic principles of gender segregation [4]. In another example in Morocco, where unrelated women and men engaging on phones was culturally taboo, SMS codes helped women communicate with water managers [46].

While these examples touch upon some implications for how women in South Asia experience privacy, it is not their focus and so we do not have a full understanding of the privacy issues women face and how they cope with them. Our work contributes to this body of work by focusing on women's privacy challenges and practices in a cultural setting where device and account sharing is typical. Distinctively, women in our study *had* access to phones and were not reliant on borrowed phones.

3. METHODOLOGY

Our research inquiry was focused on understanding mobile phones in daily life, as part of a larger project on studying how women in South Asia encountered technology. We conducted focus groups with a total of 199 women. The research was conducted from May to December of 2017. In total, we conducted over 500 hours of fieldwork across India, Pakistan, and Bangladesh (see Table 1 in appendix for a breakdown of participants and sites). We conducted focus groups of three participants per group (triad focus groups) with 199 participants who identified as women. Focus groups were chosen because it was easier to break the ice and share common experiences on the sensitive nature of the topics covered. Each focus group session lasted about 2 hours on average. The focus group discussions were semi-structured in nature and organized around aspirations, phone and Internet use, device sharing, privacy practices, identity models, and safety concerns. We ended every focus group by asking the participants what topics or issues they would like to highlight the most in our research reports, giving them a chance to reflect upon the conversations and represent their voices in their own terms. Interview questions are provided in the appendix.

The study followed a comparative fieldwork format [33]; rather than a thick description of behavior and context, comparative fieldwork helped us understand points of transition where phenomena break, continue, or transform.

Here we describe participant recruitment, data collected, analysis, and ethical considerations in reporting this research.

3.1 Participant recruitment

Participants were recruited through a combination of non-governmental organizations (NGOs), personal contacts, and recruitment agencies, using snowball and purposive sampling that was iterative until saturation. Prior to the sessions, recruitment contacts and NGO staff verbally mentioned the purpose of the study, the categories of questions (access, information & content, privacy and safety), and the affiliation of the researchers, providing potential participants an opportunity to decline participation prior to any contact with our team.

Focus group participants were already known to each other, like friends and neighbors, in order to help with rapport and trust. Incentives varied depending on the country, demographic and

format of session. Sample size was determined based on ensuring representative coverage, balanced with recruitment resources available in each country. In order to obtain a well-balanced sample, participant recruitment was divided such that roughly a third of participants each were of high, medium, and low socioeconomic status (SES) as determined by SES definitions per country and verified through income, education and material possessions [27]. Participants were from 18 to 65 years old. All were Internet-enabled phone owners. See the appendix for more detail.

3.2 Moderation and incentives

In all three countries, focus group moderators were native female researchers and regional language speakers, to leverage common cultural ground [25]. Another researcher took notes. Due to the mixed gender nature of our design-research team, male designers were observers during interviews. Country-specific incentives are noted below. The incentives were ethically determined to not be coercive, based on socio-economic segments. Incentives were determined via research experts from and specialized in the countries. All participants were verbally thanked for their time at the end of interviews.

3.3 Analysis

Interviews were conducted in local languages and translated to English in transcription (see country sub-sections below). Inductive analysis was conducted on the raw interview data [49]. We focused on stories about (1) access to devices and software; (2) technology usage by women; (3) privacy considerations in shared spaces; (4) management of uncomfortable or sensitive information on shared devices; (5) identity and account handling in shared use situations; and (6) aspirations for a different social order around device usage. From a close reading of transcripts, we developed categories and clustered excerpts together, conveying key themes from the data. Three team members created a code book based on the themes, with four top-level categories (identity, co-located privacy, access, online privacy) and several sub-categories *e.g.*, micro-deletions, public environments, and technology literacy). Codes were iterated in the order of conducting research: India codes were developed first, then iterated with Bangladesh and Pakistan. The five practices that are the focus of our results were then developed and applied iteratively to the codes (see appendix).

3.4 Research ethics

To protect our participants and to create neutral and non-judgmental spaces, we invited them to coffee shops, restaurants, university campuses, and NGO locations where they felt safe and comfortable. Having a neutral, safe space was important as contextual interviews in the home or work posed the possibility of other co-located members like in-laws and children overhearing, which could open up possibilities of participant harm and compromise accuracy of responses. Same-gender and same-ethnicity moderation was employed to leverage common cultural ground and build trust. Note-takers were men on our research team, who positioned themselves to sit in the background to not obstruct the rapport between the participants and moderator. For sensitive topics, such as privacy and surveillance, male research members pro-actively left the room to give participants space.

Verbal informed consent was translated by a native speaker into local languages, explained and obtained from all participants. Fifteen-to-twenty minutes were spent explaining the purpose of the interviews, answering any questions, and building rapport. Participants were made aware that they had the right to terminate the study at any point without forfeiting the incentive. Methods of recording, *i.e.*, audio, video, notes, or none of the above, were explained to participants, who chose the most comfortable technique. In a few interviews, we stopped recording and taking notes when participants became emotional; we retroactively wrote textual notes after the interview. All data were stored on a locked Google Drive folder, with access limited to the research team.

Only pseudonyms are used in this paper. Any identifying information has been redacted. Age ranges are reported to protect participant privacy. Locations are only specified if the population is larger than 100,000.

3.5 Country-specific details

3.5.1 India (n=103)

In India, our 103 female participants included college students, housewives, domestic maids, village farm workers, IT professionals, bankers, small business owners, teachers, and two women with physical and visual disabilities (banker and microenterprise owner). Focus groups were conducted in Chennai and Bangalore (south India); and Delhi, Kanpur, and villages in the state of Uttar Pradesh (north India).

Focus groups were conducted in rented conference rooms, community centers, cafes and restaurants, universities, and quiet public spaces like communal seating areas. The first author conducted each interview in Hindi, Tamil, and English, depending on the participants' language preference. Recordings were transcribed into English by the research team. Each participant received $10-15 USD for participation, depending on urban versus rural locations.

3.5.2 Pakistan (n=52)

In Pakistan, our 52 female participants included working women, housewives, and students. Occupations of working women included gym trainers, janitors, beauticians, school teachers, security personnel, corporate employees, university instructors, and home tutors. Focus groups were conducted in Lahore, Multan, and Rawalpindi (central Pakistan); Peshawar (northwest Pakistan, bordering Afghanistan); Karachi (south Pakistan); and Hunza (north east Pakistan, bordering India). We chose places like community centers, schools and facilitators' homes for conducting the focus groups according to the comfort levels of participants.

Participants were recruited with the help of local facilitators. We visited Muslim, Christian and Ismailee communities with facilitators to recruit participants and to conduct the focus groups in their communities. Goody bags consisting of food items worth up to $5 USD were distributed among the participants who showed up for interviews. Cash incentives worth $50 USD were given to facilitators in each city. All focus groups were conducted in Urdu and responses were audio or video recorded after obtaining verbal consent from participants. Recordings were transcribed into English by the research team.

