"Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh

Syed Ishtiaque Ahmed
Computer Science
University of Toronto
Toronto, Ontario, Canada

Md. Romael Haque
Computer Science
Marquette University
Milwaukee, WI, USA

Irtaza Haider
Computer Science
Georgia Tech
Atlanta, GA, USA

Jay Chen
Computer Science
New York University
Abu Dhabi, UAE

Nicola Dell
Information Science
The Jacobs Institute, Cornell Tech
New York, NY, USA

ABSTRACT

People in South Asia frequently share a single device among multiple individuals, resulting in digital privacy challenges. This paper explores a design concept that aims to mitigate some of these challenges through a 'tiered' privacy model. Using this model, a person creates a 'shared' account that contains data they are willing to share and that is assigned a password that will be shared. Simultaneously, they create a separate 'secret' account that contains data they prefer to keep secret and that uses a password they do not share with anyone. When a friend or family member asks to check their device, the user can tell them the password for their shared account, with their private data secure in the secret account that the other person is unaware of. We explore the benefits and trade-offs of our design through a three-week deployment with 21 participants in Bangladesh, presenting findings that show how our work aids digital privacy while also highlighting the challenges that remain.

KEYWORDS

HCI4D; ICTD; Privacy; Access; Shared Use; Mobile Devices.

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300410

ACM Reference Format:
Syed Ishtiaque Ahmed, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. "Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300410

1 INTRODUCTION

Many existing mobile device usage, access control, and authentication mechanisms are based on the Western paradigm of 'personal computing' [12, 42, 59], which assumes that a device is generally owned and used by a single person. However, a growing body of work suggests that this model of personal computing is not well-suited to populations living in South Asia, where intermediated access and device sharing are common [9, 10, 16, 50, 55]. In particular, a recent study in Bangladesh describes the digital privacy challenges that arise when people share devices, highlighting how the design of existing privacy mechanisms does not adequately meet the needs of these populations [6].

In short, technology users in South Asia are faced with a fundamental trade-off: on one hand, they want, need, or are compelled to share devices with others, usually friends and family, and refusing to share could have potentially serious negative social consequences. On the other hand, as one of our participants said, *"everyone has some personal stuff"* that they would prefer to keep private and not share with others. The contribution of our work is to explore this trade-off via a prototype design, called *"Nirapod"* (a Bengali word that means safe or protected). *Nirapod* provides a mechanism for enabling 'tiered' privacy that allows people to share their phones while keeping their personal data private. The interface is also designed to hide the fact that multiple tiers exist, thereby reducing the likelihood that people can be compelled to reveal private data.

Although the concept of tiered privacy can theoretically support an arbitrary number of tiers, we chose to initially explore a model that makes use of two tiers. One tier is a 'shared' account that contains data the user is willing to share with others and that is assigned a password that can safely be shared with friends and family. The other tier is a 'secret' account that contains data they prefer to keep secret and that uses a password they do not share with anyone. Then, when someone asks to use their device, they can hand it over and safely tell them the password for the shared account, with their private data securely stored in the secret account that the other person is unaware of. Since it is important to keep the existence of the multiple accounts secret, *Nirapod* provides a common entry point into both the shared and secret accounts, with the system identifying the account to open based solely on the password entered.

To explore the benefits, challenges, and trade-offs of our tiered privacy model, we implemented *Nirapod* as a prototype photo gallery app, since prior work suggests people especially care about the privacy of their personal photos, making this a compelling test scenario [3, 6, 41, 61]. After designing and testing our prototype, we conducted a three-week deployment with 21 participants in Bangladesh, a lower-middle income country with a large population that is rapidly adopting smartphones and experiencing digital privacy challenges for the first time [31]. Bangladesh is also a strongly patriarchal and predominantly Muslim society [17] that is socially and culturally different to the Western (e.g., US and European) cultures that have dominated the design of devices and privacy mechanisms.

Pre-study interviews reveal that our 21 participants face numerous privacy challenges when sharing devices with friends and family. Quantitative usage data of our prototype shows that participants were able to use the app, with most participants using the secret account more than the shared account. Post-study interviews suggest that *Nirapod's* tiered privacy model does help with some privacy challenges, with participants describing how they were able to share their device with others and still feel confident that their private data was protected. However, participants also had trouble remembering multiple passwords and worried about confusing their secret and shared passwords, fearing that they would accidentally type in their secret password when they meant to use their shared password (although this did not happen during our study). Our analysis also raises interesting questions regarding the gendered nature of privacy in a patriarchal society like Bangladesh, with women often under more pressure to reveal their private data to others, particularly husbands, boyfriends, or parents. Taken together, our findings advance the HCI community's knowledge of how to design for digital privacy in non-Western contexts.

2 RELATED WORK

The modern definition of privacy is heavily influenced by Western liberal ideologies that considers an individual's private information as an inseparable part of their identity and a basic ingredient of a functioning democracy [14, 26]. For example, when Warren and Brandeis [62] defined privacy as *"the right to be let alone"*, they argued for establishing 'privacy', a tight integration between a person's economic, social, and political identities and their properties, as a right for every lawful citizen in a country. This idea of privacy as personal possession over one's properties later extended to the world of information technology [42], and a piece of information attached to one's identity and actions became integral with one's privacy rights [63]. This digital privacy of computer users has become vulnerable to intrusions as computing has become more personalized, ubiquitous, and connected. Discussions around privacy are therefore a growing concern in Western contexts, especially as privacy rights are frequently violated, as is the case after large-scale illegal surveillance or data breaches are discovered [24, 32, 64].

A rich body of work in HCI and related disciplines has focused on human-centered privacy. For example, scholars have studied password construction and use [22, 25, 33, 34, 38], privacy-related behavior on social networks [18, 23, 30, 30, 36, 47, 65], recommendation systems [43], mobile devices [53, 68], and use of the Internet by specific groups of people (e.g., children, older adults, and disabled people) [20, 37, 66, 67]. However, with a few exceptions, research on usable privacy has focused on Western contexts.

Many privacy scholars have discussed how the idea of privacy is dependent on the context, and may not be transferable from one context to another. For example, Nissenbaum defined privacy as 'contextual integrity', and argued that, with the change of social and cultural context, the notion of privacy changes [48, 49]. Petronio has also contributed to the idea of the situated nature of privacy by developing the concept of Communication Privacy Management [52], explaining how individuals maintain the 'boundary' of their private information by managing their 'self-disclosures'. These studies turn us toward the cultural theories to perceive the differences in 'privacy practices' in 'the West' and those in the 'other' places. For example, Hofstede [35] describes how the 'individualistic' culture of the West is very different from the 'collectivist' culture in China or within the Indian subcontinent. Although Hofstede's claim suffers from some over-generalizations [13], it is true that individualistic values are more prevalent in Western 'developed' countries than in 'developing' countries in Asia and Africa [60]. These collectivist values often cause a person's identity as a 'free individual' to be supplanted by, or create tension with, their familial, communal, cultural, and religious identities. HCI4D

scholarship has long been studying, analyzing, and designing for various challenges rooted in these collective values (see [9, 10, 51, 55], for example). However, very few design initiatives have been undertaken to address the privacy challenges associated with these collective values.

