Mahdi Nasrullah Al-Ameen*, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna

"We, three brothers have always known everything of each other": A Cross-cultural Study of Sharing Digital Devices and Online Accounts

Abstract: Although many technologies assume that a device or an account would be used by a single user, prior research has found that this assumption may not hold true in everyday life. Most studies conducted to date focused on sharing a device or account with the members in a household. However, there is a dearth in existing literature to understand the contexts of sharing devices and accounts, which may extend to a wide range of personal, social, and professional settings. Further, people's sharing behavior could be impacted by their social background. To this end, our paper presents a qualitative study with 59 participants from three different countries: Bangladesh, Turkey, and USA, where we investigated the sharing of digital devices (e.g., computer, mobile phone) and online accounts, in particular, financial and identity accounts (e.g., email, social networking) in various contexts, and with different entities - not limited to the members in a household. Our study reveals users' perceptions of risks while sharing a device or account, and their access control strategies to protect privacy and security. Based on our analysis, we shed light on the interplay between users' sharing behavior and their demographics, social background, and cultural values. Taken together, our findings have broad implications that advance the PETS community's situated understanding of sharing devices and accounts.

Keywords: Privacy, Interview, Cross-cultural Study, Digital Devices, Online Accounts, Shared Use

DOI 10.2478/popets-2021-0067
Received 2021-02-28; revised 2021-06-15; accepted 2021-06-16.

***Corresponding Author: Mahdi Nasrullah Al-Ameen:** Utah State University, E-mail: mahdi.al-ameen@usu.edu
Huzeyfe Kocabas: Utah State University, E-mail: huzeyfe.kocabas@aggiemail.usu.edu
Swapnil Nandy: Jadavpur University, E-mail: swapnilnandy2@gmail.com
Tanjina Tamanna: University of Dhaka, E-mail: turnatatatu666@gmail.com

1 Introduction

With the increasing use of computing technologies, people have been exposed to a variety of privacy issues and security vulnerabilities [48, 70, 71, 82]. Many technologies have been developed based on the assumption that they will be used by a single person. This 'single user' assumption is also reflected in the authentication solutions, where entering a password gives access to all of the contents in a digital device (e.g., computer, mobile phone), or an online account. However, the one-to-one mapping between a technology and a user does not consider the security vulnerabilities and privacy risks for people when they share their devices or accounts with others.

We adopt the definition of *sharing* from existing literature [4, 52], referring to any situation in which multiple people use a single device or account, either synchronously or asynchronously. The prior works examined the sharing of digital devices in a household setting, including mobile phone [15, 19], computer that is located in a public space at home [18], and IoT devices [34]. A recent study [52] looked into the sharing of an online account with the members in a household, e.g., an entertainment account to watch movies. Several studies examined the needs of sharing devices and accounts with caregivers (e.g., parents, spouse) by the people with visual impairments or certain disabilities [41, 73], and explored the usability and privacy challenges of sharing devices with the children in a household [18, 51].

We extend the findings from existing literature through addressing the following research questions: **RQ1:** What are the contexts and reasons of sharing digital devices and online accounts when the sharees include not only the members in a household, but also others in a wide-range of personal, social, and professional settings? **RQ2:** What are the risk perceptions, and concerns of users as they share their devices and accounts? **RQ3:** What are the access control strategies

of users in the process of sharing their digital devices and online accounts?

To address the above research questions, we conducted semi-structured interview with 59 participants from three different countries. The studies around privacy have predominantly been influenced by Western liberal values, including the early work of Warren and Brandeis [80], and Westin's call for freedom from surveillance [83], where a large body of prior works examined the privacy issues in the USA. However, the recent literature [24, 59, 62] suggest that privacy is contextual, where we need a situated understanding to explore the design and policy practices; the studies [3, 5, 6, 8, 38, 76] conducted in Bangladesh (a developing country located in South Asia) demonstrated the importance of focusing more on digital technology users and privacy issues in developing countries. To this end, we included both USA, and Bangladesh in our study. We also included Turkey – a developing country straddling Eastern Europe and Western Asia. Turkey is one of the underrepresented countries in privacy literature, while several studies [9, 20, 27] highlighted the significance of examining privacy issues in regions that are less studied in prior works. As a whole, our findings contribute to the situated understanding of contexts, privacy risks and concerns, and the privacy behavior of users as they share devices and accounts with different entities (not limited to the members in a household).

In this paper, the term *digital device* or *device* refers to the computer and mobile phone, unless otherwise specified. For online accounts, we focused on the sharing of financial and identity accounts (e.g., email, social networking), considering the sensitivity of user information stored in these accounts *.

1.1 Contributions and Key Findings

In this section, we first provide insights into our contributions on the contexts and reasons of sharing digital devices and online accounts (**RQ1**; see §5.1 for details).

Our findings present new sharing contexts that are less explored in prior studies, including *Geographic relocation* (§5.1.1): The geographic relocation may lead users, including the immigrants to collaborate with friends and family members in their native country to manage financial, and identity accounts (e.g., email, social networking); & *Collaborative social networking* (§5.1.5): The relatively older, or less-educated users in Bangladesh collaboratively use a single social networking account, where they help each other to maintain an online presence, address technical issues, learn to use new features, and recall password if forgotten.

We extend the findings from prior studies with respect to multiple sharing contexts, including *Trust and affection* (§5.1.3): While the trust on family members make people comfortable with sharing devices [37, 52], we also found instances of sharing devices and online accounts as a way of building trust with romantic partners, to express affection to friends, as well as to maintain transparency in a conjugal life. In Bangladesh, it might come as a natural expectation and event for the people that they would share personal devices and accounts with a 'close' group of peers with whom a person has grown up since childhood; & *Intermediate help* (§5.1.7): The prior studies [7, 41, 52, 73] reported the sharing of passwords with family members (e.g., spouse, parents) while taking help with device or account management. We found that our relatively older, or less-educated participants from Bangladesh share their passwords (or ask to create one for them) for online accounts not only with their family members, but also with colleagues, and friends while taking help with account creation and management.

Our results show differences across countries on the extents of sharing (e.g., with whom a device or account is shared) in the contexts of *Collaborative financial management* (§5.1.2), where the sharing of a financial account depends upon family structure and dynamics; & *Sharing the same physical space* (§5.1.4), where the possession of a device may not be constrained by a physical boundary once that is shared with household members in Bangladesh and Turkey. We found that the context of sharing could be specific to a country. For instance, in the process of business management and providing informal services at digital service centers in Bangladesh, the owner's identity account (e.g., email account), and admin-computer are shared not only with the employees but also with customers (§5.1.6). The sharing context could be also specific to the groups of users in a country, e.g., collaborative social networking among relatively older, or less-educated users in Bangladesh (§5.1.5).

In prior studies [18, 34, 52] that focused on people's sharing behavior at home, the participants seldom voiced concerns about sharing devices or accounts with their family members. In our study, we revealed peo-

* The study of Haque et al. [39] divided online accounts into four categories (e.g., financial, identity, content, and sketchy), where the authors emphasized on the protection of financial, and identity accounts (e.g., email, social networking).

ple's risk perceptions and concerns where the sharing of a device or account is not limited to the household members (**RQ2**; see §5.2 for details). Our participants reported a wide range of concerns with sharing devices and accounts, which include loss and leakage of personal information and credentials, because of careless use or unauthorized access by a sharee (§5.2.1); misuse of devices, where the consequences may not be limited to privacy violation, and embarrassment in personal and professional scenarios, but also raise the question of legality and socially accepted behavior (§5.2.2); and change in relationship with the sharee, leading to blackmailing, and damaging reputation (§5.2.3). We unveiled participants' privacy concerns about *secondary sharing*, where the sharees of an online account share the login credentials with other entities without informing the primary sharer, i.e., owner of that account. Our analysis shed light on the privacy and social issues that could emerge when the expectations of a sharer is not well communicated to the sharees, where the differences in societal background between the sharer and sharee could exaggerate the misunderstanding of expectations in the collaborative use of a device or account.

As we looked into our participants' access control strategies while sharing a digital device or online account (**RQ3**; see §5.3 for details), we identified that the privacy-preserving behavior of a user might not be triggered by her risk perceptions, where only in a few cases, we found a relation between the user's privacy behavior and risk perceptions. Most of our participants do not take any steps to protect their privacy while sharing a device or account, where the reasons reported by our participants confirm several findings from existing literature to hold true in the contexts of sharing devices and accounts both within and outside of Western contexts, including lack of knowledge [2, 81], optimism bias [81, 90], and procrastination until harms occur [90]. Further, we identified a blind trust on technology in protecting user information that makes our participants from Bangladesh and Turkey not taking any privacy-preserving actions. Our study unpacked the adhoc based strategies adopted by users for privacy protection while sharing a device or account, where we found that some of these approaches could pose privacy risks for sharees, fail to protect the security and privacy for sharers, and bring further security risks for them.

2 Background: Bangladesh and Turkey

In this section, we provide a brief overview of the countries, where we recruited participants outside of the USA.

Bangladesh, officially the People's Republic of Bangladesh is located in South Asia. Bangladesh is one of the most densely populated countries in the world with a population of above 164 million [84]. Bangladesh is a developing country, according to the classification by United Nations [58], where the GDP per capita (US$) is 1855.7 as of 2019 [11]. According to the data from the World Bank [12], Bangladesh has a literacy rate of 75% as of 2019. 'Bengali' is the official language of Bangladesh [84]. Family and kinship are the core of social life in Bangladesh [40, 43]. The family unit in Bangladesh, which provides economic stability and a form of social identity to the people, usually consists of a husband and wife, their unmarried children, their adult sons with their wives and children, and the grandparents [40, 43].