3.5.3 Bangladesh (n=44)

In Bangladesh, our 44 female participants included garment workers, housewives, teachers, medical doctors, engineers, and day laborers. Focus groups were conducted in Dhaka (central

Bangladesh), Chittagong (southeast Bangladesh, bordering India), and Sylhet (northeast Bangladesh, bordering India). Participants were recruited by contacting each group through a known contact, such as through members of the research team, university staff, and known professional and personal contacts, in order to gain the trust of participants.

Focus groups were conducted in Bengali, and recordings were later transcribed to English. Incentives of warm food along with monetary incentives of $12 USD, or the gift equivalent, were provided for each participant.

3.6 Gender in South Asia

We picked these three countries for the study since they share a great amount of cultural and economic similarities. The three countries used to be one unified country, India, before the British partitioned India into three free countries when they left in 1947: India, East Pakistan, and West Pakistan. In 1971, West Pakistan became Pakistan and East Pakistan became Bangladesh. In all three countries, women occupy a tenuous position between empowerment and disempowerment. All three countries have had female Prime Ministers, CEOs, and public intellectuals since independence. Yet, women face gender inequality in multiple areas, including health, education, and the economy, due to complex cultural beliefs and practices.

4. FINDINGS

An overarching theme in our results is that participants had to cope with an expectation that they allow their phones and accounts to be frequently monitored by a variety of social relations. In the first section below, we describe device sharing as a cultural expectation and how this led to mediated and monitored technology use for participants. Since participants were embedded in this cultural context where their technology use was monitored, they were generally accepting of it; we discuss these perceptions of privacy in the second section below. However, participants experienced situations when they wanted to avoid having others learn about their digital activities. In the third section below, we describe the practices they adopted to maintain some privacy when device sharing was expected.

4.1 Device sharing as a cultural expectation

In our study, cultural norms for women were one of the major factors that led to phone sharing (also seen in [3,44]). Participants experienced a cultural expectation that they, as women, would share their devices with social relations. In practice, this could involve multiple onlookers as they used their device, having their device passed between multiple people, or using a device that was primarily shared in nature. Since women are typically viewed as the caregivers, participants often reported that their children used their phones to play games or watch videos. Note that this cultural expectation of sharing did not end with phones; participants were also expected to share personal belongings like jewelry, savings, and *saris* (clothing) with other family members.

Other factors also motivated device sharing. While access to a phone was not a barrier in our study (phone ownership was a criterion for participation), the high cost of mobile data sometimes led to shared use. In most of the cases, sharing was reported to be a voluntary act, including in some cases where it may have been considered (by the participant) a man's or elder's right to monitor the woman's devices. Regardless of the perception of sharing among our participants, all of them created practices to maintain a sense of privacy.

Below, we highlight various contexts in which our participants' device use was shared, mediated and monitored.

4.1.1 Shared usage (IN (India): 83; PK (Pakistan): 31; BG (Bangladesh): 11)

Many participants reported sharing mobile phones in the household (83 out of 103 participants in India, 31 out of 52 in Pakistan, and 11 out of 44 in Bangladesh stated experiencing this theme). In Peshawar and Hunza in Pakistan, some participants noted that they were not able to own their own phones until they were married (they did own at the time of the interview). When women had mobile phones, their devices were often viewed as 'family' devices. Several mothers in our study reported that their phone became the default shared phone of the family. A mother's loss of identity in possessions and space has been well documented, *e.g.*, [26,45]; however, this generally gendered issue takes on a specific locational nature in South Asia, discussed here around mobile phones. Some women in Bangladesh reported that their children would immediately grab their phone when the women returned home from work but left the father alone or asked to use his phone much less. As Shaina, (a 20 to 25-year-old young mother of two from Chittagong, Bangladesh) noted:

"*My kids don't touch the father's phone. They only use mine all the time. They are scared of him....my daughter broke my husband's phone and got a lot of beatings. She only uses mine. So I have an app lock on my phone.*"

4.1.2 Mediated usage (IN: 33; PK: 20; BG: 4)

Mediated usage refers to one person setting up or enabling a digital experience for a less tech-savvy user (*e.g.*, a daughter might search for and play a video for her mother). Some participants from all three countries described that it was common for a man in the family to load content that she desired.

As documented elsewhere, mediated usage builds upon the social infrastructure and enables women, especially those with lower technical literacy, to make use of tools they find challenging to use [40].

While some men enabled female relatives to access technology, this practice was also restrictive in that it required women to rely on others for access. As Zeenat (a small business owner, 30 to 35-year old in Lahore, Pakistan) described, she depended on her husband each time she logged in to social media:

"My husband created my Facebook account and he didn't enter my complete information. Because I didn't know how to create a profile, I asked him to create it for me. Now every time I want to use it, he logs in for me."

4.1.3 Monitoring (IN: 43; PK: 17; BG: 2)

Monitoring refers to situations in which someone other than the primary user examines the phone, without otherwise having a need to use the phone. Among the 62 participants who experienced monitoring, their reactions to it were mixed. Roughly half of these participants viewed it as being acceptable for men, elders and in-laws to monitor their devices, and they did not usually reciprocate

by examining the device of the person doing the monitoring (although, in a few cases, participants reported checking on their husband's devices secretly). Some of these participants reported that they appreciated when male members checked their phones to ward off unwanted calls and attention on social media, or to check for viruses, as these participants perceived that their technological skills were lower than those of the person monitoring.

Being open to monitoring was performative, in that in enabled participants to show and feel they fit the role of a good family member. As Sujata (a 20 to 25-year old receptionist in New Delhi, India) noted, enabling her parents to check her device fit with upholding the image of being a 'good daughter.'

"My parents can pick up my phone and check whenever they want because they have the right to. They give us freedom all the time. We have nothing to hide from them."

In another case in old Dhaka, Bangladesh, Nilima (a 50 to 55-year old school teacher) told us how her husband had the right to check her messages, and she felt that it was acceptable.

In some cases, monitoring was viewed as coercive. In Bangladesh, two (out of 5 whose husbands worked abroad) participants reported that their husbands installed tracking tools on their phones to monitor their phone activities. Aysha (a 25 to 30-year old domestic worker) reported feeling upset when her husband first mentioned putting spyware on her phone (it is unclear if he actually did so), but she has now found ways to deal with the monitoring. She explained,

"When I call my mother or make personal calls, I borrow my employer's phone."

Small spaces and multi-generational households also led to over-the-shoulder looking. Participants reported that content was accidentally viewed by family members around the home, especially large content, visual content, and the applications women used.

4.2 Participants' notions of privacy

In this section, we describe what 'privacy' meant to our participants. At the outset, it should be noted that the term 'privacy' carried a variety of connotations and implications for the women we interviewed. Across the three countries, it was often challenging to discuss privacy. The term itself was sometimes considered objectionable, particularly among the participants with lower and middle SES backgrounds. Many participants described that 'privacy' was for upper class families, where boundaries in personal and social settings were acceptable, but it was not a part of their cultural ethos that emphasized openness.

'Privacy' was often viewed as a Western concept, imported along with cultural goods like *"jeans and dating,"* as Bhanu (a 30 to 35-year old housewife from Delhi, India) described. A direct analogy offered by Raahat (a 25 to 30-year old office clerk in Dhaka, Bangladesh) was that of *"closing doors...we don't allow it in our family unless there is a special situation. Privacy is like that, it is against our values."* To contextualize the analogy, in some socio-economic segments, the idea of closing a door is considered unacceptable or even unheard of, especially among lower-income families that inhabit one-room homes.