Recent privacy-focused work in HCI4D has surfaced attitudes and practices that appear to be a consequence of the conflict between user privacy norms and the privacy mechanisms available. For example, Abokhodair et al. have reported how the privacy and security issues in the gulf countries are closely tied with their political tensions and conservative cultural norms [1, 2]. In the context of South Asia, Kumaraguru et al. have studied the use of communication media in India and reported on how their way of dealing with privacy is different from people in the West [40]. Similarly, Sambasivan et al. [54] recently reported various ways women in India, Pakistan, and Bangladesh negotiate their privacy with digital media, while Srinivasan et al. [56] showed how such privacy decisions are often transnational and relational in India. Ahmed and his colleagues conducted a series of studies on privacy in Bangladesh that are closely related to and motivate our work. For example, they discussed privacy vulnerabilities that arise in informal repair markets [5]. They also reported on how the privacy of Bangladeshi citizens is negotiated with the broader security demands of the country [7]. Most recently, Ahmed et al. studied the privacy tensions associated with shared device use in Bangladesh, showing how individual users desire privacy while sharing devices [6].

Although these studies have unveiled areas of tension surrounding privacy, **no prior work has explored the deployment of a technology intervention** that engages with these challenges. To the best of our knowledge, ours is the first paper to attempt such a deployment in South Asia, and our findings regarding participants' experiences with our design yield new knowledge for the HCI community.

Privacy with Shared Devices

Many existing authentication mechanisms are designed to enable people to secure their private data on mobile devices, including passwords, pattern locks, and biometrics (e.g., fingerprint scanners). Each of these mechanisms may be applied at the level of the entire device (e.g., phone screen lock), for specific applications (e.g. app lockers), or for individual users (e.g., user login). Many of these authentication mechanisms are based on the Western paradigm of 'personal computing' [12, 42, 59], which assumes that a device is generally owned and used by a single person. In the West, where a mobile phone or a laptop is generally considered to be 'private', device-level locking and authentication mechanisms match and often produce the desired privacy outcome. A recent study by Matthews et al. focused on device sharing in US families, highlighting some privacy tensions around casual sharing of mobile devices [45]. However, as the paper discusses, such sharing in US families is incidental.

In South Asia, by contrast, device sharing is systemic [9, 16, 50, 55], which necessitates a finer-grained sharing mechanism [44]. Using a password to protect a device or app may make it unsharable, while not using a password may result in the data being unprotected. To overcome this problem, it is very common for people to share the passwords required to access their device and applications [7, 38, 55]. Although several vendors have enabled the creation of multiple user accounts on a single device [11, 58], prior work suggests that people do not use this functionality because of poor usability and because logging out of one's account before sharing it with a family member would imply a lack of trust in that family member or arouse suspicion by suggesting that there is something to hide [6, 39].

Hidden vaults are a possible alternative, but most vault-based apps on the market (e.g. Aspire News, Calculator Vault Gallery Lock) do not hide their purpose or their presence on the device, allowing an adversary to see the app is installed and pressure the user into exposing data. Other apps with "stealth modes" (hiding the app) either: a) have a separate entry point to reveal the hidden vault or b) once the vault is opened, the user interface is clearly identifiable as being not the "normal" interface so that if someone sees it open it will raise suspicion. In addition, there are no deployments or user studies documenting the usability or acceptability of existing vault-based apps.

We are not aware of attempts to address the design paradox of supporting a desire for personal privacy while also enabling device sharing. The contribution of our work is to explore a mechanism for enabling 'tiered' privacy that allows people to share their phones while keeping their personal data private. We now discuss our design in detail.

3 PROTOTYPE DESIGN

The challenges described in the literature highlight important trade-offs for technology users in South Asia who need to share their device with others but who also want to be able to keep some personal data private. Our goal is to challenge and further explore these trade-offs through a prototype design concept, called *Nirapod*. Specifically, *Nirapod* uses a 'tiered' privacy mechanism that aims to allow people to share their phones with others while keeping their personal data private and reducing the possibility of being pressured into revealing their private data. Our intervention enables a single user to have multiple accounts, with the existence of the multiple accounts kept secret.

Our initial design supports a two-tiered model. This model enables a person to create a 'shared' account that contains data they are willing to share and that is assigned a password

that will be shared with friends and family. Simultaneously, they can create a 'secret' account that contains data they prefer to keep secret and that uses a password they do not share with anyone. Then, when a friend or family member asks to check their device, they can hand it over and tell them the password for the shared account, with their private data securely stored in the secret account that the other person is unaware of.

In our current design, the data in the shared tier is a subset of the data in the secret tier, i.e., all data is visible in the user's secret account, but only data specifically designated as safe to share is visible in the shared account. We chose this design because it is more privacy-preserving. For a photo to be shared, the user must explicitly mark it as such, rather than sharing everything by default, with users explicitly marking what is private. Since it is critical to keep the existence of the multiple accounts secret, *Nirapod* hides the existence of the secret account by providing a common entry point into both the shared and secret accounts, identifying which account to unlock using only the password entered (similar to the concept of panic passwords [19]).

Implementation

We explored the concept of 'tiered' privacy described above by implementing a prototype gallery application, called *Nirapod*, that stores and displays photos. We focused on photos because previous studies indicated that many users care deeply about the privacy of their personal photos [6], although the concept could be extended to other data types as well. Our current design uses two tiers of privacy (shared photos and secret photos) but could be extended to more than two tiers. Like many off-the-shelf privacy apps, *Nirapod* encrypts photos in a gallery that cannot be viewed without a password and that is meant to serve as a secure replacement for the default photo gallery.

Our design uses a password interface, with users setting one password to access the "shared" gallery and another to access the "secret" gallery. Using this design, a person can select photos they are willing to share, place them in the shared gallery, and safely share the password for this gallery. At the same time, they can place photos that they wish to keep private in their secret gallery, protected by a different password that is not shared with anyone.

