"We Don't Give a Second Thought Before Providing Our Information": Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh

Mahdi Nasrullah Al-Ameen
Utah State University, USA
mahdi.al-ameen@usu.edu

Tanjina Tamanna
University of Dhaka, Bangladesh
turnatatatu666@gmail.com

Swapnil Nandy
Jadavpur University, India
swapnilnandy2@gmail.com

M A Manazir Ahsan
Utah State University, USA
manazir.ahsan@aggiemail.usu.edu

Priyank Chandra
University of Toronto, Canada
prch@cs.toronto.edu

Syed Ishtiaque Ahmed
University of Toronto, Canada
ishtiaque@cs.toronto.edu

ABSTRACT

With a rapid increase in the use of digital technologies, people in the Global South including Bangladesh are exposed to a wide-range of smartphone applications (termed as *apps* in this paper), which offer a variety of features and services. However, privacy leakage through apps has increasingly become a major concern in Bangladesh, where the app collecting users' sensitive information without their consent was reported in news media for privacy violation. Our study with 32 participants from varying age, literacy level, and profession in Dhaka, Bangladesh unveils the perceptions of people around data collection and sharing by the app reported in privacy leakage news. All of our participants were aware of information leakage through the app they use, where they possess varying perceptions around providing personal information, like a sense of benefit, necessity and contribution, indifference, fear, or (no) authority over data collection. Our analysis reveals the relation between users' privacy perceptions, local infrastructure, and social practices in Bangladesh, where we identify the situated challenges that interfere with people's understanding of privacy notice. Our results lead to a discussion on how people's privacy perceptions are influenced by rapid urbanization and the opportunities offered by digitization in Bangladesh. Based on our findings, we provide recommendations to develop situated and sustainable strategies to enhance privacy awareness and practices in the social setting of Bangladesh, and Global South.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; **User studies**; • **Security and privacy** → **Human and societal aspects of security and privacy**.

KEYWORDS

Privacy, Global South, Interview.

COMPASS '20, June 15–17, 2020, , Ecuador

ACM ISBN 978-1-4503-7129-2/20/06…$15.00
https://doi.org/10.1145/3378393.3402244

ACM Reference Format:
Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, M A Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. "We Don't Give a Second Thought Before Providing Our Information": Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS) (COMPASS '20), June 15–17, 2020, , Ecuador*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3378393.3402244

1 INTRODUCTION

Bangladesh, a developing country in South Asia, has experienced a recent boom in digital technology use fueled by the government's initiatives of transforming the country into "Digital Bangladesh" [50, 57, 89]. As of February 2019, Bangladesh is the ninth largest mobile phone market in the world in terms of the number of subscribers [54], where the smartphone market in Bangladesh is reported to have a recent 45% growth year-on-year (YoY) [25]. In addition, about 100 million people which is 55% of the total population in Bangladesh [14] now have the Internet access [30]. With such advancement in technology use, digital privacy issues need to be identified and addressed with further importance in the context of Bangladesh [5, 70, 85].

Like many other developing countries in Global South, Bangladesh is shifting from traditional paper-based system to digital medium for managing information and services [5, 17, 111]. With the recent advancement in technology use, smartphone apps (termed as *apps* in this paper, unless otherwise specified) are becoming increasingly popular in Bangladesh, many of which have been launched to meet specific local needs [31, 61, 92]. Subsequently, with new business opportunities opening, people have started to get the benefits of app-based services including mobile banking, ride sharing, and social communication [61, 92].

However, privacy leakage through apps has increasingly become a major concern in Bangladesh. In 2018, the ride-sharing app 'Pathao' was in the news for collecting users' personal information not required for its core functionality [48, 62, 64], including SMS and contact list. Users were not notified about the purpose of collecting user private data, and the incident was identified as an act of privacy violation [48, 62], with the news media even comparing it to malware used by adversaries to steal user information [64].