Conversely, the more educated and wealthier participants did not associate a stigma with the term 'privacy', which prior work attributes to their education in liberalized institutions and association of higher social classes with westernized values of individuality [5].

In contrast to the verbal dissociation of the concept of privacy, *all* participants in our study—no matter their SES background—employed strategies and techniques that the usable security and privacy community would likely call safeguarding and controlling their 'privacy' on their devices. While many of the lower to middle SES participants did not think of these practices as privacy-related, the practices were intentional steps taken to protect device activities and content from being revealed to co-located household members. The higher SES participants did associate these practices with the concept of privacy.

4.3 Privacy practices in device sharing

Despite the wide range of views on what 'privacy' meant and how applicable it was to them; our participants used an assortment of practices to keep others from learning about some of their digital activities. In the cultural contexts of our study, the outright refusal for a woman to hand over her phone to men or elders was considered disrespectful or impolite. Thus, our participants used several privacy practices—phone and app locks, content deletion, private modes, and technology avoidance—to maintain individual privacy (see Figure 1 for a summary). These privacy practices were *dynamic* and *situated* in the social setting, in that they varied according to the social relationship, space, and device activity. They were also *performative* in that they enabled participants to uphold the impression of openness that was culturally expected of them, while maintaining some privacy. The level of sophistication of the privacy practices varied based on the participants' familiarity with technology.

4.3.1 Phone locks (IN: 83; PK: 27; BG: 6)

Participants regularly locked their phones with pins or patterns to prevent misuse by strangers or in cases of theft. Such *phone locks* can be an effective strategy in many contexts [11,18]; however, they were almost never effective in preventing proximate family members or friends from accessing the mobile phone. Many participants reported living in small spaces and maintaining open social environments, such as spending time in the living room and not necessarily having one's own room, which led to over-the-shoulder device onlooking. As Jyoti, a 40 to 45-year old housewife in Kanpur, India noted,

"Since I want to prevent my kids from using my phone, I use phone locks. But my kids open it each time I change it. They are too smart. I have to change my app lock pin every week. I have done it so many times that I often forget my pin."

Phone locks were most effective in providing peace of mind in theft and unmonitored scenarios. As Yasmin, a 30 to 35-year old garments worker in Dhaka, Bangladesh described, phone locks brought comfort when strangers may have accidental access to the phone.

"I am extra careful about phones as it is confidential. My phone was misplaced once and I panicked. Later when it was returned I remembered that it had a phone lock."

4.3.2 App locks (IN: 43; PK: 9; BG: 6)

Following phone locks, the second most commonly used strategy reported by our participants was that of *app locks*. App locks, such

as Do Mobile app lock, Security Master, and Cheetah Mobile, provide users with the ability to password- or pin-protect specific applications, content, or folders. In comparison to the largely ineffective strategy (as reported by participants) of using phone locks in co-located groups of families or friends, app locks were reported to provide more control to participants, although not always.

App locks provided privacy protection to participants who shared their phones but wanted to maintain privacy over certain applications or folders. In many cases, app locks were enabled after a privacy violation had occurred among co-located others. Sanaa (an 18 to 25-year-old beautician in Lahore, Pakistan) noted how she had to turn over her phone to her employer during work hours per work rules. In her case, a prior incident of monitoring by the receptionist staff motivated her to install an app lock.

"My friend introduced me to app lock. As I work in a beauty salon. I have to submit my phone to the receptionist when I go to work. Other staff also do this. I found out that some of my messages were read by someone when I submitted my phone to the receptionist. I told my friend about this, and she said that the receptionist did this to her too when we were not looking, and she asked me to install app lock. Now I feel secure. Anyone can borrow my phone for calling."

As Sanaa notes above, app locks allow users to share their devices, instead of blanket refusal, by providing granular control over specific apps or content. Most of our participants hid social media applications, photo and video folders created by social applications, and Gallery (a photo editor and storage folder). A few participants reported hiding other applications like menstrual period trackers, banking applications, and adult content folders. As Gulbagh (a 20 to 25-year old college student from Multan, Pakistan) described:

"I have enabled app locks in addition to the phone lock. I have it on WhatsApp, Messenger, and Gallery because sometimes friends share some pictures and videos with you that are only meant for you [smile]. My brother is never interested in my phone but it is my younger sister who is a threat [laughs]. So I have an extra shield of protection."

App locks also prevented friends or children from accessing data-intensive applications. In a context where the cost of mobile data is relatively high as a proportion of monthly expenses, many moms in our study reported locking apps (*e.g.*, video apps) to prevent children from spending too much mobile data. Another common concern was that children would accidentally delete an application. However, app lock passwords were sometimes easily known to co-located household members, similar to phone locks.

"Both my elder daughters use my phone. I have enabled an app lock on my phone but my kids learn the lock pin easily. Even if I change, they learn it."

The design of most app locks enables privacy, without consideration for secrecy. Five participants mentioned that the visible app lock password or PIN screens when invoking certain applications, or the very presence of the application on the phone led to questions such as, "what are you hiding?" Some app lock applications were reported to enable invisibility, but that often costs extra. As noted in [36,38], there is a general reluctance among technology users in many emerging markets to pay for online applications, services, or content due to freely available pirated content and lower affordability.

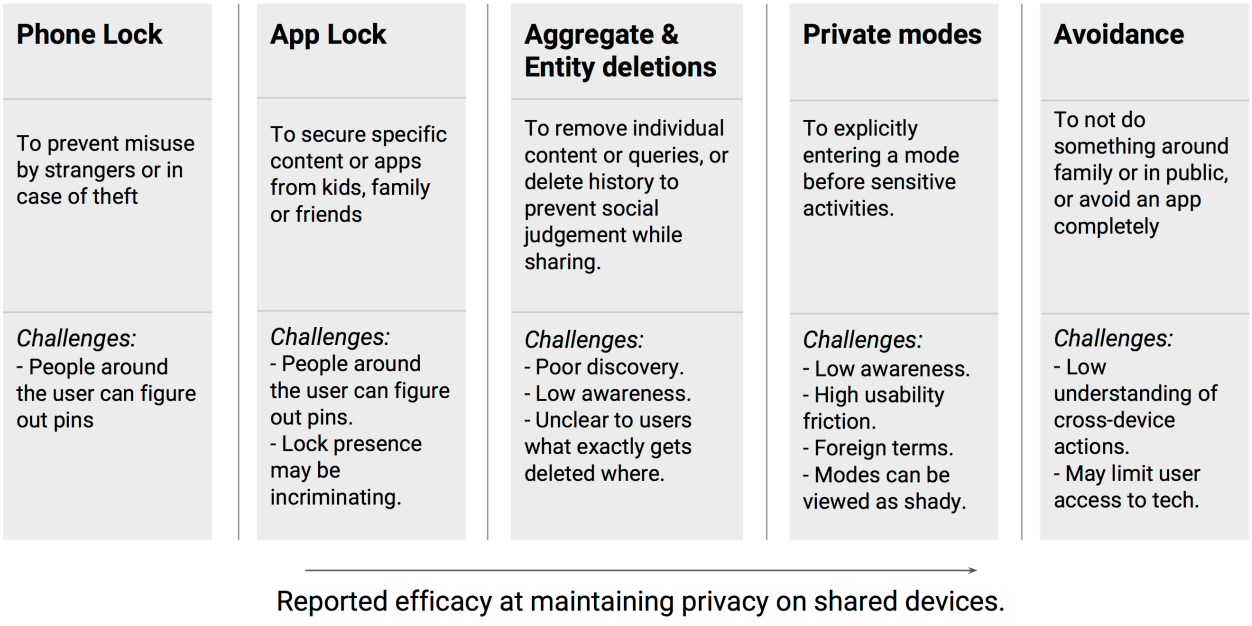


Figure 1: Reported efficacy by participants in achieving their privacy goals on shared phones

As Rupa, 30 to 35 years old, from Chennai, India, explains,

"If you hold a button on Vault, you can see a screen where it allows you to hide the app lock. But you have to pay to use it. I heard there is another app where if you press a button five times it becomes visible."