We developed the *Nirapod* prototype as an Android application that is compatible with devices running Android version 6.x and above. *Nirapod* stores the passwords for both accounts in a local SQLite database and maintains two encrypted folders on the device's internal storage for each of the two accounts. The application interface was in English because the populations in Bangladesh that we target already have their operating systems set to English and are accustomed in using English interfaces. Figure 1 summarizes the application workflow. When a user installs the application and opens it for the first time, they are prompted to create two passwords: a shared and a secret password. Then, they are directed to a single login screen where they can enter either one of their passwords depending on the account that they wish to open. After logging into one of the accounts, the user is able to perform all normal gallery-related operations for that account. *Nirapod's* two galleries are nearly identical visually to further protect users from situations where they may be observed with the secret gallery open (Fig. 1). Within each account, available operations are:

Import photos: Move photos from the built-in gallery app to the currently open *Nirapod* account. The selected files are moved to the respective account folder maintained by *Nirapod* on the device's internal storage. The files are then removed from the built-in gallery.

Export photos: Move selected photos from the currently open *Nirapod* account to the built-in gallery app. The files are moved from the relevant *Nirapod* folder back to the original location on the device's storage. The files are then removed from *Nirapod*.

Delete photos: Delete the selected photos.

Change password: Change the password of the currently open *Nirapod* account.

Sign out of the currently open *Nirapod* account.

A few additional operations are only available when the user is signed into their secret account:

Show tier: See the current privacy status of photos in *Nirapod*. A lock icon indicates photos that are only visible in the secret account.

Move to secret account: Move the selected shared account photos to the secret account.

Move to shared account: Move the selected secret account photos to the shared account.

When *Nirapod* is installed on a device, a random AES (Advanced Encryption Standard) key is generated and stored in the device's SharedPreferences (an Android SDK API used to store and retrieve application preferences). When a photo is imported into *Nirapod* from the device's built-in gallery app, the image file is encrypted using the AES key. A corresponding thumbnail image is generated and encrypted using the same key. The encrypted image and thumbnail are then stored in the storage folder maintained by *Nirapod* and the original image is deleted. During an export operation these steps are reversed: the encrypted image is decrypted using the stored key, the decrypted image file is moved back to the original folder, and the encrypted thumbnail is deleted.

Since our focus is to explore the benefits and trade-offs of our design in contexts of shared device use, our initial prototype does not attempt to make the secret account completely undetectable by a technically-sophisticated adversary. Currently, photos stored in *Nirapod's* accounts could

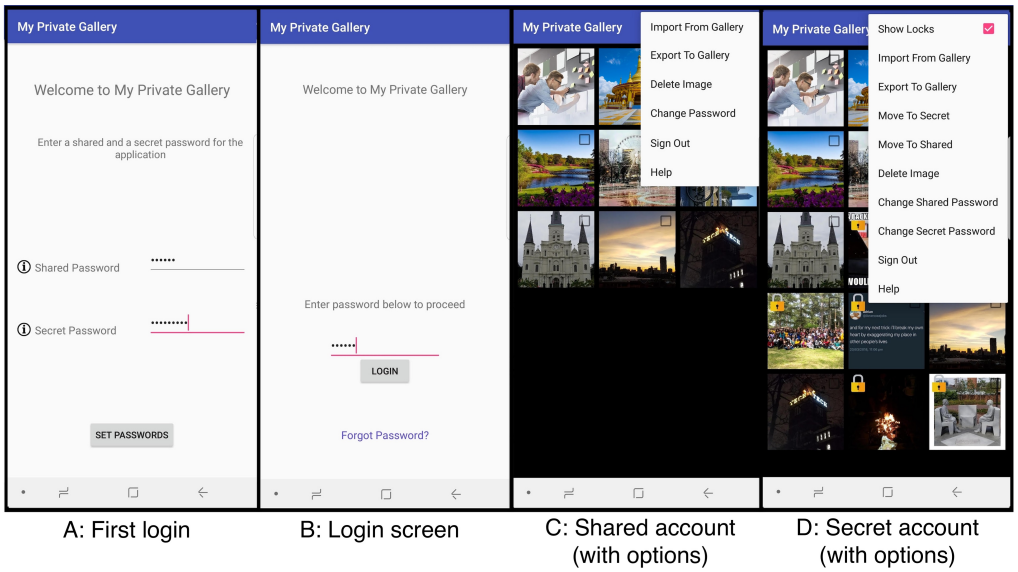

Figure 1: The *Nirapod* Interface: (A) the first login screen to set passwords for the secret and shared account; (B) the general login screen; (C) the shared account with options; and (D) the secret account with options.

be discovered in their encrypted form by a detailed inspection of the file system (i.e., although the contents of the files would not be known since the data is encrypted, an adversary could discover that the encrypted files exist). Many more sophisticated data obfuscation techniques exist (e.g., hiding encrypted photos through steganography, hiding the app icon, etc.) that could be used to enhance security in future versions of *Nirapod*, but are orthogonal to our focus on tiered privacy.

4 FIELD STUDY

After designing and testing our prototype, we conducted a three-week field study with 21 participants in Dhaka, Bangladesh. We wanted to understand the extent to which an app like *Nirapod* might fit the needs and usage patterns of people who frequently share their devices with others. All study procedures were approved by one Bangladeshi university and three North American universities' IRBs.

Recruitment and Procedure

We recruited participants through public social media posts, announcements at local universities, word of mouth, and personal contacts of the authors. We then performed snowball sampling [29] as those we initially recruited suggested people they knew to be sharing devices. We targeted a range of ages, professions, and genders. Participants only needed to possess a phone with Android version 6.0 or higher.

After recruitment, participants attended an in-person onboarding session. We began by explaining the purpose of the study, answering any questions participants had, and obtaining their consent to participate. Next we conducted a 15-minute semi-structured qualitative interview in Bengali that sought an understanding of participants' experience with technology, their privacy concerns and preferences, device usage and sharing habits, and demographics. After the interview, we installed the *Nirapod* app on the participant's phone and conducted a 30-minute training session to ensure that they understood the app and how to use it. The training was done by showing the participant a demo of the app on the researcher's phone, delivering a short presentation, and providing information sheets about how to use the app. After the training, participants were encouraged to use the app on their own devices until they felt confident and demonstrated they knew how to use it.

After installing the app and training participants, we asked them to use *Nirapod* in their daily lives for a period of three weeks. During this time, they were able to contact the researcher if they experienced any problems or challenges using the app. The system was instrumented to log all usage data, including when participants' used the app, features used, what actions taken, and so on.