Our study positions itself in this transitional period when the app-based digital economy is booming in the Global South while

being accompanied by increasing risks of privacy leakage through these apps. This paper studies how users balance their needs, conveniences, and privacy in the context of data collection and sharing by apps, with a focus on how privacy leakage incidents affect app usage behavior. We emphasize that addressing these research questions would lead the ICTD and privacy research community to develop situated strategies to help local people with making informed decision while balancing between their app usage and privacy protection.

In our study, we interview 32 participants living in Dhaka, the capital city of Bangladesh, who were aware of privacy leakage through their apps and find that they possess varying perceptions around sharing personal data. Information collection is deemed necessary by participants who believe that their data contribute towards improving app's features, expanding business and earning revenue, and ensuring digital and national security. Some participants are in favor of data collection considering the benefits they get in return, including personal safety, convenience, and personalized offer. On the other hand, some of our female participants reported concern about social harassment and physical danger as a consequence of information leakage. We also find instances where participants feel no authority over their information and believe that apps could collect any information they want. Most of our participants who perceive no control over their data or have a sense of fear about information collection by apps initiated a social discussion after learning about the privacy leakage incident; however, the privacy behavior after social discussion varied across participants.

Based on our findings, we discuss how the challenges introduced by the rapid urbanization of Dhaka, Bangladesh and the opportunities offered by digitization influence people's privacy perceptions and behavior. We shed light on privacy dependency and describe the corresponding risks and opportunities. We also identify the local challenges in Bangladesh that interfere with people's understanding of privacy notice, and outline the alternate sources leveraged by our participants to build their privacy perceptions. Our findings lead to recommendations on how we could develop situated and sustainable strategies for local people in Bangladesh to make informed privacy decision. Taken together, our study contributes to advance the technology and development community's understanding of privacy in the digital landscape of Bangladesh, in particular, and the Global South, more generally.

2 RELATED WORK

With the increasing use of computing technologies, people have been exposed to a variety of privacy issues and security vulnerabilities, many of which are related to users' perceptions and behavior [56, 88, 103]. The studies around privacy have predominantly been influenced by Western liberal values, including the early work of Warren and Brandeis [102], and Westin's call for freedom from surveillance [106]. These values were later incorporated into many academic disciplines including sociology, political science, law, and recently computing technologies [58, 69].

In the area of computing technologies, recent research have focused on understanding the security behavior of users [10, 11, 104, 105], and the relations between users' privacy mental model and various socio-technical factors, like their technical knowledge and efficacy [46, 65, 88], sense of responsibility [33, 46, 66], past experiences [33, 77, 100], risk perceptions [13, 37, 43, 45], and the familiarity with a technology and brand [38, 55, 112]. However, all of these studies are conducted in Western contexts, which may not be compatible with the community-based, traditional, and hierarchical social structure of the Global South [39, 44].

As suggested in prior literature [32, 68, 73], privacy is contextual that demands a situated understanding in order to explore the design and policy practices. The findings from recent usable privacy studies [3, 24, 59] 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 [28, 101]. Below, we briefly discuss about the notable usable privacy studies conducted outside the Western contexts.

Although online threats are global, perceptions of threat are very localized [24, 59]. The study of Kumaraguru et al. [59] demonstrated the privacy perceptions of people in India, where around one-fifth of participants were not concerned at all about public posting of their grades or railway reservation information (e.g., name, seat number in a train). In another study, Chen et al. [24] investigated the security and privacy practices of the people in urban Ghana while browsing Internet. The study [24] shows that participants judge the trustworthiness of a website based on appearance, lack of popups, and loading speed. Participants reported confidence of being able to defend against cyberattacks despite passwords often being their only line of defense. Given the low incidence of local cybercrime, authors found the current security practices of people to be adequate in Ghana for the time being [24].