To summarize, app locks were popular among our participants since they enabled a degree of privacy among co-located others. However, two challenges were (1) that passwords and PINs were often discovered by others in close proximity, and (2) if others found the app lock, that might suggest the participant was trying to hide something which could lead to tensions.

4.3.3 Aggregate and entity deletions

Phone locks and app locks were used by our participants to prevent others—acquaintances, strangers, and children—from accessing personal applications and content. Participants deleted information in situations where devices traveled freely across various users. While locks make visible the refusal to share certain applications, information deletion was used to remove sensitive content without a detectable trace. Two types of practices were observed in content deletion: (1) *aggregate deletions*, where participants deleted entire threads or histories of content, and (2) *entity deletions*, where participants deleted specific chats, media, or queries. However, many participants were not aware of these aggregate and entity deletion controls, so they often resorted to avoiding applications entirely.

4.3.3.1 Aggregate deletions (IN: 17; PK: 5; BG: 9)

Participants reported using aggregate deletions when (1) they were not able to find a mechanism to delete a specific piece of content, or (2) they wanted a large amount of their content deleted, for example browsing history, search history, or message history. Confusion appeared when participants reported wanting to delete specific content, but ended up deleting all content history, because they were not able to discover the affordances to delete specific content. In a few cases, search history was also deleted because participants perceived that it would speed up phone performance (most participants owned low-end mobile phones in the $50-$100 range). Janaki, (a 35 to 40-year-old clerk in Chennai, India), explained:

"See when I search for something, it shows what else I have searched before. Sometimes it can be a little cheap for other people to see. I like to see medical videos on ladies' topics or 'those' type of videos. But others will get doubts on my character. When my son uses my phone, he will think why is amma [mother] *seeing all this. So I just clear my search history every week to be safe."*

Among more technologically aware participants, concerns over cross-platform privacy leaks and complex strategies emerged. Chitra (a 20 to 25-year old engineering student in Bangalore, India) recounted how she deleted her search history on occasion. Recently, she had searched and shopped online for gifts for her boyfriend. Chitra was wary of ads popping up on other platforms and awkward questions from her relations, like "who are you buying a men's t-shirt for?". So she deleted her search history. Chitra's friend and classmate, Chrissie, had sophisticated practices to negotiate device privacy using pause-and-resume functionality. She noted:

"I like to watch Game of Thrones. When I see clips or highlights, I first pause my viewing history and resume after I have finished watching the clip. If I am too worried, I just delete the entire history. But sometimes I forget."

To summarize, aggregate deletions were commonly employed to achieve peace-of-mind regarding the privacy of all browsing, searching, and viewing habits. A common assumption made by our participants was that deleting history would delete all records on that original platform and other platforms that communicate with it. However, this may not be true in most cases, where deleting history may not delete personalized recommendations already trained on the user's habits and does not delete browser cookies and data exchanges to other cross-linked platforms. Private modes, discussed below, may have been more helpful to participants in accomplishing their goals.

4.3.3.2 Entity deletions (IN: 89; PK: 29; BG: 9)

Entity deletions were used to remove individual items or actions—such as texts, photos, previously searched terms, etc. While aggregate deletions were more commonly used by participants for web content and specific applications like video and shopping platforms, social media content was predominantly managed through entity deletions.

The prevailing use case for entity deletions was to remove sent and received media and messages, to control what others who used or monitored their phones would see. Photos, videos, and texts were deleted from chats and folders. Maheen, (a 20 to 25-year old housewife from Lahore, Pakistan) described her rationale for deleting specific photos and videos.

"When I open [social media] chat, sometimes my friends send inappropriate videos. Sometimes they send boyfriend photos. Then that will lead to questions from elders like 'where did you go? Who have you been with? Who is that man?' So it is better to delete the chats and avoid misunderstanding."

Families often needed to manage their content histories when sharing with children. Sahana, (a 40 to 45-year old accountant in Delhi, India) described:

"Actually, I don't have any lock on my phone since my son uses my phone. I would never want my son to watch anything that is inappropriate. Sometimes, I receive videos from friends that are vulgar for children, then I immediately delete such videos."

Entity deletion was not isolated to situations where individual integrity or ethics came into question. With the constant possibility of someone examining a phone, entity deletions offered great freedom and agency. Bushra, (a 40 to 45-year old bank employee from Peshawar, Pakistan) explained,

"I have some glamorous photos of myself on my phone. Sometimes I wear a sleeveless top and take photos. If God forbid someone checks my phone then what will happen? So as soon as I take pictures, I save them in my PC and delete from my phone. I don't rely on my phone."

Entity deletions in personalized systems were particularly challenging for our participants to discover and manage, even though they typically are available. Entity deletions in personalized systems were typically invoked through prolonged presses or hidden behind settings that required multiple clicks to find, limiting reach and value to those less familiar with technology. Take, for

example, Shaina (a 35 to 40-year old medical representative in Kanpur, India) who manages how her application's personalized home page looked to co-located others with indirect techniques. She described:

"When I watch a video that is little bit not nice, then I search for 5-6 other videos on different topics to remove it."

Shaina understood that the algorithm learned from prior history and presented personalized recommendations but was not aware of how to signal to the system to remove or dismiss recommendations through the user interface.

For one participant, the inability to control specific content presented by platforms in a public context led to unfortunate circumstances. Nafisa (a 40 to 45-year old faculty member in Dhaka, Bangladesh) recounted how she liked to show video tutorials to engage students, who in turn listened with rapt attention to her lectures. In one such class, when Nafisa opened videos for a lecture, unexpected content was displayed, which led to ridicule and laughter from the students. Not knowing how to immediately dismiss or hide it, Nafisa felt confused, left the class crying, and took the day off work. Better feedback mechanisms over content platforms and user education may positively impact such unexpected loss-of-control situations.

4.3.4 Private modes (IN: 8; PK: 0; BG: 3)

Use of *private modes*, such as private browsing, were restricted to the (1) technology-savvy and (2) censorship-conscious participants. Participants explicitly chose to use private modes for privacy. As Mary (an 18 to 25-year old engineering college student in Bangalore) described:

"I use hidden mode a few times, like when reading the 50 shades of Grey e-book on my phone…."