After three weeks, participants were invited to come back to our lab where we conducted a semi-structured interview and, with their permission, collected the system usage logs off their device and helped them to uninstall the app. The interview asked about participants' experiences using the app, challenges and issues that they encountered, how it affected their privacy, how they shared the device and/or their passwords with other people during the deployment, and suggestions for improvement. At the end of the interview,

Gender	**Age (years)**
Women: 15, Men: 6	19–25 (Median: 22)
Relationship Status	**Education**
Single: 8	Completed High School: 6
In a relationship: 11	Undergraduate Student: 6
Married: 1	Completed Undergrad: 6
Unspecified: 1	Completed Masters: 3
Household Income	**Experience with phones**
Min: 0 USD/month	0 to 3 years: 3
Median: 361 USD/month	3 to 10 years: 14
Max: 2,410 USD/month	10+ years: 4

Table 1: Participants' Demographic Characteristics

we thanked participants and compensated them with 1600 Bangladeshi Taka (roughly US$20) for their time.

Data Collection and Analysis

Our data consists of qualitative interview data and quantitative data from system usage logs. Our qualitative interviews were transcribed and translated into English by two of the authors who are both native speakers of Bengali. The transcripts were then analyzed using thematic analysis [15]. After reading through the transcripts carefully, we conducted several rounds of iterative coding to identify patterns and converge on appropriate themes. Examples of codes in our analysis include *data misuse*, *fear of data loss*, and *family photos*. We then clustered the codes into overarching themes that we used to organize our findings. Examples of themes include *strategies for protecting privacy*, *challenges using the app*, and *suspicion of the app/researchers*.

In addition to analyzing our qualitative interview data, we conducted quantitative analysis of participants' system usage logs to understand how participants used the application during the study. When collecting these logs, we discovered that three participants' log files (P6, P10, P11) were corrupted. We believe that this was due to an operating system update during the deployment. We have therefore excluded these three participants from our quantitative data, although we still include their qualitative interview data. In addition, participant P1 began but chose not to complete the study. Our participant numbers thus range from P2 to P22.

5 CURRENT SHARING PRACTICES

Before analyzing how participants used *Nirapod*, we wanted to understand their current technology usage and privacy practices. Table 1 summarizes our participants' characteristics. All participants were young, relatively well-educated adults. The majority (n=15) were women. Although all participants owned their own smartphone devices, they also all (n=21) participated in some form of device sharing. The people that our participants shared devices with included significant others, friends, roommates, siblings, other relatives, and parents. The stories shared with us made it clear that, at least for our study sample, sharing occurred as a cultural practice rather than due to economic need. One prominent theme (n=14) was for a friend or relative to ask to use the participant's phone for a specific task, such as taking a photo or playing a game, and then browsing through their personal data without permission. P15 told us,

> *"When I get home, my aunts usually inspect my phone. Sometimes my cousin takes [it] to play games. After a while, I caught them browsing my personal stuff." (P15)*

As this quote suggests, another common practice (n=16) was for a parent, relative, or significant other to take the phone and *"inspect"* it, with the goal of monitoring who the participant had been talking to or messaging. Regardless of who participants shared their devices with, they all (n=21) expressed concern that sharing would result in their personal privacy being compromised. P17 said,

> *"While sharing my phone, I'm scared they might see some private things of mine. I always feel like, please give back my phone. Give back my phone before you see anything. I felt scared." (P17)*

The most common types of private data that participants described worrying about included personal photos (n=13), messages/chats (n=14), and social media data (n=10), with all participants describing at least some kinds of data that they would prefer not to share with others. Participants also described a variety of ways in which their personal privacy had been compromised by sharing their phones with others. Fifteen participants reported that friends or family members had previously misused their personal data in some way, including how their friends played *"pranks"* on them by posting information (e.g., photos) to their social media accounts without their permission. One described how friends would use her private information to *"blackmail"* her, saying, *"give me a treat or I will leak everything" (P9).* Another theme (n=5) that surfaced was for participants' parents or elders to scold them if they discovered content that they disapproved of, particularly if these involved photos of messages from a boyfriend or girlfriend. As P21 said,

> *"If I have any pictures of me and my boyfriend in my gallery, I might get into trouble at home. Or messages…I have to hide from others." (P21)*

Participants also explained that privacy compromises sometimes resulted in misunderstandings about the data that was discovered or people getting offended by the content, and privacy breaches frequently made participants feel frustrated, annoyed, and embarrassed. P6 said,

> *"Sometimes I am being scolded. It's really embarrassing. I am an adult. When I get scolded if they see any personal pictures and messages, that's really annoying." (P6)*

Despite these feelings, participants felt that they had no choice but to share their device, since sharing is normal and expected in Bangladeshi society. When describing how her friends compromised her private data, P20 said, *"but, you know, I can't really forbid them to use [my phone]".*

In response to these privacy challenges, our participants described using a variety of strategies they used to preserve their data privacy. Thirteen participants reported that they typically lock their device using built-in functionality, including screen locks and fingerprint locks, although five participants explicitly mentioned that they share their unlock pattern with others to enable device sharing. P19 said, *"I have passwords on my phone ... but everyone knows [my password]" (P19).* Ten participants reported at some point using a third-party application to lock content on their device, although half of these no longer used any special-purpose privacy apps. Four participants said that they did not use any access control mechanisms, and instead deleted all personal content from their device, with one telling us *"the strategy is DELETE DELETE DELETE!" (P6).* Most of these findings are aligned with prior studies in this area (see [6, 7, 54, 56] for example). This suggests that our participants share these challenges with thousands of technology users in South Asia.

6 HOW PARTICIPANTS USED NIRAPOD

Having understood participants' sharing practices and privacy challenges, we now examine how they used *Nirapod* during the study. Although they differed in terms of phone models, patterns of sharing, and people they shared devices with, participants' responses in our post-study interviews surfaced common themes that highlighted their excitement, hesitation, suspicions, and struggles using the prototype.

Usage During the Deployment

Our participants exhibited varying levels of app usage. The mean number of days people used the app was: 6.1 days (SD = 4.1 days). As shown in Figure 2, which depicts the number of days during the 21-day study that each participant used the app, some participants used the app on only a couple of days (min=2 days), while others used it almost every day (max=17 days). The fact that usage varied day-to-day is expected, since image saving and photo taking practices vary. We use two other metrics to evaluate usage: (a) the number of logins into each account (Fig. 3), and (b) the number of photos imported into the *Nirapod* app (Fig. 4). Again, we see that participants' usage varied for each of these metrics. One participant logged in over 60 times, while another only logged in twice. Over

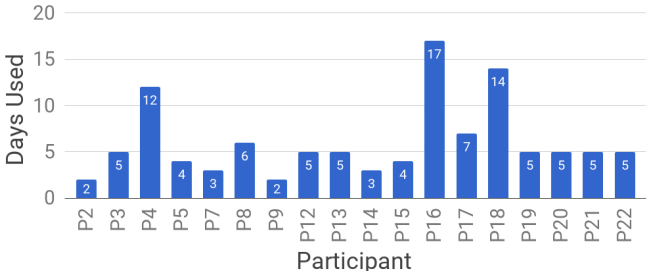

Figure 2: Number of days *Nirapod* was used by participants. (Three participants, P6, P10, P11, log files were corrupted and are therefore excluded from our quantitative data).

