Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh

SYED ISHTIAQUE AHMED, Computer Science, University of Toronto, Canada
MD. ROMAEL HAQUE, Bangladesh University of Engineering and Technology, Bangladesh
JAY CHEN, Computer Science, NYU Abu Dhabi, UAE
NICOLA DELL, Information Science, the Jacobs Institute, Cornell Tech, USA

Prior research on technology use in the Global South suggests that people in marginalized communities frequently share a single device among multiple individuals. However, the data privacy challenges and tensions that arise when people share devices have not been studied in depth. This paper presents a qualitative study with 72 participants that analyzes how families in Bangladesh currently share mobile phones, their usage patterns, and the tensions and challenges that arise as individuals seek to protect the privacy of their personal data. We show how people share devices out of economic need, but also because sharing is a social and cultural practice that is deeply embedded in Bangladeshi society. We also discuss how prevalent power relationships affect sharing practices and reveal gender dynamics that impact the privacy of women's data. Finally, we highlight strategies that participants adopted to protect their private data from the people with whom they share devices. Taken together, our findings have broad implications that advance the CSCW community's understanding of digital privacy outside the Western world.

CCS Concepts: • **Security and privacy** → *Social aspects of security and privacy*;

Additional Key Words and Phrases: HCI4D; ICTD; Privacy; Access; Shared Use; Mobile Devices.

ACM Reference Format:
Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, 2, Article 17 (November 2017), 20 pages.
https://doi.org/10.1145/3134652

1 INTRODUCTION

The extraordinary growth in global smartphone access and availability is enabling people from previously neglected or marginalized communities living in the Global South to reap the benefits provided by computing technologies and the Internet. Within the CSCW community, a growing body of research shows how these diverse communities have appropriated and used digital technologies in a variety of new and innovative ways [25, 44, 48, 64, 69]. Moreover, researchers studying technology use in the Global South have observed a range of shared and collaborative uses of technologies that are markedly different from Western contexts. For example, the prevalent Western paradigm of 'personal computing' assumes a device will be used by a single person [11, 43, 62], which is not the case for collectivist cultures where shared device usage is common [7, 9, 16, 51, 55]. The social and

2573-0142/2017/11-ART17 $15.00
https://doi.org/10.1145/3134652

cultural practices that impact how people in the Global South share devices, and the data privacy challenges that result from shared use, are currently not well understood.

By contrast, digital privacy in Western contexts has been the topic of CSCW research for decades, with recent work focusing on privacy on social media [20, 27, 32, 41, 47, 66], mobile devices [71], and Internet access by specific groups of people [22, 37, 67, 68]. However, recent theories that conceptualize digital privacy argue that notions of privacy vary substantially across cultures, times, and places [23, 26, 50, 52], which suggests that privacy research conducted with populations in Western contexts cannot simply be applied as-is to communities in the Global South.

Our work fills this gap in the CSCW literature with a qualitative study conducted with families in Dhaka, Bangladesh that (1) develops a nuanced understanding of people's mobile phone sharing practices, and (2) analyzes the privacy challenges and tensions that arise when people share devices. Through data obtained from semi-structured interviews with 72 participants from 38 families, we show how people share devices out of economic need and also because sharing is a social and cultural practice that is deeply embedded in Bangladeshi society. Through a set of three vignettes, we highlight prevalent device sharing models—between spouses, between siblings, and between parents and children—and show how each of these results in complex privacy challenges.

We then delve into a diverse set of benefits and constraints that users encounter when they share devices, including how the practice of sharing enabled them to have access to a mobile device even when their own had run out of battery power or mobile airtime. However, despite the common social practice of sharing and its perceived benefits, many users would still prefer to *not* have to share their device with others, primarily because it compromises the privacy of their personal data. We describe how participants negotiate these tensions and discuss strategies that they use to try and protect their privacy, including commercial solutions such as locking software, and social solutions, such as blackmail, negotiation, or mutually agreed rules of sharing. Our analysis highlights the social and cultural factors that impact mobile device sharing. For example, we found that gender played a substantial role in several of the most prevalent sharing models, with men frequently possessing the power to violate women's digital privacy by inspecting their devices, although the reverse was not true.

We conclude the paper by discussing some of the broader implications of our work, including how Western notions of privacy that currently drive the design of most mobile devices may not effectively address the needs and usage patterns of populations in the Global South. We also consider how the power dynamics that came up in our analysis affect different individuals' rights to privacy, particularly women. Finally, we discuss our ideas for technical innovations that might better enable data privacy for individuals using shared devices. Taken together, our findings advance the community's understanding of digital privacy outside of the Western world.

2 RELATED WORK

Scholarly debates around privacy in the West have historically revolved around the ideas of 'liberal philosophy' [21, 56, 65]. At the core of this philosophy is the basic premise that individuals are the units from which values are produced [29, 65]. Over the years, scholars have debated the merits of such an individualist view, and the discourse around privacy rights has incorporated these and related political ideas surrounding issues of accessibility, inclusion, equity, and voice [15, 46, 70]. Although this liberal spirit is highly pervasive in the Western mindset, it is not universal outside the West. Hofstede's cultural scale [31] shows, for example, that people in the Indian subcontinent are more communal than the Euro-American regions. Thus, the idea that individualistic values are always at the center of privacy concerns is called into question [49, 51].

The study of privacy within computing systems has been the focus of decades of research. Initially, digital privacy and security were formulated as primarily mathematical and engineering problems

[58]. However, in recent years there has been a subtle shift away from purely engineering solutions toward more human-centered approaches [72]. This nascent field of "usable privacy and security" [24], which lies at the intersection of computer science, privacy and security, and HCI, is now a flourishing area of research. Numerous studies have been conducted that focus on improving the usability of specific security and privacy mechanisms, including: password construction [18], text password alternatives [18], behavior on social networks [28], recommendation systems [45], and mobile computing [54], among others. In addition to improving privacy mechanisms, researchers in the CSCW community have studied privacy in a diverse range of settings, including on social media [20, 27, 32, 41, 47, 66], mobile devices [71], or Internet access by specific groups of people (e.g., children, older adults, and disabled populations) [22, 37, 67, 68]. All of this prior CSCW work focuses on Western populations and has been dominated by Western notions of privacy.

However, theories that conceptualize digital privacy suggest that it varies substantially across cultures, times, and places. Patrick and Kenny [52] frame privacy from a human rights perspective and describe how interfaces should incorporate the features of comprehension, consciousness, control, and consent. Crabtree et al. [23] argue that family members are more concerned about managing their relationships than the secrecy of their information. Palen & Dourish describe privacy as a dynamic, dialectic process that is *"conditioned by our own expectations and experiences, and by those of others with whom we interact"* [26]. Nissenbaum's theory of privacy as *"contextual integrity"* [49] argues that what is construed as private information is contextual, temporal, and audience dependent. These models suggest that the results of privacy research conducted in the West cannot simply be applied as-is to non-Western contexts and highlight an important gap in the CSCW community's understanding of privacy in the Global South that our paper begins to fill.

Researchers studying the use of technology in the Global South have observed shared and collaborative uses of technologies that are markedly different from the individualistic uses prevalent in the West [7, 9, 16, 51, 55]. Many of these studies show how communities in the Global South frequently share devices among friends or family [8, 34], which contradicts the prevalent Western assumption of 'personal computing' that assumes a device will be used by a single person [11, 43, 62]. Consequently, issues arise when these users encounter features that are meant for a single individual—for example, contact lists, call histories, and browsing histories are designed to be tied to specific, individual users rather than groups. Moreover, on modern smartphones, users install and use applications that are tied to individual online identities (e.g., Facebook or Whatsapp), which can make sharing mobile devices even more problematic. Although technical mechanisms exist that allow devices to be used by multiple users (e.g., logging out, or using different accounts) [10, 60], these mechanisms are generally not well integrated into all applications and can be unwieldy. By focusing on access alone, many of these standard security mechanisms (e.g., screen locks) are not helpful when access to the device is allowed, but specific personal data should be kept private. These challenges emphasize the need for research that examines the prevalent local practices, usage and sharing patterns, and privacy concerns and priorities of communities in the Global South.