A majority of our total participants were not aware of what the private modes in their web browsers did or where to find them. One issue was that terms used to refer to private modes were hard to understand among our participants. (Note that in India, only 10% of the population speaks English[11]). Even when advertised, private modes are often associated with 'secret' activities, threatening participants' values of openness as they performed culturally appropriate gender roles. These design issues might help explain why only 11 out of 199 participants used private modes, despite their potential usefulness. When explained as 'a button you press to temporarily browse anything you like, without affecting your recommendations or history,' participants positively appreciated the concept. Our participants foresaw the need for a private mode for a broad spectrum of informational activities, such as medical and sexuality searches, planning activities like birthday surprises, and content activities like watching adult content or intimate chats.

4.3.5 Avoidance (IN: 43; PK: 33; BG: 6)

Certain applications were *avoided* on the phone to prevent questioning or incrimination by co-located household members. For example, 24 participants described that they had a bank account hidden from their husbands, built up over time from small monthly budget remains and salary leftovers. Many participants avoided installing a banking app on their devices, due to low trust in their ability to control the app's visibility[2].

As another example, certain types of digital content or applications were entirely avoided in households with children, like watching gynecological videos, for fear that they would eventually figure out the app lock passwords or pins. As a third example, participants preferred in-person meetings or phone calls for sensitive communications (*e.g.*, about spousal issues or abortion advice), to prevent others from later seeing the conversation (*e.g.*, in chat history), similar to Tibetans in [7]. As Lathika (a 45 to 50-years old, banking professional in Bangalore) noted,

"We just call and talk to each other. Everyone in the [social media] *group knows that the phone is in the midst of the family. So we don't send anything to each other awkward or secretive at any time of the day."*

Exits were a specific type of avoidance described by participants, in which they suddenly closed an application due to contextual sensitivities (*i.e.*, who was around). Participants reported some vivid exits from apps when they unexpectedly saw embarrassing or sensitive content and wanted to avoid social judgment. In one case, Asma (a 40 to 45-year old housewife from Lahore, Pakistan) described that she threw the phone battery out when an inappropriate ad was presented to her, to ensure no one else could see the content or question her morals (she later reassembled it). Sonia (an 18 to 25-year old arts student in Chennai, India) described how she exited an app by locking the screen and closing the app privately later:

"Quite often I am watching something on Internet and suddenly a porn ad or video pops up. I immediately lock my screen in that case and look around if anybody has seen this or not. I then open it again when nobody is around, view it and then delete or close it. My brother and parents would definitely not like the idea of me watching porn."

Such exits do not remove the recorded history of content presented, even though some participants believed they did.

5. DISCUSSION

We summarize key results and discuss design suggestions, open questions, and privacy challenges for technologists to consider for our participants, and which might be relevant in other contexts where device sharing is common and expected.

---

[1] English or Hinglish, BBC, 27 Nov 2012. http://www.bbc.com/news/magazine-20500312

[2] In the case of India, demonetization in 2017 led to devaluation of 86% of the high-value currency overnight. Six participants were distrustful of installing banking applications, worried about the loss of hard-earned money, both from government decisions like demonetization and from their husbands discovering their balance. Women were among the most affected by the initiative, since they often had cash bills saved for personal and family expenses that was hidden from men in the family (participants reported that men may squander the money if discovered, sometimes for drinking), which was de-valued [54].

5.1 When device sharing is cultural

Our participants experienced culturally-shaped autonomy in their daily lives, which led to specific performative practices around device privacy. While smartphones are often designed to offer individual user experiences, close social relations are often a part of this assumed personal space. Whether it was husbands, fathers, brothers, bosses, colleagues, children, or in-laws demanding access, women often socially cherished or were expected to share access to their devices. Since device sharing is a cultural expectation and value in this region, we expect this phenomenon to continue even as the number of devices increases in the region (indeed, device sharing in India has been documented in HCI and ICTD research from 2009-10 [40,44], when phone penetration was 36% of the population [40].)

While it might be tempting to conclude that the lack of autonomy is problematic when viewing our results from outside the cultural context, our participants had a range of views regarding their limited privacy. Some felt it was acceptable or even welcome for their husbands and brothers to monitor their phones. This occurred when they felt technologically challenged or wanted protection from untoward admirers on social media (see similar views in [17]). Some others felt that they were non-consensually being monitored.

While there were divergent views on how relevant the concept of 'privacy' was to them, all participants developed privacy-related practices. Some practices were more effective in achieving their goals than others, and their sophistication varied based on their technology literacy. The five types of privacy practices they employed —1) *phone locks*, 2) *app locks*, 3) *aggregate and entity deletions*, 4) *private modes*, and 5) *avoidance*—helped them maintain privacy while adhering to the cultural expectation that they should share their mobile phones with their social relations.

Aggregate and *entity deletions* were often perceived as being useful. Participants believed that deletion, if used when no one was looking, enabled them to remove content without anyone else knowing it had been on the phone. Thus, it enabled them to perform openness (a cultural value for many South Asian women) while keeping select information private. This was unlike *phone* or *app locks*, which signaled to borrowers and co-located social relations that something suspicious might be hidden behind the authentication screen. (Note that we were not able to determine if participants had achieved their goal of deleting the content to the point of it being truly undetectable.)

However, having alternatives to deletion were valuable, since deletion was not the best way to achieve all of their goals. Participants had content they wanted to preserve and access on their phones. Moreover, aggregate and entity deletion controls were not always fully discovered by participants with lower technical literacy. In the future, we anticipate that the growing presence of cross-device, cloud-based interactions could pose new challenges for users seeking to understand the impact of content deletions performed on a device.

Phone and *app locks* were used, but participants did not always consider them to be appropriate in intimate settings. The affordances of app locks sometimes led to tensions with social relations, such as "what are you hiding" questions. Phone and app locks were viewed as effective against strangers who might use one's phone temporarily or in the event of a lost or stolen device. App locks also seemed reasonable for keeping nosy colleagues and acquaintances from snooping, and children from accidentally deleting an app or using too much data (provided that they don't learn the app's pin).

We offer the following considerations to help technologists make design choices that empower users who commonly experience device sharing, mediated usage, or monitoring.

5.2 Supporting privacy

5.2.1 Awareness and education

Our research highlights the rich variance in our participants' mental models and adaptations of device and app privacy controls. As Wash writes in his description of security folks models, *"whether the folk models are correct or not, technology should be designed to work well with the folk models actually employed by users"* [50]. Participants in our study would benefit from a better match between their mental models and the functioning of several technologies they use, especially personalized systems and private modes. Results from our study provide a basis for improving awareness and understanding of these features among South Asian women.

Our research also points to an opportunity to improve user education around available privacy features. For example, participants liked the idea of private modes, yet such modes were rarely discovered or used. Promoting such modes in a culturally appealing way could help more users benefit from them.