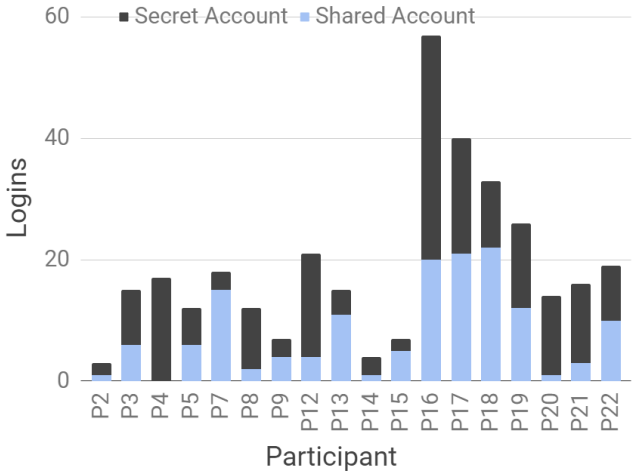

Figure 3: Number of participant logins into each account

52% of all logins to *Nirapod* were to the secret gallery. The numbers of images imported by participants are similarly skewed: two participants only imported seven photos, while one participant imported 130 photos (median=20.5 photos).

This data suggests that participants were generally able to use the main features of the app during the study, which also helps to triangulate the qualitative interview data that they provided. All participants (n=21) described how they used the app to hide their private photos. P18, who used the app on 15 out of 21 days, told us,

> *"(I used this app) almost every day. I imported photos, exported photos. Most of the days, I used this app at least two or three times." (P18)*

In addition, none of our participants reported having any difficulties understanding how the app worked. This finding is supported by our quantitative usage data. For example, Figure 3 shows the number of times each participant logged

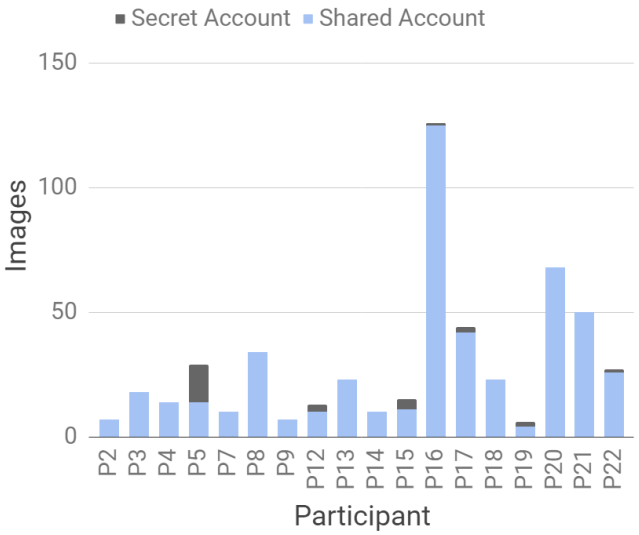

Figure 4: Number of images imported into Nirapod

into each of *Nirapod's* accounts. We see that most participants used *both* accounts by logging in to each one multiple times during the study. That said, our data does suggest that participants generally used the secret account more than the shared account: the median number of logins to the secret account was 9.5, compared to 5.5 for the shared account. However, Figure 4 shows that fewer images were imported into the secret account as compared to the shared account (although it was easy for participants to move photos between accounts). Several participants requested that we extend the app's functionality to other domains. P4 said,

> *"This is cool. I wish I had similar features for messenger. My messages are private. I cannot imagine what will happen if someone sees them."(P4)*

Six participants said they would be happier if there were more than two tiers of privacy. They described how, if the app becomes popular, people will soon know that there is an additional secret gallery, which will make it hard for them to keep it secret if put under pressure to reveal their password. To overcome this challenge, participants suggested that, instead of two accounts, they would like to have a system where they could make as many tiers as they choose. That way nobody would know how many tiers there were and their secret tiers would be able to remain *"unreachable"*.

Usage of Nirapod's Secret and Shared Tiers

When we asked participants what kind of photos they stored in their shared and secret accounts their responses varied. For example, 12 participants said that they stored family photos in their shared account, while the rest hid those photos in their secret account. Participants explained how their decisions of which account to use for particular photos were shaped by their relationships with the people that they shared their phones with. For example, P15 described how she often shares her phone with friends, and she thinks that photos of her family members should be hidden from them. As a result, she put photos of family in her secret account. On the other hand, P5 shares his phone with his family and saw no reason to hide family photos from them. All participants said they used the secret account to store photos they were not comfortable sharing with anyone. P21 said,

> *"I have some private photos in my secret account I don't want anyone to see. If anyone gets my phone and enters my gallery, then I don't want them to see the contents [of my private photos]. That is where this app was useful." (P21)*

The data that participants kept secret included photos of or with significant others: husbands, wives, boyfriends, girlfriends, or people they secretly admired. P14 said,

> *"I use the [secret] gallery for my personal photos, photos of me and my boyfriend. I don't want to share those photos with anybody." (P14)*

Safety When Using the Application

All participants said that the app made it safer for them to share their phones with others. As the previous section shows, before using our app, four participants did not store any private photos on their device for fear they would be discovered. However, with *Nirapod*, all participants said that they now felt comfortable storing their photos on their phone. For example, P15 lives in a college dormitory and does not share her phone with anyone there. However, when she visits her home, she shares her phone with her family members. Previously, she would not store any private photos on her phone because she feared that her siblings would see them, and it is very difficult for her to say no to her siblings if they ask for her phone's password. However, in her post-study interview, she told us that she could now store her private photos on her phone using our app and still share the phone with her siblings, describing that she felt a lot safer this way.