Outside of CSCW, a handful of projects consider privacy in the Global South [14]. For example, Kumaraguru et al. studied privacy-related issues with communication media among Indian populations [42]. Chen et al. considered security and privacy perceptions and practices in rural Ghana [17]. Abokhodair et al. studied the privacy and security tensions in using digital technologies in the Arab world [1, 2]. Ahmed et al. reported on the data privacy challenges associated with device repair practices in Bangladesh [4] and the privacy challenges that arose in the Bangladeshi government's mandatory mobile SIM registration scheme [5]. Taken together, these studies suggest that notions of culturally-situated privacy often contradict the assumptions held by Western designers [30, 34].

In summary, our paper makes a unique contribution to privacy research within the CSCW community by contributing the first analysis of the privacy challenges, tensions, and trade-offs

that arise as families in the Global South share digital devices. In addition to research on privacy, our paper also contributes to CSCW's growing interest in understanding and designing for diverse and marginalized populations [25, 44, 48, 64, 69].

3 METHODS

The goals of our research were (1) to develop a nuanced understanding of mobile phone sharing practices among families in Bangladesh, and (2) to analyze the privacy challenges and constraints that arise when people share devices. To achieve these goals, we conducted a qualitative field study in Dhaka, Bangladesh with families who share devices. Our data collection consisted of semi-structured interviews with 72 participants from 38 families. This section describes our methods in detail. We received IRB approval for all study procedures prior to beginning the study.

3.1 Semi-structured Interviews

We conducted semi-structured interviews with participants between March and June 2016. The interviews targeted understanding participants' mobile phone sharing practices and the privacy challenges that arise when people share devices. The first author was born and brought up in Bangladesh, spoke the local language (Bengali), and was familiar with the local culture and customs. Since the practice of sharing mobile phones among family members is very common in Bangladesh, we began by recruiting participants through convenience sampling. A total of 10 families were recruited through the social network of the first author. These first 10 families then helped us recruit an additional 28 families through snowball sampling, until we reached theoretical saturation. In total, we recruited 72 participants from 38 families.

Participation in the study was voluntary. Interviews lasted roughly 30 minutes and were conducted one-on-one. We obtained written consent from participants before their interviews. All interviews were conducted in Bengali at participants' residences and audio-recorded with permission from participants. Participants received 800 Taka ($10 USD)[1] for participating in the study. The interviews were semi-structured and guided by a list of topics. We collected participants' demographic information and asked about their family members, prior experience with technology, and the devices, services, and applications that they use. We also asked questions that sought an understanding of if, and how, they share mobile phones with friends or family members, and the benefits, challenges, and trade-offs that result from sharing devices, including tensions regarding digital privacy and security.

3.2 Participant Characteristics

Our 72 participants (42 males and 30 females) came from 38 families and ranged in age from 20 to 75 years (average = 37). Participants possessed a range of socioeconomic backgrounds. Twelve of the 38 families were low-income, with average monthly household income of less than 10,000 Taka. Fifteen families were middle-income, with average monthly household income of between 10,000 and 20,000 Taka, and 11 families were high-income, with average monthly household income above 20,000 Taka. Participants also possessed a wide range of educational backgrounds. Of our 72 participants, 14 did not finish elementary school, 17 finished elementary school, 12 finished high school, and 29 had a college degree.

The families that we studied represent a wide range of the socioeconomic spectrum present in the urban population of Bangladesh. The low-income families that we interviewed had little formal education. Their professions included night guard, chauffeur, domestic help, waste pickers, rickshaw drivers, and garment factory workers. The fifteen middle-income families were all well-educated,

[1]One USD is approximately 80 Bangladeshi Taka.

with the adults either still in college or possessing an undergraduate degree. Their professions included small-scale personal business owner, bank teller, home maker, software engineer, university teacher, and artist. The high-income families were also well-educated except for a couple of families where the highest level of education was high school. Their professions included secretary, large-scale business owner, worker at an international firm, and political leader. Of the 38 families, 34 were Muslims and 4 were Hindus. All participants were native speakers of Bengali.

3.3 Data Collection and Analysis

The data that we collected resulted in a total of 30 hours of audio-recorded interview data and hundreds of pages of field notes. Two members of our team who are native speakers of Bengali transcribed the interviews and translated them into English. We then performed inductive analysis on the interview transcripts [61]. We started by reading through the transcripts several times, allowing codes to emerge from our data. Examples of codes that emerged include, *"rules for sharing"*, *"locking apps"*, and *"deleting personal data"*. We iteratively refined the codes before clustering related codes into the high-level themes that represent our prominent findings described in the sections below. The final codes and themes were agreed upon by all members of the team.

4 PARTICIPANT DEVICE SHARING PRACTICES

Before discussing the privacy challenges that arise when participants share mobile phones, it is important to develop an understanding of *how* our participants currently share devices. Broadly, the families that we interviewed shared phones in two main ways: (1) sharing a family phone, and (2) sharing a personal phone with others. Some families possessed only one 'family phone' that was shared among all members of the family, often because they were unable to afford a separate device for each family member. However, more commonly, we found that device sharing was generally *not* governed solely by economic need. In most families, individual family members owned the phones but frequently allowed other family members to use them. In these situations, two or more members of a family would each have their own phone, but would also use the phones of others, either out of convenience or because the device possessed desired capabilities (e.g., it had a better camera). However, the social norms and implicit or explicit rules that governed the use and sharing of phones differed, as we discuss below.

The most prevalent device sharing models we found were: (1) sharing between a husband and wife; (2) sharing among siblings; and (3) sharing among parents and children. The following three vignettes illustrate each of these models and highlight the complexities associated with them.

4.1 Vignette 1: Shared use by husband and wife

Mrs. Ka is a 28-year-old housewife who lives with her husband and his family. The members of the household consist of Mrs. Ka, her husband Mr. Ka, and her husband's elderly parents, younger brother, and teenage sister, Ms. Ga, who is a big fan of Indian movies and music. Mr. Ka is employed by a local bank and is typically away at work between 8am and 6pm on the weekdays.

Mrs. Ka possesses a smartphone that she received last year as a gift from her father. It is a high-end smartphone that she describes as being *"very beautiful"*. She uses this smartphone for voice calling and text messaging, as well as to access a variety of online services and applications, including Facebook, Youtube, Viber, and Whatsapp. Although the phone belongs to Mrs. Ka, her husband frequently takes his wife's phone and uses it, often with the intention of making sure that his wife *"does not get into any danger."* As Mrs. Ka described,

> *"My husband often uses my phone and checks Facebook and Messenger. This is not because of any suspicions, because he knows I am not that kind of woman. He just wants to make*

sure that I do not interact with any foul person on the Internet. He also checks my text messages, photo albums, and Internet browsing history. Sometimes, it is annoying, but if I protest, he will be suspicious. So, I keep quiet. The worst part is that he does not like me listening to Indian music. So if he finds any Indian music on my phone, he gets angry. But, my sister-in-law also uses my phone and she often watches Indian music on it. I have to explain this [to my husband] every time. This often gets frustrating."