5.2.2 Content trail management

Most women we spoke to indicated that the ability to delete content (*e.g.*, downloaded images) and behavioral traces (*e.g.*, browsing history) was the most commonly used, powerful, and effective tool for managing their privacy. Participants described how deleting traces offered peace of mind to browse desired content, while avoiding awkward explanations to social relations. However, deletion was often hard for our participants to understand; for example, some did not realize deletion was a two-step process that required emptying the trash (a finding also reported in research on the technology experiences of survivors of intimate partner abuse [30]). Design explorations aimed to improve the discovery of deletion affordances could be valuable, especially for less tech-savvy users. We found that visual affordances for deletions (such as 'X's') worked best with our participants, since some of them had lower literacy. Technologists may consider increasing the power of tools by ensuring they provide both aggregate and entity removal for all user data (see also [30]).

Technologists should also consider the fact that many new technology users may not be aware of the concept of the cloud or that browsing actions are not just one-time actions, but train personalization models that may present recommendations in the future. Software design should consider communicating to users how cloud backups can be pushed as recommendations to users, so they do not implicate them in situations of device sharing.

Lastly, there are interesting future work directions to explore in offering the ability to transfer content from one device to another, which can help users like our participants maintain privacy on their primary device while storing content on a secondary device. It should be noted that many mobile South Asian users are familiar with downloading, storing and transferring media content between devices and memory cards, and much more comfortable with offline media than cloud-based media (offline media are often used for content consumption in low-bandwidth environments, see

[35,42]). Migration and deletion tools could consider the user's desire to keep content backed up in a safe and private place.

5.2.3 Account switching opportunities

For South Asian women, the one-device, one-user model breaks down, encouraging technologists to challenge the assumption that a single application should have a single account (also noted by [20,29] for users in other regions). Yet none of our participants had multiple user profiles on the phone, possibly due to added friction or poor discovery. Specifically, participants in our study (and in prior work [23,29]) noted that account switching in applications is laborious and time-consuming, deterring them from using this functionality unless absolutely necessary. Also, some of our participants had low literacy and most were accessing apps primarily on mobile devices, making easy account switching harder to use. These challenges are promising areas for future work. While account and profile switching can provide private spaces, they present a fairly heavy cognitive task to users. Automation holds promise for more accurate personalization and recommendations in shared use. Machine learning models to classify and differentiate multiple user activities and invoke different experiences may reduce the cognitive load on the user's part to switch accounts or profiles. On a cautionary note, automated learning should take care to avoid misprediction, in order to avoid accidental disclosure to unintended recipients.

5.2.4 Private mode opportunities

Future work may explore the idea of providing private modes within applications or at the device level, to prevent history being left behind. Private modes could ease deletion-related confusion. As an example in India, Hike Messenger, a popular social media application, allows a private mode to hide specific chats that a user wants to keep private (based on their research that Indian young adults live with parents and want to maintain privacy).[23] To improve discovery, private modes may be shown prominently where the feature is more likely to be used, such as in apps that display culturally-taboo content. Alternatively, a single device-level private mode could simplify the experience.

5.2.5 Content hiding opportunities

While a powerful way for our participants to maintain privacy was to delete content or traces (or access content from a private mode), it was often important for participants to keep content on their devices, such as motivational videos, medical documents or emotional messages. In order to support this need, technologists may consider ways to hide content within the user's device ecosystem (content hiding has also been reported to be useful to other sensitive populations [30]).

App locks allow users to protect the content, but increase the risk of incrimination, since locked apps were often viewed as obviously private. Moreover, our study points to how app locks are not reliable in preventing access by people with power over a user (*e.g.*, elders, spouses, and in-laws). They can be useful in preventing children from accessing content, but children are often quick to figure out passwords and pins, which can leave users with no choice but to keep changing passwords (which increases cognitive load).

Regardless of the method used to hide content, a visible indication of hidden content (*e.g.*, a visual lock icon) may cause more harm than good—at least for this population. Users hiding content are often aware of how their behavior could be perceived as incriminating, leading to reduced usage of the feature. We suggest that designs for hiding content carefully consider the value of making it obvious that content is hidden. Additionally, it is important to consider making such valuable invisibility features available free-of-charge.

5.2.6 Algorithm-related opportunities

While many users have become accustomed to personalized content experiences based on prior activities, many are not aware of how to control them. We recommend that technologies employing algorithms provide or continue to provide clear, easy-to-find settings for novice users to control personalized recommendations. Additionally, improving opportunities for females (and other under-represented groups) to provide algorithmic feedback may be useful in making machine learning datasets more inclusive (as the Internet has disproportionately more male users than female users in many South Asian contexts [17]).

We encourage technology designers to consider the social dynamics and implications discussed above for women in South Asia, which could alter gender power imbalances in unexpected and positively transformative ways.

5.3 Culturally appropriate text

Care should be taken to evaluate privacy controls across various cultural contexts of deployment. Technology is often designed with normative assumptions based on Western cultural values suggesting that online privacy and safety is a right. In contrast, some participants did not identify as having "privacy needs", saying *"Privacy is not for me, it's for those rich women,"* or that 'privacy' was a Western value, even if privacy-related practices were prevalent. This perspective should be considered when writing the actual text that is used to discuss privacy and safety experiences in apps and devices that will be used by women in South Asia. For example, invitations to modify privacy settings may be well intended, but may not seem as inviting to women in South Asia. We suggest that the technology community explore how to adequately explain the use cases and value of privacy-related features to audiences around the world, using terminology that is appropriate to them.

6. LIMITATIONS

This paper presents findings from a study we conducted on how women in South Asia who come from a range of occupations and socioeconomic backgrounds perceive, manage and control their individual privacy on shared mobile devices. Future research studies may examine other populations, such as teenagers, families or women in other parts of the world.

[3] In India, an App for Chats and for Keeping Secrets. New York Times. Aug 2014. https://www.nytimes.com/2014/08/26/world/asia/in-india-an-app-for-chats-and-for-keeping-secrets.html

Our approach was qualitative, hence inductive in nature. Common limitations with qualitative studies include recall bias, observer bias, participants self-censoring on sensitive topics, and limitations in the generalizability of results. We are currently deploying a large-scale survey to measure privacy attitudes in South Asia. Another limitation is the triad focus group format, which may have limited participants from opening up on certain topics in the presence of others.

A possible limitation is the cross-comparisons of countries undertaken in this paper. While we are not aware of any other research studies that focus on all the three countries sampled in this study, our claims are comparative and are likely to miss city- or country-specific nuances or depth.

7. CONCLUSION

We presented a qualitative study of how 199 female participants from India, Pakistan, and Bangladesh perceived, managed and controlled their individual privacy when social relations frequently borrowed and monitored their mobile phones. We examined the ways their social expectations were fulfilled through technological and social affordances. We described how participants used five types of practices to maintain their privacy while navigating cultural expectations to share their phones: 1) *phone locks*, 2) *app locks*, 3) *aggregate and entity deletions*, 4) *private modes*, and 5) *avoidance*. We also discussed some suggestions, open questions, and privacy challenges for technologists to consider when designing for contexts where device sharing might be common. We hope that by sharing our participants' experiences and proposing several opportunities for future work, that technologists have new insight regarding how to make privacy more usable for women in South Asia. Such improvements could, in turn, help others, especially in contexts where device sharing occurs and usage is scrutinized.

8. ACKNOWLEDGMENTS

First and foremost, we thank our participants. We also thank Taylor Marable, Asif Baki, Lauren Johnson, Dave Shapiro, Aaron Stein, Ali Lange, Cary Bassin, Francesca Ginexi, Lawrence You, Michael Falgoust, Miguel Guevara, and Thomas Roessler. We thank our SOUPS reviewers for providing feedback on this paper.