The religious views and cultural norms of people have impact on their sense of confidentiality and privacy. The study of Abokhodair et al. [1] examined how the youth in 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 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 with a goal of preserving respect and modesty. The study of Alghamdi et al. [12] investigated the security practices for households bank customers in the kingdom of Saudi Arabia, where the authors identified 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.

Digital harassment is a growing concern in many developing countries, where in majority of cases female users are the victims of such incidents [7, 70]. The study of Nova et al. [70] reveals the online harassment that women in Bangladesh have to encounter in an anonymous social media (ASM). Participants reported to receive sexually offensive messages and dating inquiries from the people in ASM. While public discussion on sex or any topic containing sexual contents are considered taboo and frowned upon in Bangladesh [67, 81], 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. [87] identified that the risks and

Table 1: The Highlight of Participants' Demographic Traits [*Either completed or currently studying at undergraduate level]

Gender	Participants
Male	P1, P3, P4, P7, P8, P10, P15 - P26, P28, P29, P32
Female	P2, P5, P6, P9, P11 - P14, P27, P30, P31
Age-range	
18-29	P1 - P22
30-39	P23 - P26
40-49	P27, P28, P30
50-64	P29, P31, P32
Literacy Level	
Fifth Grade	P21, P23
Tenth Grade	P22, P24
Twelfth Grade	P25 - P27
Undergraduate and above*	P1 - P20, P28 - P32
Profession	
Student	P2, P4, P6 - P9, P11 - P13, P15, P16
Employee at Private Organization	P3, P14, P18 P19, P25, P32
Shopkeeper	P22, P24, P26
Physician	P1, P5
Housewife	P27, P30
Musician	P28, P29
Employee at Government Organization	P31
Cook	P21
Car Driver	P23
Banker	P17
Businessman	P20
Unemployed	P10

fear of harassment refrained the women in urban India to provide their phone number for accessing public Wi-Fi services.

People may have to compromise with privacy as their personal information is collected in process of building an identity system by the government [5, 93]. The study of Srinivasan et al. [93] explored the privacy perceptions of low-income people in India while dealing with the state's identity system, named 'Adhar' that assigns a unique 12-digit number to each Indian resident based on biometric identifiers. Many participants are comfortable with the digital identity system as they consider computer to be safer than paper records, where some participants reported their ignorance about the system and unwillingness to know more [93]. Participants reported higher trust on government than the private sectors to protect their information [93], while Jacobson [51] noted that the government is more interested in surveillance over citizens than ensuring their security. In the context of introducing biometric information-based identity management for mobile SIM registration in Bangladesh, the study of Ahmed et al. [5] unpacked the privacy and security vulnerabilities in this process. The authors [5] identified a wide-range of concerns among participants including the fear of political exploitation, commercial use, and invasion into their privacy through exploiting their biometric information.

The digital devices (e.g., mobile phone) designed for developing regions often fail to satisfy their local needs. In a study conducted with low-literate Berber women in Morocco [34], 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 phone, which contributed to the mobile utility gap in that community. The studies conducted by Ahmed et al. [4] and Sambasivan et al. [86] demonstrate that the mobile phones often do not have a 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 a digital technology could disrupt the relationships with friends and family members [4, 86]. In a separate study with the women in Global South [85], the authors identified the privacy negotiation of female users from their family members while using mobile phone. The authors [85] identified a set of performative practices the participants adopted to maintain their privacy, which include management of phone and app locks, content deletion, use of private modes, and technology avoidance.

The overall findings from these studies indicate that the misconceptions about a local culture by developers or designers may result in inappropriate threat modeling, and thus, the technologies and strategies for privacy protection that are developed on Western liberal values often fail to work in the different cultural settings of Global South. In these contexts, there is a dearth in existing literature on Global South in understanding people's perceptions of information collection and sharing by digital applications, like mobile apps. As the first step to address this gap, we conducted a study in the urban area of Bangladesh where mobile apps have started to become popular in recent years [31, 61, 92].