This story highlights a number of interesting interactions. For example, Mrs. Ka described how she did not feel free to use her phone as she wanted because her husband always *"kept an eye"* on her phone. She said that she could not store any information, pictures, videos, and music on her phone that might be *"misinterpreted"* by her husband. Moreover, Mrs. Ka told us that there was no point in using any security features to protect her privacy, such as screen locks, because her husband would simply request that she unlock all her applications, and she would be unable to say no. In addition, although Mrs. Ka said that she did not mind if her sister-in-law borrowed her phone, the fact that Ms. Ga used the phone to watch Indian music and videos frequently got Mrs. Ka into trouble with her husband. Despite this, Mrs. Ka said that she did not know how to say no to her sister-in-law.

When we interviewed Mr. Ka, we asked him why he checks his wife's Facebook account and other applications. He explained to us how, although he had no *"bad intentions"*, he thought that such checking would help to *"keep her in line"*. Finally, although Mr. Ka is able to use Mrs. Ka's phone whenever he wants, the opposite is not true. When we asked Mrs. Ka if she was allowed to use her husband's phone or check his online accounts, she told us that she was not allowed to touch Mr. Ka's phone. Mr. Ka described that he kept many important documents on his phone and he was afraid that his wife would accidentally delete those documents.

4.2 Vignette 2: Shared use by siblings

Mr. Anu is a 22-year-old university student. He lives in Dhaka with his family, which consists of himself, his two older brothers, one younger sister, one cousin, and his parents. All of these family members reside together in a large apartment. Mr. Anu possesses a smartphone that he has been using for a couple of years, although this phone is shared by his siblings. Mr. Anu uses the phone to access a variety of applications, including Facebook, Whatsapp, Messenger, and Youtube. He also likes to take a lot of photos with his phone because it has a very good camera. However, he describes how he often feels uncomfortable saving photos on his phone because his brothers and sister will find them,

"You know, I often take funny photos when I am with my friends. Many of them are just trashy photos that do not make much sense. They are just for fun. But if my elder brother sees them, he will yell at me. Also, if my younger sister finds them, she will make fun of me . . . I am happy if [my siblings] use my phone, but the problem is that then they also get access to my photos. And, I cannot lock these photos either because that would trigger her interest even more. This is a big problem, but what can you do when you live with your family?"

Ms. Banu, the younger sister of Mr. Anu, does not possess her own mobile phone and uses her brother's phone mostly to play games and watch Youtube videos. She also likes to take pictures using the camera on Mr. Anu's phone. Although her other brothers also possess smartphones, which she sometimes uses, she prefers to use Mr. Anu's phone because she thinks that it has the best display.

Although Ms. Banu's parents are comfortable allowing their sons to use mobile phones, they do not want Ms. Banu to use a mobile phone too much because they are afraid that she will learn

bad things on the Internet. In addition, Ms. Banu's parents do not like some of her friends and get angry with her if they see Ms. Banu hanging out with those friends. As a result, Ms. Banu described how she must be very careful to keep secret any phone calls that she makes to her friends from her brothers' phones or any photos that she has taken with her friends using their phones. Indeed, we heard how Ms. Banu's brothers often threaten to show the photos to their parents if she does not do what they say. As a result, she tries hard to maintain a good relationship with her brothers, while also looking at the personal photos that they keep on their phones so that, if necessary, she can use them against her brothers.

4.3 Vignette 3: Shared use by parents and children

Mr. and Mrs. Masud live in Mugda area with their 15-year-old daughter, Mazeda, and their 12-year-old son, Mozammel. Mr. Masud is a banker and does not stay at home during the week. Mrs. Masud is a housewife and both of the children go to school. Mr. and Mrs. Masud both own smartphones that they share with each other, and Mrs. Masud's phone is also shared by her children. Mazeda often uses her mother's phone to call her friends or watch movies on Youtube. Mozammel primarily uses Mrs. Masud's phone to play games. Furthermore, Mrs. Masud's phone is often considered to be the 'family camera' when the family goes out or participates in events and celebrations, and the children frequently use Mrs. Masud's phone for taking photos and recording videos at those times.

Mrs. Masud told us that she has to be very careful about the content that she stores on her phone because her children have access to the device. She described how she always deletes any messages, images, or videos that her friends send her if she thinks that the content is inappropriate for her children. As Mrs. Masud described,

> *"Our friends often send us jokes, images, or videos – which are ok for adults, but not good for young kids. I have to be very careful about this. I delete these things as soon as I read them because I do not want my children to see them. This is something you need to be careful about when you are a parent."*

Mr. Masud does not allow his children to use his phone. He mentioned that he keeps important documents on his phone and that it is not a *"toy for the kids"*. In addition, Mr. Masud described how he generally disapproves of allowing young teenagers to use mobile phones because he sees them as a threat to the children's development of social skills. He described how he was aware that the children used Mrs. Masud's phone, but he frequently told his wife that she should not allow the children to use her phone.

Both Mr. and Mrs. Masud told us that, although Mrs. Masud's phone has a better camera and is frequently used for taking family photos, they almost never used Mrs. Masud's phone for their personal photos because they did not want their children to see their pictures. Instead, they used Mr. Masud's phone for taking photos because the children were unable to access his phone. Mr. and Mrs. Masud also both used screen locks on their phones, which further enabled Mrs. Masud to control her children's access to her phone, and which she considered to be a part of good parenting in this digital age.

4.4 Analysis

The vignettes presented above showcase three common device-sharing models that came up in our data and show how the practice of sharing can quickly produce complex scenarios with unique considerations that make it difficult for participants to use devices freely. In each of the vignettes, we can identify several social relationships that impact people's personal privacy with mobile phone sharing and see how these relationships are affected by social and cultural norms that are different from those in Western contexts.

For example, the first vignette reveals a prevalent male-dominated power dynamic common in patriarchal societies like Bangladesh that we encountered in all of our participant families. The most senior male person in the house (usually the father) was always the head of the family. He controlled the family's finances, made the important decisions, and the other family members respected his wishes. In many cases, wives did not have any personal income and were financially dependent on their husbands. Even in cases where wives did have their own jobs, they were still required to follow their husband's rules. In all of the families we interviewed, the husbands had the power to monitor and control their wives' use of mobile phones.

The sibling power dynamics highlighted in the second vignette demonstrate how late-stage adolescent or adult siblings (e.g., college age) share their digital devices. Siblings using each other's devices is very common in Bangladeshi society and is connected to the family-centric value system that is part of Bangladeshi culture. Elder siblings are often expected to take care of their younger siblings and society frequently holds them responsible for the actions of their younger siblings. This sense of responsibility is reinforced by parents, other family members, and religious leaders in the community. Elder brothers are often questioned if their younger siblings do anything that society does not approve of. In some communities, any activity that is not socially approved is not only attributed to the individual who committed the action, but to their whole family. As a result, older family members are often vigilant about keeping track of younger family members activities, both online and offline. This social pressure makes it acceptable for older siblings to demand access to younger siblings personal information. However, although accountability plays a major role in device sharing among siblings, they also often share devices for fun or other social reasons. In addition, our data shows that parents are more concerned about controlling the ways in which their daughters use devices than their sons, which introduces gender dynamics that we discuss in detail in the next section.

Our third vignette demonstrates the concerns of parents with regard to the digital content that their children are exposed to. In Bangladesh, many parents' concerns are intensified by the uncertainty created by the sudden intrusion of digital and mobile technologies into their lives. Parents are often unaware of the potential risks or effective cautionary steps and tools to protect their children online. In many families, the question of how much sharing of digital life is safe and acceptable is not yet settled. As a result, different parents develop and use different strategies for maintaining the required gap between their digital lives and their children. The vignette also shows how access to the father's phone may be different than to the mother's phone, which further highlights gender dynamics that we discuss in detail below.