All participants (n=17) who reported already storing private photos on their phones described how, before our study, sharing their phone with anyone made them feel anxious or afraid. However, in the post-study interviews, they described how they now felt much more secure sharing their device when using our app. One such participant said,

> *"If anyone from my home wants to see my phone I can give it to them easily now. I don't even need to lock my phone right now." (P18)*

When we asked participants what happened when the people they shared their phone with tried to check their photos, they all said that the photos in their secret account could

not be reached by those people. No participants reported having their secret photos exposed to others at any point in the study. For example, P21, who shared her phone with her boyfriend, described how she stored some secret photos in her phone that she did not want him to see:

> *"When he checked my phone, he found both the [built-in gallery] and [Nirapod]. He wanted to check [Nirapod] and I gave him my shared password, but I was still safe. He never knew there was another secret gallery there." (P21)*

However, the people that participants shared their phones with were not always happy if they discovered that photos could be hidden using our app. Several women reported facing this challenge and in most cases, it was their husbands or boyfriends who were unhappy. Three described how they had been asked about their reason for using *"another app"* to store photos. They were also asked why they needed an *"extra layer of privacy"*. In some cases, the boyfriends/husbands were supportive of using *Nirapod* to hide photos that they took with our participants from other people, but they were not happy if they found out that participants could hide photos from them. P16 said,

> *"My boyfriend sounded very positive in the beginning. He said now we could save our photos safely in my phone. But as soon as he realized I could hide something even from him, he looked anxious. I think he was upset because he did not like me hiding anything from him." (P16)*

Usability Challenges During the Deployment

Although participants generally found *Nirapod* to be useful, they also experienced challenges using the app. The most common problem participants reported was remembering multiple passwords. Six out of our 21 participants said that they had difficulty remembering two passwords. Two participants told us that they forgot at least one password or got confused about which password they had set for which gallery. Further, six participants described being afraid that they would put the wrong password into the app in front of others and their secret photos would be revealed. P14 said,

> *"I always feel scared about what password I am giving—is that my shared or my secret one? . . . It is a two-password system and you have to give the inputs in the same box. So, it can easily create confusion in your subconscious mind when entering the password. If you mistakenly put the secret instead of the shared password, your private photos will be visible to everyone." (P14)*

Interestingly, even as participants shared their struggles remembering passwords for two accounts, many described wanting to have more accounts with different tiers of secrecy. Moreover, despite facing challenges remembering their passwords, they still felt that the app was safer than the current status quo, with one participant commenting, *"obviously it's better than the normal gallery app because of this two-password system" (P20).*

Participants were also anxious about what would happen if their phone got lost or broken. One advantage of the Android gallery is that it automatically saves a copy of their photos in cloud. Since our app did not have automated syncing, they worried about losing their photos. P10 said,

> *"My photos are automatically stored in Google. That way I know that even if I delete photos on my phone, they are not lost. That way I can also save some space on my phone. This app does not give that option. What will happen if my phone is broken or lost?" (P10)*

Another participant said it was confusing to have two different gallery apps. After taking a photo they would get confused about where to store it and were afraid they might store the photo in a *"wrong"* location and later forget where they had put it. To overcome this challenge, participants suggested that we integrate cloud-syncing features into *Nirapod*, telling us that their photos would then be safely stored and they would still get better control over their privacy.

Suspicions Regarding the App/Researchers

Finally, our post-study interview data yielded an interesting theme in which participants described being suspicious of our experimental app and our intentions as researchers. For example, we received questions regarding where and how participants' photos were being stored. We explained to them that photos in *Nirapod* were encrypted and did not leave their device. As a result, no one, including us (the researchers), had access to their photos. Despite this explanation, four participants were still worried that we, the developers, would have access to their secret photos. One said,

> *"Facebook and social media already have all our personal data. I don't want to allow another app into my private space. If some [app] wants to store my private data, I will refuse. I don't trust it will store my data and not use it for their benefit." (P2)*

One participant also described how his friends discouraged him from using *Nirapod*, saying that the app would steal his data and make a business out of his private information. Another participant told us that he had been discussing our app with his friends, and his friends asked him,

> *"If this app is so secret, why it is not on Google Play? So we can check what other people say about this app." (P2)*

We (again) explained that our app was a research prototype that was being deployed experimentally, rather than a commercial product. Although we answered all of our participants' questions, it still seemed to us that one or two were not totally convinced. They wanted to *"check more"* before they felt they could use our app *"seriously"*.

7 DISCUSSION

Our findings yield numerous insights that explore how participants care about and manage the privacy of their personal data while also sharing devices. Data from our own participant interviews and from prior work [6] suggests that the fundamental issue is not that people in South Asia *do not have* personal data that they wish to keep private; rather, they want to maintain their personal privacy and *also* be able to safely share devices with friends and family. Our tiered design explicitly supports this broader usage model in an effort to help participants manage this trade-off.

Rather than seeing *Nirapod* as a final "solution" to the problem of privacy with device sharing, we instead view our prototype more as a design provocation. As such, findings from our deployment are useful primarily because of the ways they challenge and expose for future analysis a range of interesting tensions and dynamics around managing privacy while sharing devices, as we now discuss.

Plausible Deniability

The term 'plausible deniability' refers to the ability of a person to deny blame because evidence does not exist to confirm responsibility for an action. In other words, the lack of evidence makes the person's denial credible, or plausible. Our design attempts to provide users with plausible deniability by providing a single entry point to *Nirapod's* multiple accounts. As such, people cannot tell from looking at the app login page that multiple accounts exist. Instead, the system determines which account to open (and thus what data to reveal) based solely on the password entered. Findings from our study suggest that this mechanism generally worked, with participants describing how they were able to safely share devices without revealing that another secret account existed. Providing participants with plausible deniability is important because device-sharing in Bangladesh is a social and cultural norm, with people expected to share their devices if they wish to be thought of as good citizens [6]. When sharing devices, it is not socially acceptable to log out of one's account before handing it over to a friend or family member since such behavior implies a lack of trust in the other person or creates suspicion by suggesting that there is something to hide [6].

However, the sustainability of ensuring plausible deniability is challenging in the long term, and it is likely that the efficacy of our approach would deteriorate as other users become aware of how *Nirapod* works. To overcome this limitation, the design of *Nirapod* could be extended to support an arbitrary number of different tiers, which would allow users to retain plausible deniability. Under such a model, as one of our participants pointed out, there would be no way for a potential adversary to know how many tiers exist. Moreover, *Nirapod* could be adapted to allow multiple users to each have their own invisible secret accounts so that no single user prevents others from enjoying the same privacy benefits on a shared phone. At the same time, it is possible that cultural norms with respect to technology may start to shift, perhaps making it more culturally acceptable for people to keep some data private while still sharing devices. If this happens, our approach may still provide a graceful way for people to preserve their privacy by reducing social friction and avoiding questions of trust that might arise if they needed to stop and logout of an account or device before handing it over to someone else.