Turkey, officially the Republic of Turkey, is a transcontinental country straddling Eastern Europe and Western Asia. As of 2019, the population of Turkey is around 82 million [85]. According to the classification by United Nations [58], Turkey is a developing country, where the GDP per capita (US$) is 9,126.6 as of 2019 [11]. Turkey has a literacy rate of 96% as of 2017, according to the data from the World Bank [12]. 'Turkish' is the official language of Turkey [85]. In general, Turkish family can be characterized as "functionally extended", where several nuclear families of relatives live close to each other, maintain strong social ties and interactions, and function as if they were extended [77]. Both male and female children live with their parents until they get married, where individuals frequently interact with a wide network of relatives, including grandparents, aunts, uncles, and cousins [13, 77].

3 Related Work

3.1 Taxonomy of Sharing

The study of Derlega and Chaikin [26] demonstrates that self-disclosure can be classified on a breadth dimension, which depends upon several different areas in an individual's life that are revealed in communication.

Here, an individual may feel comfortable to share information only with a closed group of people, while others might prefer to keep everything to themselves. Such preferences and behavior create the boundary of information disclosure, which often relate to the varying social relationship of an individual with the surrounding people [26]. These findings are supported by the study of Johnson et al. [47] in the context of users' sharing preferences on social media. The study [47] highlights the complicated sharing behavior of users in an online social networking site, influenced by multiple factors including trust, and relationship with peers. The authors [47] presented a hierarchy of sharing preference based on the user's comfort level, where they are most comfortable sharing personal information with immediate or extended family members, close friends, and people whom they frequently socialize with, followed by coworkers, acquaintances, and strangers. In a separate study, Wisniewski et al. [87] examined users' information sharing behavior on online social networking sites (SNS), where they created a framework representing users' coping strategies on social media through filtering, ignoring, blocking, withdrawal, aggression, compliance, and compromise. The study [87] showed that users develop these strategies, in addition to using traditional SNS privacy controls, in order to attain the desired level of privacy while interacting, and sharing information on social media.

The sharing of mobile phone with family members is common among users [15, 19], where Steenson and Donner [74] described two categories of sharing: proximate (multiple close relations use a single phone), and distributed (person X calls person Y to reach person Z, who may not have a phone). The study of Brush and Inkpen [18] found that family members share a computer located in a public space at their home. In a shared computer, the family members frequently use each other's OS-level profile, and switch to their individual profile only when they intend to complete a task that demands some degree of privacy and personalization [29].

The practices of sharing digital devices with family members are influenced by two primary factors: trust in sharees, and convenience [37, 52], where Matthews et al. [52] found that people underestimate the frequency of sharing a device with the members in their household. The authors [52] divided such sharing in a household setting into multiple categories, which include borrowing (e.g., temporary lending of a digital device that benefits the sharee), mutual use (e.g., multiple inhabitants in a household regularly use the same device), helping the sharer with setup and use, broadcasting (e.g., watching a movie with family members), and accidental (e.g., unintentional access by a member in the household). In a separate study, Geeng and Roesner [34] examined the interaction of people in a multi-user smart home, where they found two categories of users for shared devices: smart home driver and passive user. Here, a smart home driver takes initiative to learn about and use smart devices, where a passive user adapts to device usage and rely on the smart home driver to control functionality and fix technical issues of the shared devices in a household [34].

The study of Mazurek et al. [53] investigated the perceptions and behavior of household members in controlling access to digital contents within their home environment. The authors [53] found that the ad-hoc access control techniques adopted by users may not alleviate their privacy concerns. In this regard, the ideal access control policies could be complicated considering the entities who access, the locations where access occurs, the device that is accessed, and requiring users to deal with the social model of politeness and permission [53]. In a follow-up study, Mazurek et al. [54] examined whether and how a reactive model could contribute to making access control more usable in a home setting, where users can dynamically update their policy in response to access requests. The study [54] showed that the reactive model could offer dynamic, situational access-control policies, and effectively support users' needs in policy creation in terms of control and interactivity.

In the present era, children are the active users of digital devices in a household [51, 52], where Livingstone et al. [51] explored how the sharing of a device with children relates to the people's socio-economic background, education, and parenting style. The authors [51] found that even though parents choose to share their devices with the children, there lacks suitable features to preserve their privacy, and provide a safe browsing environment for the children. The study of Brush and Inkpen [18] shows that the trust on family members while sharing a device does not always extend to 'parent-child' relationship, where Frohlich and Kraut [33] found that parents log into their children's accounts on a shared device to monitor their activity.

People may share passwords while sharing digital devices with their family members [21, 52]. The study of Hayes et al. [41] explored the privacy and security requirements of the people with visual impairments, where the participants reported taking help from their spouse to manage their passwords for online accounts. The find-

ings from this study [41] are in line with that of Tousif et al. [7], which reveals that the people with visual impairments struggle with password management, e.g., correctly typing a password. In another study, Singh et al. [73] found that people with certain disabilities take help from their caregivers (e.g., parents) to manage their passwords.

3.2 Situated Privacy and Security

Privacy is contextual that demands a situated understanding of users' perceptions and behavior in order to explore the design and policy practices [24, 59, 62]. The findings from recent usable privacy studies [3, 8, 20] support this argument that local values often contrast with the liberal notions of privacy embedded in current computing systems. However, the digital privacy research beyond Western contexts and a liberal framing is still at its very early stage [22, 79]. Below, we briefly discuss the notable usable privacy studies conducted outside the Western contexts.

Although online threats are global, perceptions of threat are very localized [8, 20, 38, 50]. The study of Al-Ameen et al. [8] explored how the privacy perceptions of people relate to their effort to deal with the issues of urbanization and the opportunities that come with digitization in the Global South. The authors [8] examined how users balance their needs, conveniences, and privacy in the context of data collection and sharing by apps, and unveiled how privacy leakage incidents affect app usage behavior. The study of Haque et al. [38] presented how clientelization, reputation, and situated morality influence the privacy behavior of people in the digital service centers at Bangladesh. In another study, Chen et al. [20] investigated the security and privacy practices of the people in urban Ghana while browsing Internet. The study [20] shows that participants judge the trustworthiness of a website based on the appearance, lack of popups, and loading speed, where they reported confidence of being able to defend against cyberattacks despite passwords often being their only line of defense.

The religious views and cultural norms of people have impacts on their sense of confidentiality and privacy. The study of Alghamdi et al. [9] investigated the privacy and security practices for households bank customers in Saudi Arabia, showing that trust, driving restrictions, and the esteem placed in family motivate female participants to share their banking information with male family members, including their father, and husband. The study of Abokhodair et al. [1] examined how the youth in the middle east conceptualize values such as privacy, intimacy, and freedom of expression in the context of social media. The authors [1] found that the interpretation of privacy among participants goes beyond the concerns for security, safety, and having a control to separate oneself from a larger group, where they observed adherence to Islamic teachings, maintenance of reputation, and the careful navigation of activity in social media to preserve respect and modesty.

Digital harassment is a growing concern in many developing countries, wherein the majority of cases female users are the victims of such incidents [6, 60]. The study of Nova et al. [60] reveals the online harassment that women in Bangladesh encounter while using anonymous social media (ASM). Participants reported receiving sexually offensive messages and dating inquiries from the people in ASM. While public discussion on sex or any topic containing sexual content are considered taboo and frowned upon in Bangladesh [57, 64], the curtain of anonymity in ASM provides a safer way to break these invisible norms of society without being judged or scrutinized. In another study, Sambasivan et al. [68] identified that the risks and fear of harassment refrained the women in urban India to provide their phone number for accessing public Wi-Fi services.

Digital devices, such as mobile phones that are designed for developing regions often fail to satisfy their local needs. In a study conducted with low-literate Berber women in Morocco [27], the authors examined the gap between high rates of mobile phone ownership and low use of productive features - noted as 'mobile utility gap'. The study identified that lack of functional literacy and non-standard mobile phone interface including a complex language environment with both Arabic and Berber dialects presented significant barriers to using mobile phones, which contributed to the mobile utility gap in that community. The studies conducted by Ahmed et al. [5] and Sambasivan et al. [67] demonstrate that the mobile phones often do not have one-to-one mapping with a user in the resource-constrained settings of developing countries, while the social fabric in these societies is based on the notions of trust and collectivism. Thus, the strict privacy requirements in using digital technology could disrupt the relationships with friends and family members [5, 67]. In a separate study with women in Global South [66], the authors explored the privacy negotiation of female users from their family members while using a mobile phone.