5 UNPACKING SHARED USAGE AND DATA PRIVACY

The vignettes described above provide a rich understanding of how our participants share devices with their families. We now discuss the benefits that participants receive from sharing, unpack the gender dynamics and challenges associated with sharing, and discuss the privacy issues and concerns that arise as participants share devices.

5.1 Sharing is Convenient and Offers Access to Resources

Several participants described that device sharing was a convenient usage model that gave them access to a device in times of need. Sometimes, it was simply about being able to use whichever device was closest. At other times, such as in times of family emergency, having multiple devices that could be used to communicate with family members was beneficial. One participant told us how he was able to use his friend's mobile phone when he was unable to access school materials on his own phone, describing,

> *"The good thing is accessibility. Suppose I don't have any pdf, lecture, or other important study materials on my phone, but my friends have it on their devices. Then I can easily access these things on their phones."* (Family 5, Member 3)

Beyond convenience, we also found that sharing mobile phones helped our participants get access to resources that were otherwise unavailable. Participants described how sharing multiple devices between them meant that it was more likely that at least one would contain sufficient battery power or mobile airtime for the tasks that the participant wished to achieve. For example, one participant said,

> *"The good thing is, if I don't have any airtime in my own phone, or if there's no battery, then I can use their device without any hesitation."* (Family 5: Member 1)

This participant was a college student with no regular income who depended on a small amount of pocket money from his parents. He often ran out of money and thus his phone would also run out of airtime. He also frequently talked to his girlfriend for long periods of time at night on his mobile phone, which would often cause his phone to run out of battery during the day. Therefore, being able to use his brothers' phones when he could not use his own was very helpful for him. Of course, using up another family member's airtime or mobile phone battery also introduced tension, since the person who paid for the airtime would not be happy that it had been used up.

5.2 Sharing is Socially and Culturally Expected

Our analysis reveals that participants often allow others to use their devices, even when they would prefer not to, because sharing is an accepted social and cultural practice that is deeply embedded in Bangladeshi society. Unlike individualist Western contexts, where it is socially acceptable to *not* share devices, Bangladesh is a more collectivist society and it is expected that individuals share resources with their friends and family members.

We found that device sharing was prevalent even when each family member possessed their own device. In particular, participants told us that, although they would prefer not to share their device, they felt that they had *"no choice"* but to say yes if their siblings or friends asked to use their mobile phone since it is considered to be "unkind" or "rude" to say no if a familiar person (e.g., friend or family member) wants to share somebody's phone. This practice is not limited to mobile phones and is deeply rooted in Bangladeshi culture; people in Bangladesh often share things in their daily life, including clothes, vehicles, food, and animals. Further, participants expressed that failing to share their device with a family member would suggest that they did not trust that family member, which could harm their relationship.

5.3 Sharing Offers Safety and Transparency

Many of our participants shared that their relationships benefited from the practice of sharing devices. In the context of married couples, participants described how sharing phones was one way to increase transparency in their relationship. One participant told us how it was *"natural"* to share her phone with her husband, because she had *"nothing to hide"* and never engaged in activities that might put her in an embarrassing position. She further explained that she also never hesitated to allow other people that she knows to use her phone if they needed it, adding that refusing them would be *"unkind"*. In other cases, we found wives sharing their phones with their husbands, but not sharing the phone with anybody else. Many participants said that they stored private photos on their phones that could only be shared with their husbands. Regardless of whether they shared their phones with outsiders or not, all of them reported that sharing their phones with their husbands positively impacted their relationship through better transparency and by creating moments of shared joy that resulted from watching or discussing things together.

Several participants also described how sharing devices with their husbands helped to keep them safe. Many women expressed that their husbands were more knowledgeable than they were about digital technology and the Internet, and they therefore considered it helpful for their husband to look after their mobile phones. A few participants also described different security-related threats that could happen to them. For example, one of our participants was a homemaker in a middle-income family. Although she graduated with a Bachelor's degree in Philosophy, she spends her time at her home with her young children. She mentioned not knowing much about electronic devices and computers, but had heard several scary stories from her friends and relatives. She said,

> *"One of my friends was harassed through Facebook. One guy started talking to her pretending to be a lady. She even gave the guy some money and also invited him to their place. Later her husband figured out that it was a guy behind that profile. Imagine what would happen if her husband did not find that out! That is why I always feel safe when my husband checks my phone. Also, you know there are so many viruses that I have no idea of."* (Family 31: Member 2)

When we talked to this participant's husband, we discovered that he also did not have any formal training with electronics or technology. He graduated with a Bachelor's degree in Business Administration and worked at a local bank. His knowledge about computers and mobile phones was acquired through articles that he read on Facebook that were shared by his friends, some of whom were computer experts. He also expressed feeling safer checking his wife's mobile phone, because, *"there are so many things happening"*. In general, we found that gender played a large role in people's device sharing practices, as we now discuss.

5.4 Gender Dynamics Impact Sharing

Our analysis shows that gender plays an important role in participants' device-sharing practices, with many of the stories that we heard revealing unequal sharing relationships based on gender. Gender discrimination is prevalent in Bangladeshi society [3, 6] and our study shows how the power differences between males and females impact women's ability to have data that might be kept private from her husband. In several cases, our female participants reported that they are not allowed to keep anything private from their husbands. In some cases, the husbands forced their wives to enter their passwords and open Facebook or Messenger so that they could go through their personal data and usage history. Moreover, in many cases all of the devices in the house have been purchased by the husband, and thus the women do not actually own their device. We heard stories of how the husbands would use the fact that they were the wage-earners as an excuse to access their wives' devices and accounts.

Challenges associated with gender also often resulted in differences between how sons and daughters were allowed to use devices. As our second vignette shows, parents are frequently more concerned about controlling the ways in which their daughters use technology than their sons. When these challenges occur, brothers often helped their sisters use technologies in ways that were kept secret from their parents. Although brothers were often willing to cover for their sisters, brothers were also able to use their knowledge of their sisters' activities to 'blackmail' their sisters into doing what they wanted. Moreover, the sisters often responded by collecting their own material to blackmail their brothers in return. The issue of accidentally forgetting to log out of online accounts further increased the potential for blackmail. One participant said,

> *"Sometimes I have downloaded their personal photos from their Facebook account and saved those in my phone. Because, you know, these photos are of good use if you need to blackmail them later."* (Family 4, User 2)

5.5 Sharing Results in Privacy Violations

The above discussion on gender dynamics begins to reveal some of the ways in which sharing devices can lead to data privacy risks and violations. Approximately half of our participants were cognizant of these privacy issues and said that, given a choice, they would prefer *not* to share devices. As in our first vignette, many female participants reporting feeling annoyed, frustrated, violated, or powerless when their husbands went through their phones to check on them. However, the most common dissatisfaction our participants expressed regarding sharing of mobile phones was the potential for the privacy of their personal data to be compromised, which made our participants feel vulnerable. As one participant said,

> *"Actually, I'm against using a shared phone. If more than one person uses the same phone, it is not possible to maintain anyone's privacy. I don't think it is completely safe to store my personal stuff in a phone, especially when it is shared."* (Family 1: Member 2)

This participant was a 20-year-old unmarried college student who shared his mobile phone with his younger brother. He reported that he was not able to store personal data on his mobile phone because his younger brother could see them. Several of the participants who were generally against sharing agreed that, in emergencies, sharing might be necessary. However, one also said that he anticipated encountering privacy issues even in emergency situations, telling us,

> *"If someone takes my phone for their emergency phone call or something like that, I've sometimes seen them try to access my pictures or personal messages. So, ultimately, I find no good side of sharing."* (Family 4: Member 1)

This participant was a 35-year-old bank officer, who stored his family pictures on his phone. As these excerpts suggest, participants were often worried about people intentionally trying to look at their personal information, including photos, videos, and private messages. However, *unintentional* privacy violations were also a concern for participants, particularly since many applications and services use automated notifications to alert a user when, for example, they have received a new text message or email. These notifications frequently revealed personal information to whoever happened to be using the device when the notification occurred. One participant said,

> *"When my messages pop up on my phone screen, it's embarrassing if someone else sees them. They often misinterpret my messages. It is not safe. Anything can happen, like, they can reveal my secret stuff or they can gossip about me in their groups and spread rumors."* (Family 4: Member 2)

This participant was a young female college student. She often shared her phone with her friends, but she also had a boyfriend with whom she frequently exchanged messages. Notifications of incoming messages would often pop-up with a preview, which were potentially embarrassing when her friends were using her phone. This is an example of how the existing design of mobile devices, applications, and services, which is primarily targeted towards 'personal' use, may not be appropriate for shared device usage patterns.