Of course, making it easier for people to hide data from each other introduces social and ethical considerations. For example, there are potential implications that need to be considered should a person's private data be discovered. Several of our participants suggested that they would *"get into trouble"* if their parents or significant others discovered data they disapproved of. The fact that participants so readily adopted and used *Nirapod* was somewhat surprising; we expected more push back on the cultural acceptability of keeping secrets. Instead we found that, for many people, keeping secrets is a norm (findings also supported by [54]), and *Nirapod* made it possible to do so in ways that were usable and comfortable. Thus, our work is not introducing the concept of hiding data or keeping secrets for these participants; instead, we see our work as complementary to participants' existing strategies for preserving their privacy by providing them with another option for keeping their private data safe. These findings expand our understanding of how privacy is conceived in communal contexts as well as the cultural acceptability of privacy-preserving designs like *Nirapod*.

Gendered Privacy

Although our sample size is too small to make any general claims about gender and privacy, our data does hint at a number of potentially gender-related privacy issues. Our experience in the field was that our participants who were women were generally more concerned about the privacy of their personal data and more interested in new tools that might provide better privacy. In addition, our qualitative interviews suggest that our women participants were more often quizzed about their use of the app, usually by family members or boyfriends who were used to being able to *"inspect"* their device and keep track of their activities.

Although we cannot attribute these observations solely to gender, they do corroborate prior work examining technology and gender in the context of patriarchal societies [4, 8, 57]. Bangladesh is a socially-conservative society, and the consequences of privacy breaches may be higher for women. For example, a leaked sensitive photo could compromise a woman's reputation, reflect poorly on her family, and lead to her becoming socially ostracized. In addition, in patriarchal societies like Bangladesh, men often control women's access to technology, making it difficult for women to have any expectation of privacy [57]. This kind of device inspection and surveillance by family members has been discussed in the context of intimate partner violence in the US [27, 28, 46], but we find that this behavior is a social norm in Bangladesh. In our work, the fact that women find it more challenging to keep data private may make them more motivated to try out and use our app. At the same time, it heightens the potential issues they may face if they were to be caught hiding data. Further exploration of the gendered nature of privacy is a fruitful avenue for future research.

Usability Challenges

Our participants faced a number of usability challenges using *Nirapod*. Several of these were relatively minor suggestions for additional functionality, such as integrating *Nirapod* with the device's camera software or syncing photos to a backup cloud service. A more fundamental usability challenge that participants experienced stemmed from the additional overhead of needing to remember another password, which in turn led to confusion and anxiety about entering the incorrect password in the presence of others. Trouble remembering passwords is a well-known problem in security and privacy research [25, 34]. The overhead of remembering an additional password is somewhat tied to the use of password authentication to begin with, and using different authentication mechanisms (e.g., fingerprints) or easier to remember passwords may help to alleviate this burden.

Entering the wrong password is a more direct consequence of our interface design, although this could possibly also be mitigated with appropriate password selection (e.g. using the password itself as a mnemonic for which account is opened) or other more creative interface designs (e.g., using an identical but longer password for the secret account). The mental burden of memorizing passwords could be alleviated by other solutions like biometric authentication (e.g., fingerprints from different fingers used to open different accounts). However, participants may equally forget which finger they chose for which account. We consider these interface design issues to be areas for future study.

Interestingly, even as our participants were describing that they found it difficult to remember two passwords, they asked us to provide more than two tiers of privacy, which would presumably require even more passwords. In general, participants usage of our two-tiered prototype and enthusiasm for more tiers suggests that, despite usability challenges, *Nirapod's* single entry point into multiple data stores is a promising and generalizable privacy mechanism for contexts of shared use. Future work might explore how such an approach could be utilized for different application domains, such as messaging services or social media applications. Another option could be to implement this mechanism at the operating system (OS) level to mimic the functionality of a device's built-in lock screen. However, an OS-level intervention would require users to install a custom version of the OS, which would involve rooting their device. This would make it challenging or impossible to deploy the system on participants' own devices.

Limitations

Our work has several limitations. First, our study had a small sample of only 21 participants and further research is necessary to understand if or how our findings might generalize beyond our participants. The three-week deployment is also a relatively short period of time, and longer deployments are necessary to understand how people might use the app long term. We also acknowledge that we deployed a technological intervention with participants and then conducted qualitative interviews asking what they think, which may introduce participant response bias [21]. We worked to triangulate the qualitative stories that we received from participants with quantitative usage data. We also tried to focus our findings and discussion on issues that came up rather than how much participants said they liked our app. Another limitation is that snowball sampling may have recruited people who have an above-average interest in privacy. We tried to reach a population with diverse privacy habits by offering compensation of USD $20, but acknowledge that our participants may be more privacy-conscious than the general population.

8 CONCLUSION

Our research explores the problem of how to provide better privacy for people who share devices. We designed an exploratory prototype based on the concept of tiered privacy. This model enables a user to create a 'shared' account that contains data they are willing to share and that is assigned a password that will be shared, and a 'secret' account that contains data they prefer to keep secret and uses a password they do not share. Our findings from a three-week field study with 21 participants in Bangladesh expose a range of interesting cultural, social, and usability tensions and dynamics that arise when people use our prototype to manage their personal privacy while sharing devices. Although these findings constitute a valuable step forward in designing technology that better fits people's usage patterns, future studies are

needed to explore how this model might further impact or challenge notions of privacy in South Asia.

9 ACKNOWLEDGEMENTS

We thank our study participants and anonymous reviewers for their contributions to this work. This research was funded in part by NSF grant #1748903 and by Facebook.

REFERENCES

[1] Norah Abokhodair. 2015. Transmigrant Saudi Arabian youth and social media: privacy, intimacy and freedom of expression. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 187–190.

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

[3] Shane Ahern, Dean Eckles, Nathaniel S Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 357–366.

[4] Syed Ishtiaque Ahmed, Nova Ahmed, Faheem Hussain, and Neha Kumar. 2016. Computing beyond gender-imposed limits. In *Proceedings of the Second Workshop on Computing within Limits*. ACM, 6.

[5] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. ACM, 11.

[6] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (2017), 17:1–17:20 pages.

[7] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 906–918.

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

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

[10] Syed Ishtiaque Ahmed, Maruf Zaber, Mehrab Bin Morshed, Md. Habibullah Bin Ismail, Dan Cosley, and Steven J Jackson. 2015. Suhrid: A Collaborative Mobile Phone Interface for Low Literate People. In *Proc. DEV'15*. ACM, 95–103.