3 METHODOLOGY

Between February and June 2019, we conducted 32 semi-structured interviews with the people in Dhaka, Bangladesh. Our study was approved by the Institutional Review Board.

3.1 Recruitment

We recruited participants through two primary methods: the authors' personal connections, and snowball sampling. We communicated with them in person, over email, or via telephone explaining them the goals and ethics of the study. Once the participant agreed to take part in the study, we settled a time and venue for in-person interview as per the convenience of the participant. Most of the college-aged participants preferred to meet at a restaurant or cafe, while some of our participants, like the shopkeepers and professionals preferred to meet at their workplace. For relatively older participants, the researchers visited them at home to conduct the interview. According to the Bangladeshi custom [42, 95], no compensation was given. However, the participants were offered light refreshment, like snacks and beverages.

3.2 Participants

We provide a highlight of our 32 participants' demographic traits in Table 1, who were from diverse age-range, literacy level, and profession. For example, the age of the participants P1 to P22 were between 18 and 29, while the age of participants P27 to P32 were between 40 and 64. The participants P21 to P24 did not study beyond tenth grade, while participants P25 to P27 discontinued their academic education after twelfth grade. The other participants had at least a bachelor degree, or currently an undergraduate student. We

interviewed a diverse group of participants, including student, musician, housewife, physician, banker, car driver, shopkeeper, cook, and the employee at government and private organization. Except P7 who had formal training in Cyber Security, none of the participants had any degree, formal training, or professional experiences in Cyber Security. All of our participants use apps.

3.3 Procedure

We conducted the interview in local language (Bengali). Upon getting consent from the participants, we asked them about their general app usage behavior, and perceptions of information collection and sharing by apps, followed by the questions on their perceptions of deletion provision offered by the apps. In the later part of interview, we asked about their reaction to the news on privacy leakage incident involving the app they use. We also asked them about the behavior and challenges around reading and understanding the privacy policy of apps. The interview ended with a set of demographic questionnaire. The participants gave consent to audio record the interviews. On average, each interview took between 20 and 30 minutes.

3.4 Analysis

We transcribed the audios and translated them into English. We then performed thematic analysis on our transcription [21, 22]. We conducted multiple passes through the data in which we iteratively identified and clustered themes or codes present in the data. Two researchers independently read through the transcripts of several 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 further organized and taxonomized our codes into higher-level categories.

4 RESULTS

Our participants had been using apps in their smartphone for above two years, where about half of them reported using the apps for above five years. Most of our participants use the ride-sharing, social networking, and communication apps, where a few participants also use online banking, utility, game and entertainment, and antivirus apps. The participants reported using apps multiple times a day. To note, in social setting of Bangladesh, sometimes people are expected to share their smartphone with family members [4, 6]. A few of our participants reported using apps from a smartphone that is shared with their family members. However, the sharing expectations may not be always well lined up with the willingness to share, leading P15 to remove an app to avoid possible conflicts with family members.

Our participants learned of multiple privacy leakage incidents related to the apps they use, where most of them mentioned about the news on a popular ride-sharing app in Bangladesh. Participants also reported of information leakage incident through a widely-used social networking app. These news informed them of the app sharing its users' personal information and sensitive credentials with other entities, which could put their privacy at risk. The participants learned about information leakage incidents from different sources, including digital news shared over social networking sites, printed newspaper, and in-person communication with friends and family members. In the majority of cases, participants continued using the app without taking any privacy-preserving step despite learning about the incident of information leakage through that app, where they reported a wide-range of reasons in support of their decision.

In the following sections, we present participants' perceptions of data collection, factors influencing their perceptions, and the impact of those perceptions on their actions.

4.1 Sense of (No) Authority

Some of our participants do not feel to have any control over data collection and sharing by their apps. They also think, it is not possible to permanently delete their data once collected by an app. On top of that, they do not find an alternate to using these apps. For instance, P7 mentioned, *"The thing is that we are actually in a loop where we are bound to share our information."* He does not think that switching to a new app would yield any better outcome in preserving privacy.