5.6 Existing Practices for Protecting Private Data

Although many participants felt that the risks to their personal privacy outweighed the benefits that they received from sharing, and expressed that they would prefer to not share their devices if it was an option, our analysis shows that they are actually not against sharing *per se*, but rather how the current design of mobile devices, services, and applications are insufficient for supporting their privacy needs. We now discuss participant tactics for preserving their data privacy in the face of challenges that arise due to shared usage.

We asked our participants what tactics they used to protect their private information on the mobile phones that they shared with others, and most participants described a variety of techniques used to preserve their privacy. The types of information that participants were concerned about keeping private were relatively straightforward: photos, videos, and message conversations – both on platforms like Facebook and Whatsapp and via SMS text messages. Several participants also mentioned that they would not want anybody to look at their browsing history or details of the people that they called. Common tactics for protecting private data included restricting their own usage, deleting any personal data, developing a set of rules or guidelines that were agreed upon by the people sharing the device, coming up with tricks to prevent others from finding private information, and using commercial software to lock specific applications and prevent others from looking at them. We discuss each of these tactics in turn.

5.6.1 Restricting use and deleting personal data. One prevalent tactic that participants used to protect their privacy was to simply not store any private or personal information on their phone, especially anything that they would consider to be embarrassing if it was discovered. A few participants achieved this by restricting their own use of the device because, if the personal data did not exist, it could not be used to embarrass the participant. As one described,

> *"Sometimes I do not take pictures or do not store information that is personal and that I wouldn't want to share with others. I always have to keep in mind that another person is sharing the phone."* (Family 2: Member 1)

In addition to restricting their use of the device, some participants described that they would try to preserve the privacy of their data by going through all of the captured data and deleting anything that could be misinterpreted or potentially construed as embarrassing, including deleting their mobile phone call history, or deleting photos or videos that have been downloaded after watching them. Finally, participants mentioned that they needed to try and remember to sign out of all their online accounts when the device was going to be used by someone else, including email, Facebook, Whatsapp, and others. This was frequently challenging to achieve, in part because unlike logging into an account on a website through a browser, in which it is relatively easy to log out, the design of many mobile apps is based on the 'personal use' paradigm, in which the app is tied to a specific user account (e.g., Android devices require a specific Google account through which users download and install apps and is also used as the account for the email apps). Understanding the intricacies of these app designs and how to coordinate logging in and out of apps was frequently confusing or challenging for our participants. Our participants described how they would frequently discover that someone who shares the device with them had failed to properly log out of their accounts. One participant said,

> *"People use my phone to check their Facebook but they often forget to log out. So when I open my browser I can easily see their Facebook messages, photos, status, friend lists, and so on."* (Family: 4, member 2)

This and similar stories indicate that using a shared mobile phone comes with a number of responsibilities not otherwise present when the device is personal, such as understanding how personal data can be leaked, hiding or deleting personal data after use, and not looking at other people's data.

5.6.2 Specifying rules for sharing. Another common tactic that participants used to manage shared devices was to develop a set of 'rules' that everyone who shared a device agreed to follow. Generally, the goal of these rules was to protect everyone's privacy. For example, one participant who shared his phone with his brother reported,

> *"We have a rule for the phone. He will not look at my personal stuff and I will not look at his personal stuff."* (Family 2: Member 1)

His brother further elaborated on how the rule-based system that they had developed worked,

> *"If I left the phone without logging off from Facebook, he will first log out of my Facebook before using the phone."* (Family 2: Member 2)

Both brothers reported to us that they expected the other to respect the rule. The rule itself was based on a sense of reciprocity where each individual values the privacy of the other. However, although this rule is easy to understand in situations like logging out of Facebook, it can be difficult to enforce and navigate in the cases of pictures or text messages where the storage space is shared and there is no way to not look at the other person's data when using the device to look at one's own data. Indeed, the brothers reported that they were careful to avoid storing sensitive data on the phone despite having sharing rules in place. This example reveals how sharing rules are shaped by the way different applications work on mobile phones.

In addition to rules between siblings, there were frequent rule systems that governed the ways in which children were allowed to use their parents' phones. One parent told us,

> *"I often tell my son not to touch my phone. Sometimes my friends send vulgar messages or pictures and I don't want my sons to see them. That's why I tell them not to touch my phone. I delete those messages and pictures before they touch my phone."* (Family 4: Member 1)

In some cases, the rules are mutually agreed upon. More frequently, however, we found that the rules were created by the owner of the phone, and the other people who share the device are required to follow the rules if they wish to use the phone. One participant wanted to control the people who were allowed to contact him and told us,

> *"I have saved some phone numbers on the device. And I told [my wife] which calls she can pick up and which ones she can't. And if any number is calling that is not saved, she doesn't pick up."* (Family 7: Member 1)

This participant was a retired bank officer who would share his phone with his wife. Following the male-dominated social and economic infrastructure of the country, he owned everything in the house. His wife was a homemaker and also "owned" a phone given to her by her husband. Although the wife could use her own phone, like most things in their household, rules governed its use as well. This example reveals how the rules for sharing are also connected with the broader social and cultural norms of the country, and are not necessarily based on equity and reciprocity.

5.6.3 Workarounds used to preserve privacy. Rules and policies do not always work, and many participants who used such rule systems still experienced breaches of privacy. We also learned about tactics that our participants used to try and handle embarrassing situations that occurred when someone discovered their private information. One common technique was for the participant to simply deny that the information was theirs. For example, one of our female participants from a low-income family who shared her phone with her husband told us that she did not want her husband to know that she used her phone to talk to her sisters. Her husband did not like her to be talking to her relatives because he feared that her relatives might ask her for money. The wife told us that she had quarreled with her husband a number of times over this issue. Although this participant earned more money than her husband, she was not allowed to spend money without his consent. She described how, if other people (including her husband) discovered the contact numbers of her sisters in her call history, she would deny that the numbers were connected to her,

> *"If I get a phone call from my sister, I will tell others that the call came from a wrong number and that I hung up."* (Family 7, User 1)

As in Vignette 1, the phone revealed information that the owner of the data was required to account for [63], but that would have been unnecessary if the owner's privacy had been preserved. Another tactic was to negotiate with the other person so that, although they now knew the private information, they would not go and spread it further by telling others. Negotiation tactics ranged from using anger and blackmail, to trying to *"be nice"* to the person. One participant said,

> *"I feel very irritated and angry [when someone compromises my privacy]. Because then I have to convince the witness not to share my data with anyone else. I might get caught sometimes and then I'm kind of bound to him, because he knows my secret! This is really big trouble."* (Family 4, User 2)

5.6.4 Using commercial software to protect data privacy. In addition to creating rules and regulations to govern sharing practices, many participants also described that they would use commercial software or phone features to lock private data on their phones. Almost all of our participants had turned on the device's screen lock to prevent unauthorized access. However, it was common for anyone who shared the phone to know the PIN code required to unlock the phone. Thus, although locking the device may prevent strangers from accessing it, it does not solve the problem of preventing unwanted access by people who are authorized to share the device.