Gender	Participants
Male	BP1-BP3, BP6-BP9, BP11, BP15, BP17-BP29, UP1-UP4, UP7, UP8, UP10-UP12, UP14-UP16, UP18, UP20-UP22, TP1, TP3, TP4, TP6, TP8
Female	BP4, BP5, BP10, BP12-BP14, BP16, UP5, UP6, UP9, UP13, UP17, UP19, TP2, TP5, TP7
Age-range	
18-24	BP4, BP7, BP8, UP5, UP6, UP19, UP21, UP22
25-29	BP2, BP3, BP5, BP6, BP9, BP19, BP20, BP25, UP2, UP7-UP15, UP18, UP20, TP1-TP3
30-34	BP1, BP17, BP18, BP21, BP24, BP28, UP1, UP3, UP16, UP17
35-39	BP23, TP6
40-44	BP16, BP22, BP26, BP27, BP29, UP4
45-49	BP14, TP4, TP7
50-54	BP15, TP5, TP8
55+	BP10, BP11, BP12, BP13
Literacy Level*	
Fifth Grade	BP19, BP27, BP29, TP6, TP7
Between Eighth and Tenth Grade	BP17, BP20, BP22, BP24, BP25, BP26, BP28, TP4
Twelfth Grade	BP12, BP18, BP21, BP23, UP19, UP21, UP22, TP2, TP5, TP8
Undergraduate and above	BP1-BP11, BP13-BP16, UP1-UP18, UP20, TP1, TP3
Profession	
Student	BP4, BP5, BP7, BP9, UP1-UP3, UP6-UP14, UP18, UP19, UP22
Employee at Industry	BP1-BP3, BP6, BP8, BP11, BP17-BP19, BP21-BP29, UP5, TP3, TP4, TP6
Employee at Educational or Non-profit Org.	BP10, BP15, UP4, UP15-UP17, UP20, UP21, TP1
Car Driver	BP20
Housewife	BP12-BP14, TP2, TP5, TP7
Physician	BP16
Retired	TP8

Table 1. The Highlight of Participants' Demographic Traits [*Either completed or currently studying at the noted education level]. **Notes:** *UP*: Participants living in the USA; *BP*: Participants living in Bangladesh; *TP*: Participants living in Turkey. Five U.S. participants (UP3, UP6, UP13, UP17, UP20) are the first-generation immigrants, who are originally from the countries in Asia.

Our Study. The overall findings from these studies indicate that the misconceptions about local culture by developers or designers may result in inappropriate threat modeling, where there is a dearth in existing literature to understand the contexts, risk perceptions, and access control strategies of users as they share their digital devices and online accounts not only with the members in their households, but also with others in various personal, social, and professional settings. We addressed this gap in our work, where we conducted a study with the participants from both developing (e.g., Bangladesh, Turkey) and developed (e.g., USA) countries.

4 Methodology

We conducted semi-structured interview with 59 participants. In preparing the questionnaire for interview, the authors of this paper conducted several rounds of focus group discussion. We also gathered feedback from the colleagues at our labs. We improved the structure and clarity of questionnaire based on our focus group discussion, and the feedback from our lab members. Our study was approved by the Institutional Review Board (IRB) at our university.

4.1 Participant Recruitment

We recruited adult participants in this study, where anyone above 18 years (self-reported) could participate. We recruited participants through posting flyers on college campuses, neighborhoods, restaurants, and other public places. We shared recruitment messages on our social media profiles with 'public setting'; re-shared by many others. We reached out to participants through email listservs of social clubs, and local communities. We also used snowball sampling, recruiting a few participants from the recommendation of participants who had taken part in this study.

Our recruitment materials (e.g., flyer, email, social media post) specified that the study is about a user's perceptions and experiences on sharing digital devices and online accounts, where we did not do any additional pre-screening based on a participant's sharing experience.

4.2 Procedure

We interviewed the participants over telephone, via Skype, or in person. We conducted interviews in the country's official language. That is, the interviews with the participants living in the USA, Bangladesh, and Turkey were conducted in English, Bengali, and Turkish, respectively. During the interview, participants responded to a set of questions on sharing digital devices (e.g., computer, smartphone) and online accounts, in particular, financial and identity accounts (e.g., email, social networking). We asked them about the contexts of sharing devices and accounts, whom they share with, their concerns, negative experiences, and the strategies they use to protect personal information in the process of sharing. At the end, participants responded to demographic questionnaire. We audio recorded the interviews. On average, each session took between 25 and 35 minutes.

4.3 Analysis

We transcribed the audio recordings. For the interviews with the participants from Bangladesh and Turkey, the researchers who are the native speaker of Bengali and Turkish translated the transcriptions into English. We then performed thematic analysis on our transcriptions [16, 17]. Two researchers independently read through the transcripts of half of the interviews, developed codes, compared them, and then iterated again with more interviews until we had developed a consistent codebook. Once the codebook was finalized, two researchers divided up the remaining interviews and coded them. After all interviews had been coded, both researchers spot-checked the other's coded transcripts and did not find any inconsistencies. Finally, we organized and taxonomized our codes into higher-level categories. The inter-rater reliability (Cohen's Kappa) of the raw agreement between two coders was 0.87.

4.4 Participants

Table 1 presents the demographic information of our 59 participants, where 16 of them are women, and 43 are men. Almost all of our participants were in the age range of 18 to 55, where four participants were above 55 years old. The literacy level of 39% of our participants was between fifth and twelfth grade, where others were either undergraduate students or had already earned the degree. Thirty-two percent of our participants were students, where others were from diverse professions, including physician, car driver, housewife, and the employee at industry, educational institution, or non-profit organization. Among our participants, twenty two of them live in the USA, eight participants live in Turkey, and 29 participants live in Bangladesh. In this paper, the participants living in the USA, Bangladesh, and Turkey are denoted by *UP*, *BP*, and *TP*, respectively.

5 Results

In this section, we present our findings on the contexts and reasons of sharing digital devices and online accounts (§5.1), risk perceptions of users (§5.2), and their strategies of access control with regard to such sharing (§5.3). For consistency, we use these terms based on the frequency of comments in participants' responses: *a few* (0-10%), *several* (10-25%), *some* (25-40%), *about half* (40-60%), *most* (60-80%), and *almost all* (80-100%).

5.1 Contexts and Reasons of Sharing

5.1.1 Geographic Relocation

Several participants, including our immigrant participants in the USA have reported that when they travel to a different country from their primary location, they

face challenges to log into their online accounts, and their ability to access desired features in an account gets limited. In these circumstances, our participants reach out to their friends or family members living in their primary location (e.g., their home country) to avail help with making a financial transaction, recovering an email account, or updating the settings and features in a social networking account.

Many service providers block suspicious login attempts from unusual location to protect their users' online accounts from an unauthorized access. In such cases, a user might be asked to prove her identity by entering a one-time-code delivered to her phone number, registered with the system [30]. We found that such security measures could pose accessibility challenges to users, where a few participants lost access to their email account, as their phone number, used for two-factor authentication changed once they had relocated to a new country. To recover their account, they mailed the SIM card related to their old mobile phone number to a friend or family member in their native country, along with sharing the password for their email account. In another instance, one participant forgot the password for her email account after moving to the USA, and did not have a recovery email but a recovery mobile phone number that she used to use in her native country. She recovered her access to that email account through creating a new password in collaboration with a friend in her native country, whom she had to mail her old mobile SIM card.

UP13 is originally from a country in Asia, who currently lives in the USA. Upon moving to the USA, she could not access all of those features in her social networking account that she used to access in her native country. However, she has found a workaround to maintain her accessibility despite geographic relocation. She has shared her password for the social networking account with a few friends in her native country, whom she trusts (the participant mentioned them as 'close friends'). Whenever needed, UP13 requests one of her 'close friends' to make changes in her account on her behalf that she could not do from her current location.

The participants, UP3 and UP6 are originally from Iran (a country in Western Asia) and China (a country in East Asia), respectively, who currently live in the USA. They share their login credentials (e.g., username, password) for banking account with their spouse (UP3) or parents (UP6) living in their native country. UP6 believes, having direct access to her banking account would let her parents address any urgent financial needs with skipping the latency to reach out to her. UP3 mentioned, *"I need to have, for example, one person in Tehran whom I can trust, like my wife. Especially when I am not in Tehran, my hometown, but I need to transfer money from my account to another desired account, my wife does that for me."*

5.1.2 Collaborative Financial Management

Several participants share the login credentials of their bank account with family members to collaboratively manage the financial activities. With whom the bank account is shared depends upon the structure and dynamics of a family. The participants who are married and residing in the USA, live with their spouse in a nuclear family setting; UP11 and UP12 are among those participants. UP12 and his wife divide their role in managing financial activities, where his wife takes the responsibility of paying bills. He shares his login credentials for the bank account with his spouse so that she could log in and pay the bills on time. In the case of UP11, his wife takes the full responsibility for managing financial activities, where he mentioned, *"I share my bank account information with my wife because she is in charge of all the expenditure for the family. She gets the [bank] statement."*

Some of our participants from Bangladesh and Turkey live in an extended family (or 'functionally extended family' - see §2) setting, where several participants share their login credentials of the bank account with multiple family members. BP6, who is unmarried, shares his bank account details with his father and brother so that they could help with managing the expenditure for the family. Here, BP3 takes a more privacy-preserving approach towards managing his financial accounts, *"My family has a bank account which is created under my name and I deposit money in that account so that they can have that money. I also have my salary account which I don't share with anybody."*

A few participants mentioned having a contingency plan in case of an emergency situation, where they might not be able to access their bank accounts. So, they share their login credentials with their family members, especially spouse, so as to ensure accessibility to their financial accounts. UP10 said, *"Anything could happen! What? Let's say you die, and you have all of your money stacked in one place, nobody knows how to get it, and the money dies, you know there. So I think it's important [to share], especially with spouse."*

5.1.3 Token of Trust and Affection

We found instances where participants share their digital devices and online accounts to express affection for their trusted peers. For example, UP13 said, *"I do like to share [my smartphone] with them [partner, friends] because I love them."* Several participants consider the sharing of their devices and accounts as a way of building trust with their romantic partner; UP7 added, *"My password is my fiancée's name, so she already knows about it. I really trust her, we are together. So, for example, password of bank account is shared between us."*

The social networking sites are criticized for the negative impact on interpersonal relationship outcomes, including breakup, and divorce [31]. While transparency and trust between partners could help to avoid such unexpected outcomes, one of our participants (BP23) mentioned sharing his login credential for the social networking account with his wife, so that she could monitor his activity anytime she wants. Another participant (TP5) said, *"I don't have anything to hide from my husband, so I share everything."* As these participants perceive, such sharing and transparency help them to alleviate the complications in conjugal life that might come with the use of digital devices and online accounts.