9. REFERENCES

1. 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*, 672–683.
2. Syed Ishtiaque Ahmed, Nova Ahmed, Faheem Hussain, and Neha Kumar. 2016. Computing beyond gender-imposed limits. In *Proceedings of the Second Workshop on Computing within Limits*, 6.
3. Syed Ishtiaque Ahmed, MD Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *CSCW*.
4. Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *SOUPS*, 297–308.
5. Arjun Appadurai. 1996. *Modernity al large: cultural dimensions of globalization*. U of Minnesota Press.
6. Jakob E Bardram. 2005. The trouble with login: on usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing* 9, 6: 357–367.
7. AJ Bernheim Brush and Kori M Inkpen. 2007. Yours, mine and ours? Sharing and use of technology in domestic environments. In *UbiComp*, 109–126.
8. Lorrie Faith Cranor, Adam L Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and teens' perspectives on privacy in a technology-filled world. In *Proc. SOUPS*.
9. Kelly Derby, BETH EASTERLING, and others. 2012. Snooping in Romantic Relationships. *College Student Journal* 46, 2.
10. Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5: 413–421.
11. Serge Egelman, AJ Brush, and Kori M Inkpen. 2008. Family accounts: a new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, 669–678.
12. 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* (CCS '14), 750–761. https://doi.org/10.1145/2660267.2660273
13. Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders. *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW) Vol* 1.
14. Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 667.
15. Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 124.
16. GSMA. 2015. Bridging the gender gap: Mobile access and usage in low-and middle-income countries.
17. GSMA. 2018. *The Mobile Gender Gap Report 2018*.
18. 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 *Symposium on usable privacy and security (SOUPS)*, 213–230.
19. Eiji Hayashi, Oriana Riva, Karin Strauss, AJ Brush, and Stuart Schechter. 2012. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2.
20. Jeffrey James. 2011. Sharing mobile phones in developing countries: Implications for the digital divide. *Technological Forecasting and Social Change* 78, 4: 729–735.
21. Jeffrey James. 2016. Mobile phone use in Africa: Implications for inequality and the digital divide. In *The Impact of Mobile Phones on Poverty and Inequality in Developing Countries*. Springer, 89–93.

22. Kelby Johnson. 2003. Telecenters and the gender dimension: an examination of how engendered telecenters are diffused in Africa.
23. Amy K Karlson, AJ 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*, 1647–1650.
24. Neha Kumar. 2015. The gender-technology divide or perceptions of non-use? *First Monday* 20, 11.
25. Ann Light, Ilda Ladeira, Jahmeilah Roberson, N Bidwell, Nimmi Rangaswamy, Nithya Sambasivan, and Shikoh Gitau. 2010. Gender matters: Female perspectives in ICT4D research.
26. Karen Danna Lynch. 2005. Advertising motherhood: Image, ideology, and consumption. *Berkeley journal of sociology*: 32–57.
27. Market Research Society of India. 2011. The New SEC system. Retrieved from http://mruc.net/uploads/posts/b17695616c422ec8d9dadafc1c3eec26.pdf
28. Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.
29. 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*, 5921–5932.
30. Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2189–2201.
31. Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, and others. 2010. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 645–654.
32. Laura L Murphy and Alexandra E Priebe. 2011. "My co-wife can borrow my mobile phone!" Gendered Geographies of Cell Phone Usage and Significance for Rural Kenyans. *Gender, Technology and Development* 15, 1: 1–23.
33. Bonnie Nardi, Ravi Vatrapu, and Torkil Clemmensen. 2011. Comparative informatics. *interactions* 18, 2: 28–33.
34. David Nemer. 2016. "LAN Houses Are for Boys and Telecenters Are for Girls:" CTCs As Gendered Spaces. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (ICTD '16), 54:1–54:4. https://doi.org/10.1145/2909609.2909638
35. Jacki O'Neill, Kentaro Toyama, Jay Chen, Berthel Tate, and Aysha Siddique. 2016. The increasing sophistication of mobile media sharing in lower-middle-class Bangalore. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, 17.
36. Nimmi Rangaswamy and Nithya Sambasivan. 2011. Cutting Chai, Jugaad, and Here Pheri: towards UbiComp for a global community. *Personal and Ubiquitous Computing* 15, 6: 553–564.
37. Nimmi Rangaswamy and Supriya Singh. 2009. Personalizing the shared mobile phone. *Internationalization, design and global development*: 395–403.
38. Nithya Sambasivan and Paul M Aoki. 2017. Imagined Connectivities: Synthesized Conceptions of Public Wi-Fi in Urban India. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5917–5928.
39. Nithya Sambasivan, Garen Checkley, Nova Ahmed, and Amna Batool. 2017. Gender equity in technologies: considerations for design in the global south. *interactions* 25, 1: 58–61.
40. Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated technology use in developing communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2583–2592.
41. Stuart Schechter. 2013. The user is the enemy, and (s) he keeps reaching for that bright shiny power button. In *Workshop on Home Usable Privacy and Security (HUPS)*.
42. Thomas N Smyth, Satish Kumar, Indrani Medhi, and Kentaro Toyama. 2010. Where there's a will there's a way: mobile media sharing in urban india. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 753–762.
43. Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate partner violence, technology, and stalking. *Violence against women* 13, 8: 842–856.
44. 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: 231–250.
45. Julie Stephens and others. 2004. Beyond binaries in motherhood research. *Family matters*, 69: 88.
46. Sarah Revi Sterling, Leslie Dodson, and Hawra Al-Rabaan. 2014. The fog phone: water, women, and HCID. *interactions* 21, 6: 42–45.
47. Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh.
48. Divy Thakkar, Nithya Sambasivan, Purva Kulkarni, Pratap Kalenahalli Sudarshan, and Kentaro Toyama. 2018. The Unexpected Entry and Exodus of Women in Computing and HCI in India. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 352.
49. David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* 27, 2: 237–246.
50. Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 11.
51. Pamela Wisniewski. 2018. The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Security & Privacy* 16, 2: 86–90.
52. Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference*

on Computer Supported Cooperative Work and Social Computing, 51–69.
53. Delanie Woodlock. 2017. The abuse of technology in domestic violence and stalking. *Violence against women* 23, 5: 584–602.
54. 2016. What of the women who hide cash to feed their children or to escape abuse? *Scroll.in*. Retrieved from https://scroll.in/article/821255/note-demonetisation-what-of-the-women-who-hide-cash-to-feed-their-children-or-to-escape-abuse
55. *Census of India, 2011*. Retrieved from http://www.censusindia.gov.in/2011census/F-series/F-1.html
56. *Pakistan Bureau of Statistics*.
57. *Bangladesh Bureau of Statistics*. Retrieved from http://www.bbs.gov.bd/

10. APPENDIX

A. Interview script

Moderator instructions

Work on building a strong rapport, be personable.

Approach intimate topics with care. If the participant is uncomfortable, leave the topic. Offer some examples to help them open up from your own stories

When topics get sensitive, please use your judgement to ask other Googlers to leave. *e.g.*, ask them to check on something, buy batteries etc. so they can leave.