One common commercial product that came up often in our data was an app called "CM Security" which, in addition to protecting phones against viruses, would also allow people to lock each of their applications separately. Participants described how this was a particularly useful tool that gave them more granular control over what applications were shared and what private data might be vulnerable. For example, a participant could choose to share the text message application, but not the Facebook application. As one participant described,

> *"Facebook, WhatsApp, Messenger, Gallery, Video Player. Mailbox should be locked too. Sometimes my friends check my mailbox and forward important or sensitive emails to their account without my permission. So I keep the mailbox locked. My call list is also sensitive because my parents often check my call list. If I have contact with anyone that they don't like, then it creates a family quarrel."* (Family 4: Member 2)

Unfortunately, however, this locking mechanism quickly became ineffective if the person who shared the device also needed to use a locked application. For example, one of our participants described how he would lock Facebook but then had to just unlock it every time he shared the phone with his brother, so that his brother was also able to use Facebook.

Although locking individual apps was one useful mechanism that helped some participants to better protect their private data, they also described how the act of locking an application could result in social challenges that affected their family relationships. For example, participants reported that their partners would get upset, sad, or angry if they encountered any applications on the device that were locked. In addition, almost half of our participants reported that locking specific data or applications might also raise suspicions in the mind of their partners who were sharing their phones. This was particularly true for device sharing between married couples.

Finally, all participants agreed that the existing privacy protection mechanisms available to them are not sufficient to protect their personal privacy in the face of risks and challenges that occur as a result of device sharing. Instead of locking mechanisms that are evident to anyone who is using the device, several participants told us that they wanted a new application that was capable of hiding their private data in such a way that their partner would not be able to tell that anything was hidden. We discuss this idea in greater detail in the next section.

6 DISCUSSION

Our analysis provides an understanding of how and why families in Bangladesh share devices and the privacy challenges and concerns that arise through shared use. This section discusses some of the broader issues that result from our findings, including how some of the privacy challenges experienced in the Global South could lead to innovations that improve privacy in Western contexts as well. We also discuss how the Western notions of privacy that drive the design of most modern mobile devices may not effectively address the usage patterns and needs of populations in the Global South, and consider how the power dynamics that came up in our analysis affect different individuals' rights to privacy. Finally, we present concrete design implications for researchers interested in designing applications or services that better support privacy with shared devices.

Our analysis reveals that sharing mobile devices is both an expected cultural practice and a necessity. People often face problems of mobile phones running out of battery or airtime balance, which result in users in contexts like Bangladesh frequently relying on shared devices to keep their communication channels functional. Although especially prevalent in the Global South, these kinds of situations may also arise in Western contexts, particularly during disasters and breakdowns [35, 36]. In this way, the practices associated with sharing mobile devices that are prevalent in Bangladesh can inform the use of mobile phones for Western contexts.

Our findings are aligned with the growing literature of post-colonial computing in the CSCW and HCI communities [8, 34]. The Western notions of privacy that are inscribed in the design of modern mobile phones, and their assumed use, along with the mismatch of these notions when it comes to local cultural practices in Bangladesh, depict why it is important for researchers to situate the design of technologies into local practices. However, our study also reveals that mobile device users in Dhaka were not always happy about the need to share their devices with other family members. The desire to keep information private still exists in these contexts, and people often need or want a personal space where they are able to safety store their private data. However, the prevalent cultural practice of sharing devices, combined with the privacy challenges that arise during sharing, means that it is not always possible for people to find such personal space. Hence, the idea of privacy in Dhaka consists of a complex mixture of both revealing and hiding personal information. Instead of defining these contexts through their differences with Western cultures by labeling them as "collectivist" rather than "individual" as Hosftede did [31], we see these contexts more as simply *different* settings, with their own unique tensions and trade-offs. We believe that these differences are important to conceptualize in order to design technologies that are more appropriate for communities living in the Global South.

Our analysis reveals that practices surrounding digital privacy are still subsumed within existing power infrastructures. Numerous examples show that locking private data with passwords, or by other means, often does not work when the mobile phone is shared with somebody who has more power than the user, such as when a wife is forced to unlock her device and let her husband inspect it. Within these kinds of power hierarchies, is it possible for individuals to still protect or maintain their privacy? This question moves the design space from a domain that is purely technical to the discourse of political theories. Individuals in such circumstances can decide whether to fight, negotiate, or adopt other workarounds to try and engage with the power-holders. In most existing technical solutions, such as current systems that enable users to lock applications, it is clear to the other people who are sharing the device that the user is trying to keep information private, which may or may not be an appropriate mechanism for protecting the user's privacy rights. If we see technology as a tool for freedom (and thus "development" [57]), we need to also protect individual users' voices in and through these technologies [19]. Hence, our study connects the discourse around privacy-protecting interfaces to wider scholarly discussions around

democracy and development. If technology is to be considered a vehicle for development—as espoused by scholars within CSCW and related disciplines—then that technology may also need to be either situated within a democratic environment or actively designed toward achieving democratic outcomes.

One particularly salient power dynamic surfaced in our study is gender inequality, which connects our work to scholarship within CSCW and related disciplines around the feminist agenda in computing. A rich body of work examines how mainstream computing embodies and reproduces male-chauvinist values that eventually limit the role of women in technology [12, 13, 38, 53, 59]. A parallel thread of work specifically reports on how technology practices in the Global South often hold women back, are used against women, or contribute to the larger infrastructure that systematically promotes misogynistic agendas in the Global South [3, 6, 33, 39, 40]. Our study contributes to both of these bodies of work by showing how the existing design of mobile phones and the paradigm of "personal computing" have not worked for women in Bangladeshi societies. Both the design of the components themselves (for example, women can be harassed through these devices) and the practices that evolve around the design (for example, wives can be forced to unlock their devices) prove to be inappropriate for preserving the privacy of Bangladeshi women who live at the intersection of postcolonial politics and male-chauvinist value systems.

Our findings also resonate with Crabtree et al.'s [23] explanation of privacy among family members, which claims that the family's digital devices are the interface between the family's privacy and the connected world, and characterizes a family's digital devices as an "attack surface". They argue that privacy research should focus on managing *"the potential 'attack surface' of the digital on everyday life occasioned by interaction in and with the networked world"* and *"that privacy dissolves into a heterogeneous array of relationship management practices."* In our study, limited resources, cultural norms, and power dynamics all act to expand rather than reduce the privacy attack surface, thus making it more difficult for family members to manage their relationships through their technology interactions. We now outline design ideas motivated by our findings that may reduce the attack surface extended by device sharing.

6.1 Design Implications

Our findings point to several ways in which new technical tools could be designed to better protect data privacy on shared devices. We discuss two ideas: (1) enabling people to hide personal information in ways that keep secret that there is hidden data, and (2) re-designing applications to better fit a "shared use" paradigm instead of a "personal use" paradigm.

Although several technology companies have recently enabled the creation of multiple user accounts on a single device [10, 60], our findings suggest that people do not use this functionality, partly because poor usability makes it time-consuming and inconvenient to switch accounts, but also because logging out of one's user account before sharing it with a family member would imply a lack of trust in that family member or arouse suspicion by suggesting that the person has something to hide. This fear of arousing suspicion is especially prevalent among women who do not want to be perceived to be keeping secrets from their husbands. These challenges suggest that one problem with current approaches to multiple user accounts is that *the existence of the multiple accounts is clearly visible* to others (e.g., husbands) who are able to simply demand access.