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

[12] Thierry Bardini. 2000. *Bootstrapping: Douglas Engelbart, coevolution, and the origins of personal computing*. Stanford University Press.

[13] Rachel F. Baskerville. 2003. Hofstede never studied culture. *Accounting, Organizations and Society* 28, 1 (2003), 1–14.

[14] Seyla Benhabib. 2005. Borders, boundaries, and citizenship. *PS: Political Science & Politics* 38, 4 (2005), 673–677.

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

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

[17] Mead Cain, Syeda Rokeya Khanam, and Shamsun Nahar. 1979. Class, patriarchy, and women's work in Bangladesh. *Population and Development Review* (1979), 405–438.

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

[19] Jeremy Clark and Urs Hengartner. 2008. Panic passwords: Authenticating under duress. *HotSec* 8 (2008), 8.

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

[21] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. Yours is better!: participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1321–1330.

[22] Serge Egelman. 2013. My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2369–2378.

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

[24] David H Flaherty. 1989. *Protecting privacy in surveillance societies*. Chapel Hill: University of North Carolina Press.

[25] Alain Forget, Sonia Chiasson, and Robert Biddle. 2007. Helping users create better passwords: Is this the right approach?. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*. ACM, 151–152.

[26] Nancy Fraser. 1995. Politics, culture, and the public sphere: Toward a postmodern conception. *Social postmodernism: Beyond identity politics* 291 (1995), 295.

[27] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction* Vol. 1, CSCW (2017), Article 46.

[28] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. (2018).

[29] Leo A Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

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

[31] GSM Association. 2018. Country overview: Bangladesh. https://www.gsmaintelligence.com/research/?file=a163eddca009553979bcdfb8fd5f2ef0&download. [Online; accessed June 27, 2018].

[32] Jürgen Habermas. 1994. Three normative models of democracy. *Constellations* 1, 1 (1994), 1–10.

[33] SM Taiabul Haque, Matthew Wright, and Shannon Scielzo. 2014. Hierarchy of usersŒş web passwords: Perceptions, practices and susceptibilities. *International Journal of Human-Computer Studies* 72, 12 (2014), 860–874.

[34] Morten Hertzum. 2006. Minimal-feedback hints for remembering passwords. *interactions* 13, 3 (2006), 38–40.

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

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

[37] Haiyan Jia, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proc. CSCW'15*. ACM, 583–599.

[38] Joseph 'Jofish' Kaye. 2011. Self-reported Password Sharing Strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2619–2622. https://doi.org/10.1145/1978942.1979324

[39] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3393–3402.

[40] Ponnurangam Kumaraguru and Lorrie F Cranor. 2006. Privacy in India: Attitudes and Awareness. *Privacy Enhancing Technologies* (2006), 243–258.

[41] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and Users' Experience of Obfuscation As a Privacy-Enhancing Technology for Sharing Photos. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 67 (Dec. 2017), 67:1–67:24 pages.

[42] Carolyn A Lin. 1998. Exploring Personal Computer Adoption Dynamics. *Journal of Broadcasting & Electronic Media* 42, 1 (1998), 95–112.

[43] Heather R Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer, and Jason Watson. 2009. Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites. In *Proc. CSE'09*, Vol. 4. IEEE, 985–989.

[44] Yabing Liu, Krishna P Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 61–70.

[45] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll Just Grab Any Device That's Closer": A Study of Everyday Device and Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 5921–5932.

[46] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.

[47] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. In *Proc. CSCW'17*. ACM, 581–593.

[48] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Wash L. Rev* 79, 119 (2004).

[49] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[50] Tapan S Parikh and Koushik Ghosh. 2006. Understanding and Designing for Intermediated Information Tasks in India. *IEEE Pervasive Computing* 5, 2 (2006), 32–39.

[51] Tapan S Parikh, Koushik Ghosh, and Apala Lahiri Chavan. 2003. Design studies for a financial management system for micro-credit groups in rural india. In *In ACM SIGCAPH Computers and the Physically Handicapped*. 15–22.

[52] Sandra Petronio and Wesley T. Durham. 2008. *Interpersonal Communication: Multiple perspectives* (1st ed.). Sage Publications, USA, Chapter Communication privacy management theory, 309–322.

[53] Norman Sadeh, Jason Hong, Lorrie F Cranor, Ian Fette, Patrick Kelley, Madhu Prabakar, and Jinghai Rao. 2009. Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. *Personal and Ubiquitous Computing* 13, 6 (2009), 401–412.

[54] N Sambasivan, G Checkley, A Batool, N Ahmed, D Nemer, LS Gaytán-Lugo, T Matthews, S Consolvo, and E Churchill. 2018. Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association.

[55] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated Technology Use in Developing Communities. In *Proc. CHI'10*. ACM, 2583–2592.

[56] Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri. 2018. Privacy at the Margins: The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India. *International Journal of Communication* 12 (2018), 20.

[57] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. (2018).

[58] Tech Crunch. 2017. Why Android Jelly Bean 4.2's Multiple User Account Switching Is Tablet-Only? (Hint: Nokia Patented It For Phones). https://techcrunch.com/2012/10/29/why-android-jelly-bean-4-2s-multiple-user-account-switching-is-tablet-only-\hint-nokia-patented-it-for-phones. [Online; accessed July 10, 2017].

[59] Ronald L Thompson, Christopher A Higgins, and Jane M Howell. 1991. Personal Computing: Toward a Conceptual Model of Utilization. *MIS quarterly* (1991), 125–143.

[60] Harry C. Triandis. 2018. *Individualism and collectivism*. Routledge.

[61] Emanuel von Zezschwitz, Sigrid Ebbinghaus, Heinrich Hussmann, and Alexander De Luca. 2016. You Can't Watch This!: Privacy-Respectful Photo Browsing on Smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4320–4324.

[62] Samuel D Warren and Louis D Brandeis. 1890. The right to privacy. *Harvard Law Review* (1890), 193–220.

[63] Alan F Westin. 1968. Privacy and freedom. 25 Washington and Lee Law Review. 166.

[64] Wikipedia. 2018. Cambridge Analytica Data Scandal. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal. [Online; accessed April 19, 2018].

[65] Pamela Wisniewski, AKM Islam, Bart P Knijnenburg, and Sameer Patil. 2015. Give social Network Users the Privacy They Want. In *Proc. CSCW'15*. ACM, 1427–1441.

[66] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Preventative vs. Reactive: How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proc. CSCW'15*. ACM, 302–316.

[67] Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2014. Adolescent Online Safety: The Moral of the Story. In *Proc. CSCW'14*. ACM, 1258–1271.

[68] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proc. CSCW'16*. ACM, 1676–1690.