A few participants from Bangladesh mentioned that they are used to sharing *"everything"* within a *close circle* since their childhood. This close circle comprises siblings, cousins, or friends with whom they have grown up. As they have stepped into using online accounts, it comes out as natural and expected to them that their login credentials would be shared within their close circle. For instance, BP20 shares his email account with his cousins, where he mentioned, *"We, three brothers have always known everything of each other."* Similarly, BP17 shares his social networking account with his friends, *"They are so trustworthy that I don't feel unsafe sharing the password [of social networking account] with them. I know their password and they know mine."*

5.1.4 Sharing the Same Physical Space

Several participants from Turkey and Bangladesh have stated that a digital device purchased by any of their family members is considered as a common property of the inhabitants at their home. TP8 believes that there should not be any expectations of personal privacy as it comes to helping the family members through sharing a laptop or smartphone. BP4, who lives with her extended family in Bangladesh, purchased a laptop; she explains the sharing of her laptop with the family members at her home, *"If someone needs to fill up [online] forms, they use my laptop to do that. If my brother needs to use his Facebook, he uses my laptop. And whenever anyone in my family needs any type of work on a computer, they use mine. My uncle buys ticket using it. My mother uses it for her official work."*

As shared, the possession of a digital device might not be constrained by a physical boundary; BP27 provided an example, *"When my brother goes to coaching class, he needs a mobile phone, so he borrows mine."* While such sharing is culturally expected in Bangladesh and Turkey, participants also referred to economic constraints in several instances, as to why they could not afford a separate device for individual family members. One of our participants mentioned, *"I think people like us need to share their devices because we can't afford to buy separate device for individual [family members]. I think, sometimes it is risky. One can access another person's information."*

Two of our participants (UP13 and UP17) who are originally from Asia, and currently live in the USA, reported that they used to share the smartphone and computer with their parents and siblings in their native country. They added, such sharing behavior contributed to their habituation and comfort with sharing digital devices with their spouse upon moving to the USA.

While living or working in a same physical space, the sharing of devices could extend beyond family members. For instance, BP8 lives in a city apart from his family, where he shares an apartment with few others; he mentioned sharing his computer with his roommates. UP11 reported a different scenario: He has got a licensed software on his computer at the workplace. The other computers do not have that software installed. So, he has to share his computer with his colleagues so that they could access that software as per their needs.

5.1.5 Collaborative Social Networking and Communication

In recent years, the use of online social networks has experienced a sharp rise in many developing countries, including Bangladesh [32, 76]. Not only the young and tech-savvy population, but also relatively older and less-educated users in Bangladesh have started to get the benefits of online social networking. Some of our relatively older, or less-educated participants from Bangladesh use the social networking site in a collaborative manner: They create and use one account, which

is shared among a small group of peers who trust each other. This small group generally consists of friends, colleagues, or family members.

BP22 learned how to use a social networking site with the help of friends in his group who collaboratively use a social networking account. BP11 has formed his collaborative group with colleagues and family members, where he relies on them to deal with the changes in features and interface of the social networking site. He also seeks help from his group when he forgets the password for their social networking account, or wants to change the privacy setting of his posts. BP12 sees two-way benefits in the collaborative use of a social networking account, *"I help them [her group] with their needs [in collaborative social networking]. They help me to understand the use of any features that I want to know from them."*

Many people in Bangladesh do not have a Wi-Fi access at home, where they rely on the pre-paid mobile Internet service [65]. As their data budget is exhausted, their access to the Internet gets blocked. In these circumstances, collaborative social networking helps them to keep their presence alive in social media. BP20 explained the reasons of sharing a social networking account with his cousins, *"To help each other. They [cousins] share photos and posts on my behalf while I am not around, and I do the same for them."*

The women in Bangladesh often encounter online harassment or have to deal with aggressive comments in their posts on social networking sites [6, 60]. As a workaround, when our participant, BP4, wants to make a post on any controversial issue, she uses her partner's social networking account. They also share two email accounts with each other, where one of them is for regular use, and the other account is used for registration at relatively unknown or less-trusted websites. Another participant (UP13) has mentioned that she often forgets to respond to the emails. So, she shares her email account with her husband, who reminds her to reply to emails on time.

5.1.6 Business Management and Informal Services

Among the participants from Bangladesh, several of them are the owner of, or employees at digital service centers that offer a variety of services to their customers, which include filling up an online application form for the job, visa, or academic admission, paying fees online, printing, photocopying, and sending emails. Here, the range of offered services may vary across these service centers [38]. Our participant, BP23, is the owner of a digital service center. He shares his email account with his employees and lets the customers use this account, where he mentioned, *"Employees access it [email account] for managing business related emails. Customers use it for sending documents to any other email ID."*. He also explained how they manage paying online fees for their customers, *"While customers need to make payment for visa, admission, or anything related to online fees, our shop's [debit/credit] card number is shared [with customers] based on their needs. The card number, expiry date, and CVV are printed and kept below a [transparent] desk so that the employees can easily access them."*

A few participants reported maintaining separate accounts for their business purpose and personal use. For instance, BP29 does not share his personal email account with his employees or customers. Rather, he has created a separate email account, which is shared with his employees to manage business related activities and with customers to offer the service of sending emails. One of our participants (BP17) runs a family business with his brother. He has two different bank accounts: one for business, and the other one for personal use. He provides his brother with the full access to the bank account used for their business. For his personal account, he shares the bank account number with his brother but does not share the password to access that account online.

In a digital service center, run by BP25, customers are provided with printing and photocopying services, where the shop-owner takes care of printing tasks for the customers from his computer with administrative privilege. Occasionally, customers are allowed to use this admin computer; our participant explained the scenarios, *"Sometimes the customer needs to edit their document before printing. Also, when the work pressure is low, we give them access to browse the Internet."* Here, Internet browsing is not one of their core services, rather offered to customers as an informal service if there is a scope.

5.1.7 Intermediate Help

Several participants from Bangladesh, who are relatively older, or less educated reported taking help from others with creating and managing their online accounts. In this process, a caregiver either created the password for them, or participants shared their authentication secrets with the caregiver. For instance, when BP27 first came to know about the online social network, he was

not quite sure about how to create an account. So, he reached out to one of his friends, who helped him with registering for Facebook and created a password for him; the participant added, *"I still use the same password (created by his friend)."*

In another instance, BP11 could not access some of the features at his bank account. So, he asked help from the IT support at his organization. In the process of getting help, he shared the password of his bank account with IT personnel, however, did not change his password afterward. Our participant, BP12, takes help from her grandson to deal with the technical issues in managing her email account. She said, *"My grandson knows everything, and he has created my email account. Whatever I want to know, I just ask him, and seek for any kind of help I need from him...My password is written in a diary and whenever I change it, I update the password in the diary as well. The diary remains on my desk, and anyone can look inside if they want."*

5.2 Risk Perceptions

5.2.1 Loss and Leakage of Personal Information

A few participants reported concern about multiple users using the same computer in their workplace, where a shared computer could be infected with malware if one of the users is not careful. UP17 mentioned her experience of losing data and files from a shared computer, *"When I was a graduate student in South Korea, I used to use a shared computer in our lab. Students had folder in their name to store project files. Unfortunately, one student used to use that computer for fun, watching video or like that. Then, the computer got some virus. So, we had to format the computer, and I lost all of my project files stored in that computer."*

UP16 is concerned about the privacy breach from his computer at the workplace. He shares the password of his desktop computer with his colleagues so that they could address their professional needs, like using a licensed software that is not installed in other computers. He used to keep his online accounts logged in, trusting his colleagues not to access them. However, one day, he found that one of his colleagues had logged him out of his email account, to log into his own account from that computer. The participant worried that his privacy might have been compromised due to the exposure of his personal emails to his colleague.

TP1 and TP3 store their passwords for online accounts in a file on their personal device, to address the memorability issues. They worried that an entity, with whom the device is shared, might accidentally delete that password file, and in turn, they would lose access to their online accounts. As a contingency plan, TP1 writes down his passwords on a physical notebook, too. Another participant (UP16) reported concern that the login credentials for his online accounts could be leaked to adversaries if the sharee of his accounts becomes a victim of the phishing attack; he added, *"I am actually concerned about online bank accounts, because I don't want to lose my money without my fault, and sometimes those accidents happen...when I decide to share my password and ID, I think the ID and the password go out of my control. Even though every person who shares my account is careful about that, you know, some [phishing] websites can steal the ID and password."*

Several participants referred to unpredictable human traits that could compromise their privacy when they share their personal devices. They told about their past experiences where they had shared their phone with a friend or family member to let them access a particular document or application, but later found that they had also accessed other personal files and apps. BP5 said, *"I shared my device [smartphone] with my friend to show some pictures from the gallery. But she breached my privacy and went into the applications like WhatsApp and Facebook."* BP2 reported a similar incident of privacy breach, *"One day I gave my phone to my younger brother for playing games. At that time, my Facebook account was logged in. He then accessed my [Facebook] account, and made some changes."*

In a digital service center, BP25 offers mobile phone repair services to the customers. He is concerned that the people are not careful enough in protecting their information when they share their personal device with a shopkeeper to avail the repair service. He mentioned, *"Customers have no option other than giving their device [mobile phone], unlocked to us. So, if we want, we can access all the important information of our customers, but we prefer not to. On average, if ten customers bring their device for repair, around three of them have all of their information stored in it."* In this context, one of the participants who works in a digital service center, reported an incident of unintentional privacy breach, *"One of my customers left his device for repairing. While repairing, I accidentally accessed some of his folders and saw some personal pictures which I should not have seen."* BP28 told about an unintentional privacy leakage from a shared computer at his home, *"Once my brother left his Facebook account logged in. When I was using the computer, I suddenly saw*

some personal pictures and messages of him and his wife. I logged out [from brother's account], but I felt very guilty."