To overcome this problem, we plan to create an experimental system that will enable a *single user* to have *multiple accounts*, with the existence of the multiple accounts kept *secret*. This model will enable a person to create a 'shared' account that contains data they are willing to share and that is assigned a password or PIN code that will be shared with family members. Simultaneously, they can create a 'secret' account that will contain data that they prefer to keep secret and that uses a password or PIN code that they do not share. Then, for example, when a husband asks to

check his wife's device, she can hand it over and tell him the password for her shared account, with her private data securely stored in her secret account that her husband is unaware of. Of course, designing applications that enable users to keep data secret without appearing to do so could also have safety implications for potential users. For example, a husband discovering that his wife was keeping data secret from him may result in a more dangerous situation for the woman involved. Exploring these tensions and trade-offs will be part of our future work.

Finally, redesigning mobile phones from the perspective of a "shared use" paradigm, in which the default assumption is that devices are shared, presents a wide range of interesting design opportunities. For example, the tendency of notifications to pop-up at various times, regardless of who is using the device, was seen as a potentially serious privacy risk by participants, but turning on and off notifications for each app was both burdensome and required knowledge of how to navigate each app's notification settings. Similarly, although participants found it useful to be able to lock individual apps, it was irritating for them to have to lock and unlock each application before and after they allowed their partners to use their phone. We hypothesize that it would be beneficial to design a new 'sharing' mode for mobile phones that approaches the design of applications and services in ways that assume the device will be shared and that automatically sets app behaviors accordingly (e.g., notifications, app locking). Users should then be able to easily configure the actions and features for both the "shared use" and "personal use" modes as desired.

7 CONCLUSION

This paper describes a qualitative field study that we conducted with the goals of (1) analyzing how families in Bangladesh currently share mobile phones, and (2) evaluating the privacy tensions and challenges that arise as individuals seek to achieve their personal goals using shared devices. Findings from our study reveal that participants use a diverse set of device sharing models to share mobile phones with different family members, including spouses, siblings, parents, and children. Participants also used a complex mix of individualist and collectivist strategies to try and protect their private data from the people with whom they share devices. We provide a nuanced understanding of current sharing practices and synthesize a set of design and policy implications that could better protect individuals' data privacy on shared devices. We also discuss how Western notions of privacy are complicated by the different social and cultural values of our participants. Taken together, our findings contribute a rich understanding of mobile device sharing practices among families in Bangladesh and highlight challenges in designing privacy-preserving technologies for populations living in the Global South.

REFERENCES

[1] Norah Abokhodair. 2015. Transmigrant Saudi Arabian Youth and Social Media: Privacy, Intimacy and Freedom of Expression. ACM, 187–190. http://dx.doi.org/10.1145/2702613.2702629

[2] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & Social Media in the Context of the Arab Gulf. In *Proc. Conference on Designing Interactive Systems*. ACM, 672–683. http://dx.doi.org/10.1145/2901790.2901873

[3] Syed Ishtiaque Ahmed, Nova Ahmed, Faheem Hussain, and Neha Kumar. 2016. Computing Beyond Gender-imposed Limits. In *Proc. LIMITS'16*. ACM, Article No. 6.

[4] Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Md. Foysal Hossain, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proc. ICTD'16*. ACM, Article No. 11. http://dx.doi.org/10.1145/2909609.2909661

[5] Syed Ishtiaque Ahmed, Md. Romael Hoque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proc. CHI'17*. ACM.

[6] Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md. Rashidujjaman Rifat, A. S. M. Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A Platform for Fighting Sexual Harassment in Urban Bangladesh. In *Proc. CHI'14*. ACM, 2695–2704.

[7] Syed Ishtiaque Ahmed, Steven J Jackson, Maruf Zaber, Mehrab Bin Morshed, Md. Habibullah Bin Ismail, and Shamim Afrose. 2013. Ecologies of Use and Design: Individual and Social Uses of Mobile Phones Within Low-Literate Rickshaw-Puller Communities in Urban Bangladesh. In *Proc. DEV-4*. ACM, 14:1–14:10.

[8] Syed Ishtiaque Ahmed, Nusrat Jahan Mim, and Steven J Jackson. 2015. Residual Mobilities: Infrastructural Displacement and Post-Colonial Computing in Bangladesh. In *Proc. CHI'15*. ACM, 437–446.

[9] Syed Ishtiaque Ahmed, Maruf 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 *Proc. DEV'15*. ACM, 95–103.

[10] Android Central. 2017. Lollipop Brings Proper Multi-user Accounts to Your Phone. https://www.androidcentral.com/lollipop-brings-proper-multi-user-accounts-your-phone. (2017). [Online; accessed July 10, 2017].

[11] Thierry Bardini and August T. Horvath. 1995. The Social Construction of the Personal Computer User. *Journal of Communication* 45, 3 (1995), 40–66. http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.1995.tb00743.x/abstract

[12] Shaowen Bardwell. 2010. Feminist HCI: Taking Stock and Outlining an Agenda for Design. In *Proc. CHI'10*. ACM, 1301–1310.

[13] Shaowen Bardwell and Jeffrey Bardzell. 2011. Towards a Feminist HCI Methodology: Social Science, Feminism, and HCI. In *Proc. CHI'11*. ACM, 675–684.

[14] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A. Brewer. 2011. Computing Security in the Developing World: A Case for Multidisciplinary Research. In *Proc NSDR'11*. ACM, New York, NY, USA, 39–44. https://doi.org/10.1145/1999927.1999939

[15] Seyla Benhabib. 2002. *The Claims of Culture: Equality and Diversity in the Global Era*. Princeton University Press.

[16] Jenna Burrell. 2010. Evaluating Shared Access: Social Equality and the Circulation of Mobile Phones in Rural Uganda. *Journal of Computer Mediated Communication* 15, 2 (2010), 230–250.

[17] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *Proc. SOUPS'14*. 129–142.

[18] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2007. Graphical Password Authentication Using Cued Click Points. In *Proc. Computer Security-ESORICS*. 359–374.

[19] Padma Chirumamilla and Joyojeet Pal. 2013. Play and Power: A Ludic Design Proposal for ICTD. In *Proc. ICTD'13*. ACM, 25–33.

[20] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-methods and Multinational Study. In *Proc. CSCW'16*. ACM, 503–514.

[21] Julie E. Cohen. 2012. What Privacy is For. *Harvard Law Review* 125 (2012), 1904.

[22] Raymundo Cornejo, Robin Brewer, Caroline Edasis, and Anne Marie Piper. 2016. Vulnerability, Sharing, and Privacy: Analyzing Art Therapy for Older Adults with Dementia. In *Proc. CSCW'16*. ACM, 1572–1583.

[23] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking "Privacy" for a Networked World. *Proc. CSCW'17*, 1–36.

[24] Lorrie F Cranor and Simson Garfinkel. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE Security & Privacy* 2, 5 (2004), 16–18.

[25] Nicola Dell, Trevor Perrier, Neha Kumar, Mitchell Lee, Rachel Powers, and Gaetano Borriello. 2015. Digital Workflows in Global Development Organizations. In *Proc. CSCW'15*. ACM, 1659–1669.

[26] Paul Dourish and Leysia Palen. 2003. Unpacking Privacy for a Networked World. In *Proc. CHI'03*. ACM, 129–136.

[27] Casey Fiesler, Michaelanne Dye, Jessica L Feuston, Chaya Hiruncharoenvate, Clayton J Hutto, Shannon Morrison, Parisa Khanipour Roshan, Umashanthi Pavalanathan, Amy S Bruckman, Munmun De Choudhury, et al. 2017. What (or Who) Is Public?: Privacy Settings and Social Media Content Sharing. In *Proc. CSCW'17*. 567–580.