Find private and neutral spaces to chat.

After the core topics of the interview, please ask Googlers to leave so that you can talk about intimate topics freely.

Always ask for consent before the interview. Ask for permission before recording.

Interview script

Hi, thank you for coming here. My name is X and these are Y and Z. We are here from Google.

Today we are conducting research on what it means to be a Pakistani/Indian/Bangladeshi woman and use Internet, smart phones, apps. Everything you know and use daily. This is not an exam, everything you say is going to be helpful to us.

The purpose is to help us understand how to improve technology for women like you. We encourage you to be frank and open, so we can really learn how you are using phones and improve the experience overall. Some of the topics may be a little intimate or personal because we are talking about women. If you are uncomfortable, just let us know.

Everything we discuss today is confidential. Please do not discuss with your friends or family. Anything we discuss today can be used to improve or build new Google products and features.

Could I get your permission to record this interview (video, audio and photos)? It will be stored confidentially and be used for research purposes only. If you feel uncomfortable, just let us know. Any questions?

Grand tour

Intent: to understand their background, life situation, stresses, and context in which they live.
Could you introduce yourself? Name, profession, age.

Whom do you live with? What do they do?

What's a typical day like in your life?

What are your pastime activities?

What do you look forward to doing each day? What do you dislike doing everyday?

What do you wake up worrying about?

Device and Internet mapping

Intent: What is their device/internet technology landscape like, and why? Why did they choose some devices over others? What struggles do they have with technology and internet? What trade offs did they make and why? What is important to them and why?

I'd like to learn about your devices at home.

What devices do you access?

When did you buy your phone?

Why did you buy this model?

How were you able to finance it? / Who funds it?

When did you buy your first ever smartphone? Do you remember why?

What data and Internet plans do you have?

What do you do on your phone?

Access issues

Intent: how does being a woman affect their access to technology and information? Why? What are the barriers they face with getting access to a phone/Internet? What are barriers with using a phone/Internet?

Are there things you want to do with your phone that you are unable to do for any reason?

How much control do you feel you have over your phone?

How do you fund your data plan?

How about credit money (for Internet or calls), time allowed to spend on phone, time allowed to spend online, apps considered acceptable for women...how are these different from the men in your lives?

What apps do you have on your phone?

Which ones do you use the most?

Which ones do you use the least?

How often do you install new apps?

What motivates you to try out a new app?

Who makes the choice on which app to install, *e.g.,* you, husband, friend?

Device and account sharing

Intent: understand what extra technology demands are placed on women (vs men) and how they handle it. What privacy implications does this have, and how do women accomodate (or not) this?

In a given day or week, does your phone get shared with other people? Tell me more (who, why, how long, what access)

Do you borrow other devices in your family or from your friends?

Tell me how you deal with shared use.

Do you have any privacy considerations with leaving traces online?

Do you ever hide stuff from people around you on your phone or online, say parents, in-laws, husbands or children?

Have you ever tried to delete or remove some browsing history, search queries or recommendations so it does not show to anyone else?

Are there times when you wished you could erase what you have done? Or do stuff without leaving a trace? Tell me more (situations, how, when).

Do you use app locker? Tell me more (which app, which apps hidden, situations, instances)

Which apps do you lock? Why?

Do you ever see a need to view history of what you have browsed or done?

What aspects of identity are private and not to be relieved in a closed circle vs. open circle?

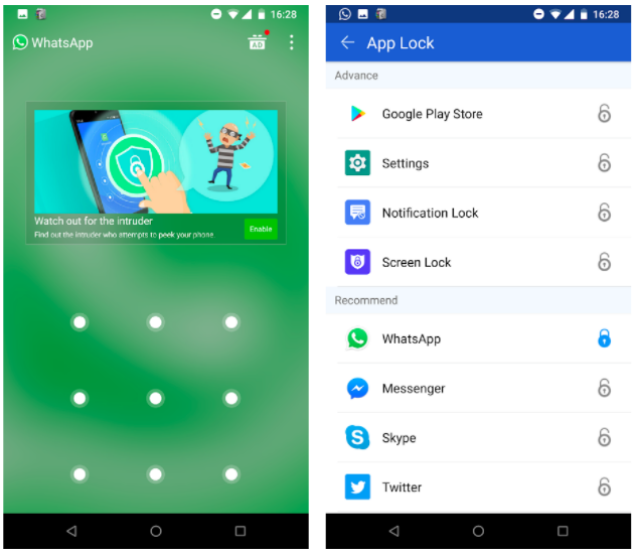
Conclusion

If we write a report based on this interview, what should we highlight?

That brings us to the end of this interview. Do you have any questions for us?

Thank you very much for your time and patience! We learned a lot from you!

Figure 2: Do Mobile's App Lock with over 100 million installs. (Left) Password screen when opening a protected app, (Right) Settings to invoke passwords on apps and folders.



B. Participant table

Table 1. Research sites and locations

Country	N	Locations	SES	Ages	Professions	Education	Tech access
India	103	Chennai (42) Bangalore (16) Kanpur (9) UP villages (15) Delhi (21)	Low (39) Mid (52) High (12)	18-25 (33) 26-35 (24) 36-45 (27) 46-55 (11) >56 (8)	Informal sector (24) Salaried (34) Business owner (6) IT/CS (9) Not employed (12) Student (12) Retired (6)	School dropout (7) High school (31) Undergraduate (45) Postgraduate (14) PhD. (6)	Mobile phone (103) Laptop (37) Tablet (17) PC (15)
Pakistan	52	Lahore (17) Peshawar (8) Karachi (6) Hunza (9) Multan (6) Rawalpindi (6)	Low (12) Mid (32) High (8)	15-20 (9) 20-25 (10) 25-30 (20) 30-35 (10) >40 (3)	Students (11) Not Employed (11) Self-Employed (3) IT/CS (1) Business owner (1)	School dropout (15) High school (7) Undergraduate (16) Postgraduate (13) PhD. (1)	Mobile phone (51) Laptop (30) PC (6)
Bangladesh	44	Dhaka (24) Sylhet (11) Chittagong (9)	Low (9) Mid (21) High (14)	18-25 (1) 26-35 (12) 36-45 (5) 46-55 (3) >56 (6)	Informal sector (6) Salaried (13) Business owner (1) Not employed (3) Student (18) Retired (3)	School dropout (9) High school (22) Undergraduate (6) PhD. (7)	Mobile (41) Laptop (24)

C. Codebook

Top-level category	Definition	Codes
Identity	Identity management of the user, including profiles, self-presentation and settings	Identity management Reputation management Family feedback loops
Co-located privacy	Considerations and management of privacy on shared, mediated or monitored devices	Family sharing Mediation Monitoring Views on privacy Phone locks App locks Micro deletions History deletions Private modes VPN Avoidance Subversion Sensitive content or activities
Access	Ability to use a technology at will, including time, location and social factors	Onboarding Motivations for access Pressures and concerns Money Time Mobility Social perception of access Online activities Fears Mitigation practices Myths of Internet
Online privacy	Considerations and management of privacy on apps, websites and services	Safety concerns Safety practices Information disclosure App-specific privacy models Privacy settings Privacy affordances Privacy violations