5.2.2 Misuse of Shared Device and Account

Several participants are concerned that the entities, with whom they share their digital devices, might exploit them for a wrong or unethical purpose. A few of them reflected onto their experiences from the past, where BP14 shared an incident that did put her family in an embarrassing situation, *"One of my nieces planned to elope with a guy and my son helped her by giving her my mobile phone for communicating with the guy. If I hadn't shared my phone then that would not have happened."*

UP13 has reported concern that her friends, with whom she shares her online accounts, might share those accounts with others without informing her, who could eventually misuse her information. She also said, *"I share accounts with my trusted friends. But, sometimes they might be manipulated by others [to share my account]."* One of our participants told about a friend of hers, with whom she had shared the login credentials for her university account during her undergraduate study so that her friend could access the university's Wi-Fi network. Later, she identified that her friend had shared her password with more people allowing them access to her university's Wi-Fi network.

The misuse of a shared device or account could be unintentional or accidental, however, could put a user in an unexpected and embarrassing situation. UP9, our Native American participant, shares her social networking account with a few of her friends in the university. In some cases, her perspective of the appropriate photo or post that could be posted in social media varies from her friends. She referred to the past incidents where her friends had posted inappropriate photos and posts from her shared social networking account, leading her to encounter social embarrassment within her Native American community. A few participants reported concern that the unintentional misuse of a shared device or account by a friend or family member could create problems in their professional life. BP4 reported an incident to explain his concerns, *"While browsing on my phone, my brother accidentally clicked on a drive URL and asked permission for access to some confidential research data from my lab. Later, I had to toil hard to make my supervisor understand the reason of my account asking for permission to access those data."*

A few participants worried that their friends might misuse the shared device or account for amusement and fun, where it might lead our participants to social embarrassment. UP3 is a graduate student in the USA, who is originally from Iran. He mentioned that once his university friends, who had access to his social networking account, posted a life event from his account that he had got married. According to him, his friends posted this fake event for fun, however, was taken as truth by many of his friends and family members in his native country, leading him to face unwanted circumstances. Another participant (UP16) reported an incident, where a friend guessed the password for an email account based on the shared password for an online gaming account. That friend then exploited the email account to send inappropriate emails to the female students in their class.

In Bangladesh, a national ID card is required to purchase a mobile SIM card [36]. BP24, who is the owner of a digital service center in Bangladesh, keeps a scanned copy of his national ID card on his computer at the workplace. The password of this computer is shared with his employees. He explained how an employee at his digital service center had misused this access privilege, *"One of my employees took a print of it [national ID card] and managed to purchase a mobile SIM using it, but without informing me. Later, he told me about this incident out of anxiety, as he had lost his mobile phone that day, which means, if found, his phone would be returned to me as the SIM card in that mobile was purchased under my name."*

5.2.3 Change in Relationship

Some participants believe that their relationship with peers, with whom they share a digital device or online account, might affect how they would protect, or exploit our participants' information. UP15 explained, *"People turn on each other all the time. So if someone likes me now and doesn't like me after two months, then they may try to use that information [gathered from shared device or account] against me…They can use that information to damage my professional reputation or, you know, can cause financial loss."* In this context, UP8 believes that a family member would never exploit his personal information against him, however, he is concerned that the friends might breach his trust if his relationship with them changes over time. On the other hand, UP10 perceives that anyone, irrespective of a family member, a friend, or a colleague, might cause harm if his relationship with them deteriorates.

BP13 mentioned the unexpected circumstances her family had to face as a result of sharing devices, *"My daughter was in a relationship and she used to share her devices [mobile phone, laptop] with her Ex [boyfriend]. When they broke up, that guy started to blackmail her threatening that he would leak her photos [that he took in possession from the shared devices]."* Another participant (TP8) said, *"If you share [a device or account], you will be somewhat be, like the captive of whoever you shared with."*

A few participants perceive that the social networking account should be kept private, and not be shared with a partner or spouse. As they believe, without trust and mutual understanding, such sharing could hurt a relationship and lead to a breakup. UP10 shared the event from one of his friend's life, *"A friend of mine uses Facebook, and he gave access to his girlfriend because he loved her...He gave her his password so that she could log in and see what he was doing. But in the long run...the relationship ended. Because there was 'Oh, this person sends you a private message' - she reads it. I will not share my [social networking] account."*

5.3 Access Control Strategies

Around three-fourth of our participants do not take any steps to protect their information in the process of sharing their digital devices or online accounts, where we identified the following reasons behind such user behavior.

i) *Blind Trust.* Participants from Bangladesh and Turkey put blind trust on the technology to protect user information. They perceive that technology has advanced to a point that users no longer need to worry about security and privacy issues. TP2 commented, *"Actually, I feel pretty safe at the moment. The technology is already providing a lot."*

ii) *Lack of Knowledge.* Participants are unsure of how to protect their information. They perceive that they need to depend upon the trustworthiness of the peer with whom the device or account is shared to preserve their privacy. For instance, UP1 said, *"In my case, I cannot do anything! I just need to trust them (with whom the device or account is shared)."*

iii) *Optimism Bias.* Participants perceive, their personal information is of little interest to others. Thus, they believe that their information would not be accessed or stolen by others with whom they share their digital devices or online accounts.

iv) *Procrastination until Harms Occur.* Participants see the privacy violation as a 'distant harm'. So, they plan to take actions only if their information or credentials are breached; TP1 added, *"I would search on the Internet to figure out what actions I could take. What else can I do?"*

About one-fourth of our participants mentioned taking steps to protect their information in the process of sharing their digital devices or online accounts. Below, we present their reported strategies.

Biometric Authentication. We found that users might share authentication secrets in the process of sharing a digital device, where the sharee may later access that device without the sharer's (i.e., owner of the device) knowledge, which in turn, could pose privacy risks for the sharer. Our participants, UP2, BP5, BP6 and BP16 prefer that the sharee would not access a device without their knowledge. They switched from using traditional text-based password to biometric authentication on their smartphone. They believe, biometric authentication provides them with a better control on whom they would allow to access their devices.

Change of Passwords. UP15 changes his passwords for online accounts to control the access of sharees. He explained, *"I periodically change passwords, like in every three months or six months. So if the person who currently uses my account, wants to use it [in the future], he will need to ask me about new password. If I no longer want them to use my account then I would not give them the [new] password."* UP13 has mentioned, if she has to share the password for any of her online accounts with someone other than her family members or friends, she later changes that password to prevent an unauthorized access in the future.

Limited and Controlled Access. UP21 shares his mobile phone with friends and family members. He lets them use his phone for a limited amount of time that he considers sufficient to complete their tasks. He mentioned, *"I don't really let people use it [mobile phone] for a day, but like if they need it for a few minutes, or to make a phone call or check something online, that is fine. But I will not, like give it to them for a long period of time."*

UP18, BP25, and BP21 have reported that when they share their mobile phone with an unknown person, they stand beside that person to observe his activities on the phone, to ensure that he does not access any of their personal documents. BP21 further added, *"If a stranger wants to make a call from my phone, I myself*

dial that number, and just let him talk." Here, UP14 is more concerned about the logged-in online accounts on his computer and smartphone than the documents or information stored in his devices; he added, *"Before giving my digital device to someone else, I just try to logout from each account so that they cannot access my accounts."*

App Usage. BP3 worried about incurring financial loss in case of an unauthorized access to the app installed in a device that he shares with others. To prevent such incidents from happening, he does not use any financial app (e.g., the app for online banking) on his smartphone. One of our participants (UP19) reported using a folder lock app to preserve her privacy while sharing a digital device; she added, *"I keep like all my secret things locked so that no one else can see them."*

6 Discussion

6.1 Sharing Behavior: Through the Lens of Demographics, Society and Culture

The prior study [9] showed that female users in Saudi Arabia share their banking information with male family members due to driving restrictions, where their trust and esteem on family members contribute to their comfort with sharing financial credentials. We found that sharing login credentials of financial accounts (e.g., banks) may not be only specific to gender, rather could be influenced by a wide range of factors, like managing the expenditure of a family through collaboration and support, building trust in a romantic relationship, running a business in partnership with family members, and availing tech-support from IT personnel at the workplace. As it comes to collaboratively managing financial activities within a family, the sharing of a financial account depends upon family structure and dynamics. For example, participants living in Bangladesh and Turkey are comfortable with sharing their financial (e.g., bank) accounts with multiple members in their extended family (or 'functionally extended family' - see §2), which is less common in the nuclear family setting of our participants living in the USA.