[28] Ralph Gross and Alessandro Acquisti. 2005. Information Revelation and Privacy in Online Social Networks. In *Proc. Workshop on Privacy in the Electronic Society*. ACM, 71–80.

[29] Jürgen Habermas. 1991. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. MIT Press.

[30] Richard Heeks. 2012. IT Innovation for the Bottom of the Pyramid. *Commun. ACM* 55, 12 (2012), 24–27.

[31] Geert Hofstede. 1984. The Cultural Relativity of the Quality of Life Concept. *Academy of Management Review* 9, 3 (1984), 389–398.

[32] Roberto Hoyle, Srijita Das, Apu Kapadia, Adam J Lee, and Kami Vaniea. 2017. Viewing the Viewers: Publishers' Desires and Viewers' Privacy Concerns in Social Networks. In *Proc. CSCW'17*. 555–566.

[33] Faheem Hussain and Mashiat Mostafa. 2016. Digital Contradictions in Bangladesh: Encouragement and Deterrence of Citizen Engagement via ICTs. *Information Technologies & International Development* 12, 2 (2016), 47.

[34] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E Grinter. 2012. Postcolonial Computing: A Lens on Design and Development. In *Proc. CHI'10*. ACM, 1311–1320.

[35] Steven J Jackson and Laewoo Kang. 2014. Breakdown, Obsolescence, and Reuse: HCI and the Art of Repair. In *Proc. CHI'14*.

[36] Steven J Jackson, Alex Pompe, and Gabriel Krieshok. 2011. Things Fall Apart: Maintenance, Repair, and Technology for Education Initiatives in Rural Namibia. In *Proc. iConference'11*. 83–90.
[37] Haiyan Jia, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proc. CSCW'15*. ACM, 583–599.
[38] Gopinaath Kannabiran. 2014. Ecofeminism and Sustainable HCI. In *Companion Proc. DIS'14*. ACM, 185–190.
[39] Naveena Karusala and Neha Kumar. 2017. Women's Safety in Public Spaces: Examining the Efficacy of Panic Buttons in New Delhi. In *Proc. CHI'17*. ACM, 3340–3351.
[40] Neha Kumar. 2011. The Gender-technology Divide or Perceptions of Non-use? *First Monday* 11 (2011).
[41] Priya Kumar and Sarita Schoenebeck. 2015. The Modern Day Baby Book: Enacting Good Mothering and stewarding Privacy on Facebook. In *Proc. CSCW'15*. ACM, 1302–1312.
[42] Ponnurangam Kumaraguru and Lorrie F Cranor. 2006. Privacy in India: Attitudes and Awareness. *Privacy Enhancing Technologies* (2006), 243–258.
[43] Carolyn A Lin. 1998. Exploring Personal Computer Adoption Dynamics. *Journal of Broadcasting & Electronic Media* 42, 1 (1998), 95–112.
[44] Silvia Lindtner, Bonnie Nardi, Yang Wang, Scott Mainwaring, He Jing, and Wenjing Liang. 2008. Emerging Sites of HCI Innovation: Hackerspaces, Hardware Startups and Incubators. In *Proc. CSCW'08*. ACM, 371–382.
[45] Heather R Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer, and Jason Watson. 2009. Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites. In *Proc. CSE'09*, Vol. 4. IEEE, 985–989.
[46] Jane Mansbridge. 1983. *Beyond Adversary Democracy*. University of Chicago Press.
[47] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. In *Proc. CSCW'17*. ACM, 581–593.
[48] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. 2017. When the Internet Goes Down in Bangladesh. In *CSCW*. 1591–1604.
[49] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Wash L. Rev* 79, 119 (2004).
[50] Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press. https://mitpress.mit.edu/books/obfuscation
[51] Tapan S Parikh and Koushik Ghosh. 2006. Understanding and Designing for Intermediated Information Tasks in India. *IEEE Pervasive Computing* 5, 2 (2006), 32–39.
[52] Andrew Patrick and Steve Kenny. 2003. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-computer Interactions. In *Privacy Enhancing Technologies*. Springer, 107–124.
[53] Jennifer A Rode. 2011. A Theoretical Agenda for Feminist HCI. *Interacting with Computers* 23, 5 (2011), 393–400.
[54] Norman Sadeh, Jason Hong, Lorrie F Cranor, Ian Fette, Patrick Kelley, Madhu Prabakar, and Jinghai Rao. 2009. Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. *Personal and Ubiquitous Computing* 13, 6 (2009), 401–412.
[55] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated Technology Use in Developing Communities. In *Proc. CHI'10*. ACM, 2583–2592.
[56] Ferdinand David Schoeman. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press.
[57] Amartya Sen. 1999. *Development as Freedom*. Oxford University Press.
[58] Claude E Shannon. 2001. A Mathematical Theory of Communication. *ACM SIGMOBILE Mobile Computing and Communications Review* 5, 1 (2001), 3–55.
[59] Stephanie B. Steinhardt, Amanda Menking, Ingrid Erickson, Andrea Marshall, Asta Zelenkauskaite, and Jennifer Rode. 2015. Feminism and Feminist Approaches in Social Computing. In *Proc ACM CSCW'15*. ACM, 303–308.
[60] Tech Crunch. 2017. Why Android Jelly Bean 4.2's Multiple User Account Switching Is Tablet-Only? (Hint: Nokia Patented It For Phones). https://techcrunch.com/2012/10/29/why-android-jelly-bean-4-2s-multiple-user-account-switching-is-tablet-only-\hint-nokia-patented-it-for-phones. (2017). [Online; accessed July 10, 2017].
[61] David R Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2 (2006), 237–246.
[62] Ronald L Thompson, Christopher A Higgins, and Jane M Howell. 1991. Personal Computing: Toward a Conceptual Model of Utilization. *MIS quarterly* (1991), 125–143.
[63] Peter Tolmie, Andy Crabtree, Tom Rodden, James Colley, and Ewa Luger. 2016. "This Has to Be the Cats": Personal Data Legibility in Networked Sensing Systems. In *Proc. CSCW'16*. ACM, 491–502.
[64] Michalis Vitos, Julia Altenbuchner, Matthias Stevens, Gillian Conquest, Jerome Lewis, and Muki Haklay. 2017. Supporting Collaboration with Non-Literate Forest Communities in the Congo-Basin. In *Proc. CSCW'17*. 1576–1590.
[65] Alan F Westin. 1968. Privacy and Freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
[66] Pamela Wisniewski, AKM Islam, Bart P Knijnenburg, and Sameer Patil. 2015. Give social Network Users the Privacy They Want. In *Proc. CSCW'15*. ACM, 1427–1441.

[67] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Preventative vs. Reactive: How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proc. CSCW'15*. ACM, 302–316.
[68] Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2014. Adolescent Online Safety: The Moral of the Story. In *Proc. CSCW'14*. ACM, 1258–1271.
[69] Susan P Wyche, Cliff Lampe, Nimmi Rangaswamy, Anicia Peters, Andrés Monroy-Hernández, and Judd Antin. 2014. Facebook in the Developing World: The Myths and Realities Underlying a Socially Networked World. In *Proc. CSCW'14*. ACM, 121–124.
[70] Iris Marion Young. 2011. *Justice and the Politics of Difference*. Princeton University Press.
[71] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proc. CSCW'16*. ACM, 1676–1690.
[72] Mary Ellen Zurko and Richard T Simon. 1996. User-centered Security. In *Proc. Workshop on New Security Paradigms*. ACM, 27–33.

Received June 2017; revised July 2017; accepted November 2017