Female users become victims of digital harassment or have to deal with aggressive comments in their posts on social networking sites in many developing countries, including Bangladesh [6, 60]. The women in Bangladesh are often uncomfortable to report or discuss sensitive issues, including the incidents of harassment in online social media, which is conditioned and limited by male-dominated and conservative Bangladeshi society [56]. Our findings reveal the workaround of a female participant, where she uses her male partner's social networking account to mask her identity while posting on controversial or sensitive issues. In this way, the sharing of a social networking account is leveraged to express user opinion with avoiding the possible risks of digital harassment.

The immigrants, experiencing cultural shifts adjust in complex ways to their new society [10, 46]. We found that our immigrant participants in the USA collaborate with friends and family members living in their native country to regain or maintain access to their online accounts, along with remotely managing financial transactions. Our findings reveal that the habituation and culture of sharing digital devices with household members in their native country contributed to our immigrant participants' comfort with sharing devices with their family members in the USA.

In a collectivist society, people belong to 'in groups' that take care of them in exchange for loyalty, and is manifest in a long-term commitment to the member 'group' [35, 42, 63]. With the course of digitization in a developing country, e.g., Bangladesh [45, 49, 72] where the collectivism prevails in societies [42, 63], the sharing of digital devices and online accounts with a 'close' group (comprising siblings, cousins, or friends with whom a person has grown up since childhood) might come as a natural expectation and event for the people, where they are habituated to, and are comfortable with sharing personal belongings and information with their 'close' group as they have grown up together. While our results indicate a relation between people's sharing behavior and prevalence of collectivism in a society, we believe that more studies are required within this domain, including a large-scale online survey with the participants from different countries and societies.

Our results on sharing devices with household members extend the findings from prior studies [5, 18, 52]. We found that participants living in Bangladesh and Turkey share not only a family-computer (e.g., one located in a public space at home [18]), but also their personal laptop/computer where the sharing of a device could extend beyond family members, and may not be constrained by a physical boundary (e.g., carrying a mobile phone borrowed from a household member, while visiting places outside of home). Our findings indicate that economic constraints often lead to the necessity of such extended sharing in a developing country, where

societal settings and trust on peers contribute to people's comfort with sharing.

The prior studies [7, 41, 73] discussed the sharing of devices and accounts by the people with special needs, like users with visual impairments or certain disabilities. Our study joins this body of literature, where we found that relatively older, or less-educated users in Bangladesh avail help from their family members, friends, or IT personnel at the workplace to create and maintain online accounts. They also build a small group with trusted peers to collaboratively use a single social networking account; the members in such a group help each other to address technical issues, learn and use new features and settings, recall password if forgotten, and maintain an online presence when one's Internet data budget is exhausted. Our findings on collaborative use of online accounts add new dimensions to the discussion on digital inclusion in a developing country, where we emphasize on future research to gain further insights into the corresponding privacy and social implications.

The security and privacy issues in different business settings and organizational culture were investigated in prior studies [23, 38, 82, 86], where our findings advance the understanding of research community through shedding light on sharing devices and accounts in professional contexts. We found that the expectations of preserving privacy are not well communicated to the colleagues while sharing a computer at the workplace, resulting in unwanted access to one's online account. Our study extends the findings of Haque et al. [38] on digital service centers in Bangladesh, showing that the owners of these business places share their personal email account and financial information with employees to avail convenience in serving their customers. The concept of clientelization (buyers and sellers cultivate long-lasting relationships and trust through repeated interactions) discussed by Haque et al. [38] explains why our participants who are the owners of, or employees at digital service centers offer informal services to their customers despite the risks of a privacy breach.

6.2 User Concerns, Risks, and Privacy Behavior

Our findings show that the clear communication of expectations to sharees is vital for the sharer of a device or account. We identified a range of privacy and social issues that could emerge from a lack of understanding the expectations of a sharer, which could lead to unwanted access of apps, personal documents, and online accounts on a shared device, misuse of a device that puts a family in an embarrassing situation, and further sharing of an online account by a sharee (termed as *secondary sharing* in this paper) with entities unknown to the primary sharer, i.e., owner of that account.

The differences in societal and cultural background between a sharer and sharee could contribute to the misunderstanding of expectations in the collaborative use of devices and accounts. For instance, the university friends, with whom the social networking account is shared by our Native American participant, and an immigrant participant in the USA (who is originally from Iran), did not have a clear understanding of the cultural norms and values of our participants. As a result, the posts and photos on their social networking account, posted by their friends (sharees of that account) led our participants encountering unwanted and embarrassing situations within their family and community.

Our participants' comfort with sharing a device or account is often rooted in the accountability of sharees, whom they know in person, and could trust with protecting their privacy. Here, secondary sharing is a matter of concern to several participants, where the current sharees of their online account could share the login credentials of that account with other entities without informing them. The participants do not feel confident with protecting their privacy on a shared account in the presence of an entity who is not personally known to them. Participants also worried about unpredictable human traits, which could be influenced by a change in relationship between peers over time [28, 88]; we found that the personal contents taken into possession from shared devices were used to blackmail our participant's family member.

Our findings reveal several instances that are not limited within the boundary of personal trust and privacy violation in the landscape of shared devices and accounts, but also raise the question of legality (e.g., taking a copy of someone else's National ID card from a shared device to purchase a mobile SIM card in Bangladesh), and socially accepted behavior, like sending inappropriate emails to female classmates from someone else's account. We believe, future studies should focus on investigating the social and emotional implications of unexpected incidents that emerge from sharing devices and accounts.

The cultural norms and religious beliefs could impact the privacy behavior of people in social media [1]; our findings provide further insights into the relation between cultural values and self regulation in protecting other's privacy. The exposure to intimate images and

sexual contents are considered taboo and frowned upon in the culture of Bangladesh [64, 78], where a participant reported feeling guilty when he accidentally accessed the personal photos of his family members on a shared device, however, he immediately logged out and controlled himself from violating other's privacy. A few of our Bangladeshi participants who are in a profession of repairing devices at digital service centers, reported to refrain themselves from accessing the personal contents of customers on their devices despite having opportunities, where one of them reported his guilt that he had accidentally accessed personal photos of a customer.

The risk perceptions of a user may not trigger privacy-preserving behavior. Most of our participants do not take any steps to protect their privacy while sharing a device or account, where several participants adopt ad-hoc based approaches. In one approach, participants stand beside a sharee to observe their activities on the shared device. Such surveillance might protect the sharer's personal documents from unwanted access, however, could pose privacy risks for the sharee as their activities on the shared device are closely observed. It would be an interesting avenue for future research to look into privacy negotiations from the perspective of sharees while using a shared device.

Only in a few cases, we found that participants' privacy protection strategies directly relate to their risk perceptions. For instance, one of our participants (UP15) changes his password periodically to control whom he wants to share his account with, who is concerned that the relationship with sharees and so on, their accountability in protecting his information could change over time. It is not clear though, if changing a password provides adequate security and privacy protection for the participant, where prior studies [25, 69, 75] showed that users make predictable changes in their old password while creating a new one for their account.

In some cases, participants' strategies to preserve accessibility to personal information could bring further security risks; they write down their passwords on a physical notebook to preserve accessibility, in case the file on a shared device where they have stored their passwords is accidentally deleted by a sharee of that device. However, writing down or storing passwords in an unprotected medium could lead to password leakage [89], increasing the risks of unauthorized access to users' online accounts, where one of our participants explicitly mentioned about keeping a diary containing her password in an open desk without any protection (e.g., using a physical lock). The future research should further investigate how users protect the medium that they use to write down their passwords.

7 Limitations and Conclusion

We interviewed 59 participants in our study, where we followed the widely-used methods for qualitative research [14, 16, 17], focusing in depth on a small number of participants and continuing the interviews until no new themes emerged (saturation). We acknowledge the limitations of such study that a different set of samples might yield varying results. Thus, we do not draw any quantitative, generalizable conclusion from this study.

A few of our participants were recruited via snowball sampling. In snowball sampling, participants who have taken part in the study nominate people for recruitment whom they know well, and thus, it may suffer from sampling bias. In addition, self-reported data might have limitations, like recall and observer bias.

We recruited participants from three countries: Bangladesh, USA, and Turkey, where our findings should not be generalized to the entire population in the world. Our study is based in urban areas. We note that users' privacy perceptions might be different in rural areas. Since users' security and privacy perceptions are positively influenced by their knowledge and technical efficacy [44, 55, 71], and the literacy rate is generally higher in urban areas as compared to that in rural areas [61], we speculate that the privacy perceptions and behavior of users reported in this paper represent an upper bound in the context of sharing devices and accounts.

Despite these limitations, our findings contribute to the situated understanding of users' concerns, risks, and privacy behavior in various contexts of sharing digital devices and online accounts, in particular financial and identity accounts. Our analysis unpacks the relation between users' sharing behavior and their demographics, social background, and cultural values. The findings from this study inform designers about different sharing practices within and outside of Western contexts, which they can leverage to evaluate how various sharing types would impact the use of new technologies being designed. We encourage PETS community to extend the findings of this work in the contexts of different domains and field sites, and use other methods as well, if required.

Acknowledgement

We thank our participants in this study. We are thankful to our shepherd, Cheng Guo and the anonymous reviewers for their thoughtful and detailed feedback. This research is supported by the faculty startup fund provided to Mahdi Nasrullah Al-Ameen by Utah State University.

References

[1] Abokhodair, N., and Vieweg, S. Privacy & social media in the context of the arab gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (New York, NY, USA, 2016), DIS '16, Association for Computing Machinery, p. 672–683.

[2] Adams, A., and Sasse, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[3] Ahmed, S. I., Guha, S., Rifat, M. R., Shezan, F. H., and Dell, N. Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (New York, NY, USA, 2016), ICTD '16, ACM, pp. 11:1–11:10.

[4] Ahmed, S. I., Haque, M. R., Chen, J., and Dell, N. Digital privacy challenges with shared mobile phone use in bangladesh. *Proceedings of the ACM on Human-Computer Interaction 1*, CSCW (2017), 17.

[5] Ahmed, S. I., Haque, M. R., Chen, J., and Dell, N. Digital privacy challenges with shared mobile phone use in bangladesh. *Proc. ACM Hum.-Comput. Interact. 1*, CSCW (Dec. 2017), 17:1–17:20.

[6] Ahmed, S. I., Jackson, S. J., Ahmed, N., Ferdous, H. S., Rifat, M. R., Rizvi, A., Ahmed, S., and Mansur, R. S. Protibadi: A platform for fighting sexual harassment in urban bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2014), CHI '14, Association for Computing Machinery, p. 2695–2704.

[7] Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., and Kapadia, A. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (New York, NY, USA, 2015), CHI '15, Association for Computing Machinery, p. 3523–3532.

[8] Al-Ameen, M. N., Tamanna, T., Nandy, S., Ahsan, M. A. M., Chandra, P., and Ahmed, S. I. We don't give a second thought before providing our information: Understanding users' perceptions of information collection by apps in urban bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies* (New York, NY, USA, 2020), COMPASS '20, Association for Computing Machinery, p. 32–43.

[9] Alghamdi, D., Flechais, I., and Jirotka, M. Security practices for households bank customers in the kingdom of saudi arabia. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (USA, 2015), SOUPS '15, USENIX Association, p. 297–308.

[10] Ayçiçegi-Dinn, A., and Caldwell-Harris, C. L. Individualism–collectivism among americans, turks and turkish immigrants to the us. *International Journal of Intercultural Relations 35*, 1 (2011), 9–16.

[11] Bank, W. Gdp per capita. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

[12] Bank, W. Literacy rate, adult total. https://data.worldbank.org/indicator/SE.ADT.LITR.ZS.

[13] Baştuğ, S. Household and family in turkey: An historical perspective. *Autonomy and dependence in the family: Turkey and Sweden in critical perspective* (2002), 99–116.

[14] Baxter, K., Courage, C., and Caine, K. *Understanding Your Users: A Practical Guide to User Research Methods*, 2 ed. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2015.

[15] Bødker, S., and Christiansen, E. Poetry in motion: Appropriation of the world of apps. In *Proceedings of the 30th European Conference on Cognitive Ergonomics* (New York, NY, USA, 2012), ECCE '12, Association for Computing Machinery, p. 78–84.

[16] Boyatzis, R. E. *Transforming qualitative information: Thematic analysis and code development*. sage, Thousand Oaks, CA, USA, 1998.

[17] Braun, V., and Clarke, V. Using thematic analysis in psychology. *Qualitative research in psychology 3*, 2 (2006), 77–101.

[18] Brush, A. J. B., and Inkpen, K. M. Yours, mine and ours? sharing and use of technology in domestic environments. In *UbiComp 2007: Ubiquitous Computing* (Berlin, Heidelberg, 2007), J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang, Eds., Springer Berlin Heidelberg, pp. 109–126.

[19] Busse, B., and Fuchs, M. Prevalence of cell phone sharing. *Survey Methods: Insights from the Field 1* (2013), 15.

[20] Chen, J., Paik, M., and McCabe, K. Exploring internet security perceptions and practices in urban ghana. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (USA, 2014), SOUPS '14, USENIX Association, p. 129–142.

[21] Cherapau, I., Muslukhov, I., Asanka, N., and Beznosov, K. On the impact of touch id on iphone passcodes. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (USA, 2015), SOUPS '15, USENIX Association, p. 257–276.

[22] Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., and Kohno, T. Computer security for data collection technologies. *Development engineering 3* (2018), 1–11.

[23] Conway, D., Taib, R., Harris, M., Berkovsky, S., Yu, K., and Chen, F. A qualitative investigation of bank employee experiences of information security and phishing. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (USA, 2017), SOUPS '17, USENIX Association, p. 115–129.

[24] Crabtree, A., Tolmie, P., and Knight, W. Repacking 'privacy' for a networked world. *Comput. Supported Coop. Work 26*, 4-6 (Dec. 2017), 453–488.

[25] Das, A., Bonneau, J., Caesar, M., Borisov, N., and

Wang, X. The tangled web of password reuse. In *NDSS* (01 2014), vol. 14, pp. 23–26.

[26] Derlega, V., and Chaikin, A. Privacy and self-disclosure in social relationships. *Journal of Social Issues 33* (04 2010), 102 – 115.

[27] Dodson, L. L., Sterling, S. R., and Bennett, J. K. Minding the gaps: Cultural, technical and gender-based barriers to mobile use in oral-language berber communities in morocco. In *Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers - Volume 1* (New York, NY, USA, 2013), ICTD '13, Association for Computing Machinery, p. 79–88.

[28] Dominelli, L. Betrayal of trust: a feminist analysis of power relationships in incest abuse and its relevance for social work practice. *The British Journal of Social Work 19*, 1 (1989), 291–308.

[29] Egelman, S., Brush, A. B., and Inkpen, K. M. Family accounts: A new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work* (New York, NY, USA, 2008), CSCW '08, Association for Computing Machinery, p. 669–678.

[30] Eldefrawy, M. H., Alghathbar, K., and Khan, M. K. Otp-based two-factor authentication using mobile phones. In *Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations* (USA, 2011), ITNG '11, IEEE Computer Society, p. 327–331.

[31] Elphinston, R. A., and Noller, P. Time to face it! facebook intrusion and the implications for romantic jealousy and relationship satisfaction. *Cyberpsychology, Behavior, and Social Networking 14*, 11 (2011), 631–635.

[32] Faruq, M. O., Rahman, M. M., Alam, M. R., et al. Impact of social networking sites in bangladesh: Few possible solutions. *International Journal of Intelligent Systems and Applications 9*, 4 (2017), 53.

[33] Frohlich, D., and Kraut, R. The social context of home computing. In *Inside the smart home*. Springer, London, 2003, pp. 127–162.

[34] Geeng, C., and Roesner, F. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), CHI '19, Association for Computing Machinery, p. 1–13.

[35] Gorodnichenko, Y., and Roland, G. Understanding the individualism-collectivism cleavage and its effects: Lessons from cultural psychology. In *Institutions and comparative economic development*. Springer, London, 2012, pp. 213–236.

[36] GSMA. Mandatory registration of prepaid sim cards: Addressing challenges through best practice, April 2016. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf.

[37] Hang, A., von Zezschwitz, E., De Luca, A., and Hussmann, H. Too much information! user attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design* (New York, NY, USA, 2012), NordiCHI '12, Association for Computing Machinery, p. 284–287.

[38] Haque, S. M. T., Haque, M. R., Nandy, S., Chandra, P., Al-Ameen, M. N., Guha, S., and Ahmed, S. I. Privacy vulnerabilities in public digital service centers in dhaka, bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development* (New York, NY, USA, 2020), ICTD2020, Association for Computing Machinery.

[39] Haque, S. T., Wright, M., and Scielzo, S. A study of user password strategy for multiple accounts. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy* (New York, NY, USA, 2013), CODASPY '13, Association for Computing Machinery, p. 173–176.

[40] Haris, M. S., and Loyd, E. L. Countries and their cultures: Bangladesh. https://www.everyculture.com/A-Bo/Bangladesh.html.

[41] Hayes, J., Kaushik, S., Price, C. E., and Wang, Y. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (USA, 2019), SOUPS'19, USENIX Association, p. 1–20.

[42] Hofstede, G. Dimensionalizing cultures: The hofstede model in context. *Online readings in psychology and culture 2*, 1 (2011), 8.

[43] Intercultural Programs, A. Bangladeshi culture. https://www.afsusa.org/countries/bangladesh/.

[44] Ion, I., Reeder, R., and Consolvo, S. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (USA, 2015), SOUPS '15, USENIX Association, p. 327–346.

[45] Islam, S. Digital bangladesh a reality now, July 2018. https://www.dhakatribune.com/bangladesh/2018/07/11/digital-bangladesh-a-reality-now.

[46] Jasso, G., and Rosenzweig, M. R. *The new chosen people: Immigrants in the United States*. Russell Sage Foundation, 1990.

[47] Johnson, M., Egelman, S., and Bellovin, S. M. Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (New York, NY, USA, 2012), SOUPS '12, ACM, pp. 9:1–9:15.

[48] Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S. "my data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (USA, 2015), SOUPS '15, USENIX Association, p. 39–52.

[49] Karim, M. A. Digital bangladesh for good governance. In *Bangladesh Development Forum* (Bangladesh, 2010), pp. 15–16.

[50] Kumaraguru, P., and Cranor, L. Privacy in india: Attitudes and awareness. *Privacy Enhancing Technologies 3856* (2006), 243–258.

[51] Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., and Lagae, K. *How parents of young children manage digital devices at home: The role of income, education and parental style*. EU Kids Online, 2015.

[52] Matthews, T., Liao, K., Turner, A., Berkovich, M., Reeder, R., and Consolvo, S. "she'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Con-*

ference on Human Factors in Computing Systems (New York, NY, USA, 2016), CHI '16, Association for Computing Machinery, p. 5921–5932.

[53] Mazurek, M. L., Arsenault, J., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., et al. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), pp. 645–654.

[54] Mazurek, M. L., Klemperer, P. F., Shay, R., Takabi, H., Bauer, L., and Cranor, L. F. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2011), pp. 2085–2094.

[55] Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Kelley, P. G., Shay, R., and Ur, B. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (New York, NY, USA, 2013), CCS '13, Association for Computing Machinery, p. 173–186.

[56] Moitra, A., Hassan, N., Mandal, M. K., Bhuiyan, M., and Ahmed, S. I. Understanding the challenges for bangladeshi women to participate in# metoo movement. *Proceedings of the ACM on Human-Computer Interaction 4*, GROUP (2020), 1–25.

[57] Nahar, P., Van Reeuwijk, M., and Reis, R. Contextualising sexual harassment of adolescent girls in bangladesh. *Reproductive health matters 21*, 41 (2013), 78–86.

[58] Nations, U. World economic situation and prospects report: Country classification. https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf.

[59] Nissenbaum, H. Privacy as contextual integrity. *Wash L. Rev 79* (2004), 119.

[60] Nova, F. F., Rifat, M. R., Saha, P., Ahmed, S. I., and Guha, S. Online sexual harassment over anonymous social media in bangladesh. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development* (New York, NY, USA, 2019), ICTD '19, ACM, pp. 1:1–1:12.

[61] of Statistics, B. B. Literacy assessment survey 2008, Nov 2008. http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Dhaka/pdf/EDU/Literacy%20Assessment%20Survey%202008.pdf.

[62] Patrick, A., and Kenny, S. From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In *Privacy Enhancing Technologies* (Berlin, Heidelberg, 2003), Springer, Springer Berlin Heidelberg, pp. 107–124.

[63] Rahman, T. Problems of democratic consolidation in bangladesh: A cultural explanation. *Network of Asia-Pacific Schools and Institutes of Public Administration and Governance (NAPSIPAG) 569* (2006), 46.

[64] Rashid, S. F., Standing, H., Mohiuddin, M., and Ahmed, F. M. Creating a public space and dialogue on sexuality and rights: a case study from bangladesh. *Health Research Policy and Systems 9*, 1 (2011), S12.

[65] Rogers, M. Country overview: Bangladesh: Mobile industry driving growth and enabling digital inclusion, August 2014. https://www.gsmaintelligence.com/research/?file=a163eddca009553979bcdfb8fd5f2ef0&download.

[66] Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L. S., Matthews, T., Consolvo, S., and Churchill, E. "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (Baltimore, MD, Aug. 2018), USENIX Association, pp. 127–142.

[67] Sambasivan, N., Rangaswamy, N., Cutrell, E., and Nardi, B. Ubicomp4d: Infrastructure and interaction for international development–the case of urban indian slums. In *Proceedings of the 11th International Conference on Ubiquitous Computing* (New York, NY, USA, 2009), UbiComp '09, Association for Computing Machinery, p. 155–164.

[68] Sambasivan, N., Weber, J., and Cutrell, E. Designing a phone broadcasting system for urban sex workers in india. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011), CHI '11, Association for Computing Machinery, p. 267–276.

[69] Seitz, T., Hartmann, M., Pfab, J., and Souque, S. Do differences in password policies prevent password reuse? In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (New York, NY, USA, 2017), CHI EA '17, Association for Computing Machinery, p. 2056–2063.

[70] Seng, S., Al-Ameen, M. N., and Wright, M. A first look into users' perceptions of facial recognition in the physical world. *Computers & Security 105* (2021), 102227.

[71] Seng, S., Kocabas, H., Al-Ameen, M. N., and Wright, M. Poster: Understanding user's decision to interact with potential phishing posts on facebook using a vignette study. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2019), CCS '19, Association for Computing Machinery, p. 2617–2619.

[72] Shamsuddin, A. K. The real scenario of internet access, July 2018. https://www.thedailystar.net/opinion/perspective/the-real-scenario-internet-access-1611499.

[73] Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. Password sharing: Implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2007), CHI '07, Association for Computing Machinery, p. 895–904.

[74] Steenson, M., and Donner, J. Beyond the personal and private: Modes of mobile phone sharing in urban india. *The reconstruction of space and time: Mobile communication practices 1* (2009), 231–250.

[75] Stobert, E., and Biddle, R. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS)* (Menlo Park, CA, 2014), USENIX Association, pp. 243–255.

[76] Sultana, S., Saha, P., Hasan, S., Alam, S. M. R., Akter, R., Islam, M. M., Arnob, R. I., Al-Ameen, M. N., and Ahmed, S. I. Understanding the sensibility of social media use and privacy with bangladeshi facebook group users. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies* (New York, NY,

USA, 2020), COMPASS '20, Association for Computing Machinery, p. 317–318.

[77] Trommsdorff, G., and Nauck, B. *The Value of Children in Cross Cultural Perspective: Case Studies from Eight Societies*. Pabst Science Publishers, 2005.

[78] van Reeuwijk, M., and Nahar, P. The importance of a positive approach to sexuality in sexual health programmes for unmarried adolescents in bangladesh. *Reproductive Health Matters 21*, 41 (2013), 69–77.

[79] Vashistha, A., Anderson, R., and Mare, S. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (New York, NY, USA, 2018), COMPASS '18, Association for Computing Machinery.

[80] Warren, S. D., and Brandeis, L. D. The right to privacy. *Harvard Law Review 4*, 5 (1890), 193–220.

[81] Wash, R. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (2010), pp. 1–16.

[82] Watkins, E. A., Al-Ameen, M. N., Roesner, F., Caine, K., and McGregor, S. Creative and set in their ways: Challenges of security sensemaking in newsrooms. In *7th USENIX Workshop on Free and Open Communications on the Internet (FOCI)* (Vancouver, BC, 2017), USENIX Association.

[83] Westin, A. F. Privacy and freedom. *Washington and Lee Law Review 25*, 1 (1968), 166.

[84] Wikipedia. Bangladesh. https://en.wikipedia.org/wiki/Bangladesh.

[85] Wikipedia. Turkey. https://en.wikipedia.org/wiki/Turkey.

[86] Williams, E. J., Hinds, J., and Joinson, A. N. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies 120* (2018), 1–13.

[87] Wisniewski, P., Lipford, H., and Wilson, D. Fighting for my space: Coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), pp. 609–618.

[88] Yerokhin, O. The social cost of blackmail. *Review of Law & Economics 7*, 1 (2011), 337–351.

[89] Zhang-Kennedy, L., Chiasson, S., and van Oorschot, P. Revisiting password rules: facilitating human management of passwords. In *2016 APWG symposium on electronic crime research (eCrime)* (Toronto, ON, Canada, 2016), IEEE, IEEE, pp. 81–90.

[90] Zou, Y., Mhaidli, A. H., McCall, A., and Schaub, F. "i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (2018), pp. 197–216.

Appendix

See next page.

Questionnaire. At the beginning, we explained to the participants what we mean by 'digital device', and 'online account' in our study. Here, the term 'digital device' refers to the computer and mobile phone. The term 'online account' refers to financial account, email account, and social networking account in this study. The following questions represent the main themes discussed during the interviews. We may have probed for more details depending upon the participant's responses.

Q. Do you share your digital devices, and online accounts with others?

- Whom do you share with?
- Please tell us about the reasons and contexts behind your sharing.

Q. Do you have any concerns about sharing digital devices, and online accounts?

Q. Did you face any unexpected, or unwanted events in the past due to sharing digital devices, and online accounts?

Q. Do you take any measures to protect your information while sharing digital devices, and online accounts?

At the end, participants responded to demographic questions. We include the demographic questions below.

Q. What is your gender?
- Male
- Female
- Other
- Prefer not to answer

Q. What is your age-range?
- 18–24 years old
- 25–29 years old
- 30–34 years old
- 35–39 years old
- 40–44 years old
- 45–49 years old
- 50–54 years old
- 55 years old or above
- Prefer not to answer

Q. Which country do you currently live in?

Q. What is your country of origin?

Q. What is your highest level of education?
- Less than High School, please specify grade level:
- High school graduate or equivalent
- Two-year college degree
- Four-year college degree
- Graduate degree (MS/PhD)
- Other, please specify:
- Prefer not to answer

Q. Which of the following best describes your primary occupation?
- Student
- Employee at Government organization
- Employee at Educational or Non-profit organization
- Employee at Industry
- Other, please specify:
- Prefer not to answer

Contexts and Reasons of Sharing	Inter-rater Reliability
Geographic Relocation	**0.91**
Collaborative Financial Management	**0.83**
Token of Trust and Affection	**0.89**
Sharing the Same Physical Space	**0.79**
Collaborative Social Networking and Communication	**0.81**
Business Management and Informal Services	**0.83**
Intermediate Help	**0.92**
Risk Perceptions	
Loss and Leakage of Personal Information	**0.85**
Misuse of Shared Device and Account	**0.79**
Change in Relationship	**0.91**
Reasons behind not Taking Privacy-preserving Steps	
Blind Trust	**0.81**
Lack of Knowledge	**0.92**
Optimism Bias	**0.75**
Procrastination until Harms Occur	**0.88**
Access Control Strategies	
Biometric Authentication	**1.00**
Change of Passwords	**1.00**
Limited and Controlled Access	**0.88**
App Usage	**0.91**

Table 2. The inter-rater reliability (Cohen's Kappa)