4.1.1 'I am Not in Control!' Participants think that once installed, apps gain control of their phone's operating system, which enables them to collect any information they want from that device. We found evidences that participants' perceptions of control over digital data are often rooted to what they learn from their social circle. For example, P29 has heard from his friends that the apps from Google can collect his information no matter where he is, which has made him believe that users in today's world have no control over protecting their personal information.

Some participants perceive that top organizations, including Google, Facebook, and Microsoft control the overall data collection process through apps, where P28 commented, *"Giant companies like Microsoft or Google can collect every information."*; P15 added, *"Facebook has the access, from microphone to everything [in my smartphone]"*. A few participants placed Google at the center of data collection and sharing, where users' information are collected through apps including the ones available in Google App Store. They also mentioned about the existence of an internal network among organizations for sharing information that they collect through different apps. Here, they reflected onto their browsing experiences, where seeing advertisements related to recent online search made them believe that their information are shared between different apps.

A few participants mentioned about external influences that force the apps to share users' information. In general, they do not see a way to protect their personal data from such influence, especially when that comes from the government or political parties. P8 thinks that apps could use users' information for any purpose without taking their consent, which include sharing sensitive information with government and political entities. Due to such perceptions of no control over personal information, P5 did not see any benefit in taking a preventive step when she learnt about the privacy leakage news related to her app: *"Whatever information the application intended to take from me, is already taken. So, I have nothing more to lose in here."*

4.1.2 Permanent Deletion is Not Possible! Our participants think that there is no way for them to permanently delete their information from an app's database, where the collected information are retained forever. They mentioned about different reasons in support of their perceptions. Some of them believe that there is always a backdoor technology for the app-developers to retrieve users' information from their database after it is deleted by the users. According to P5, apps share users' information with other organizations. So, even if she deletes her information from an app's database, the app would re-collect that information from the organizations the information was shared with. So, she sees no benefit for users in deleting the information from an app's database.

Participants projected their experiences with technology and Web browsing onto their understanding of deletion provision. For instance, P3 mentioned, *"It's not possible to remove or delete permanently. If I delete something from memory card it can be recovered."* P16 found that his information were stored in Facebook's server even after he had deactivated his account, which has made him believe that an app can retain users' information even after it is uninstalled. P28 has reported a rather different reason of why users could not delete their information from app's database based on his experience of dealing with the physical world: *"Everything is stored unless or until it is destroyed physically. Like data remains in a hard disk until it is destroyed or burnt."* According to his perceptions, without getting a physical access to an app's information storage server, it is not possible to permanently delete users' information.

4.1.3 There is No Alternate! Users feel helpless when they do not find an alternate to using the app that might put their privacy at risk, where participants feel forced to grant access permission to the apps as otherwise they could not proceed with using them. P12 shared her sentiment: *"It [app] is a part of our everyday life and we cannot but use it. Although I understand, it is taking our personal information...still we have to use it."*

Due to a limited control users perceive to have over data collection and sharing by the apps, they feel pessimistic in protecting their privacy, as reflected in the comment of P28: *"Even if I set my privacy settings [of apps] very carefully I'm not sure if that would be able to protect my privacy."* As a result, users end up with taking no action even when they learn about a privacy leakage incident involving the apps they use.

4.2 Sense of Fear

Some of our participants are afraid that the information collection and sharing by apps would put them into the risks of financial loss, blackmailing, social harassment, and lead them to physical danger through tracking their geographic location.

4.2.1 Financial Loss. Some participants are worried about data collection and sharing by apps as their financial information might be leaked in the process, where a few of them reported concern not only about financial data but also their personal information. They are worried that if the apps sell their personal information to unverified entities, blackmailing might cause them to suffer financial loss. Some of them are also concerned about blackmailing by the app itself, where P7 is particularly worried about local apps (i.e., the apps developed by local entrepreneurs to address community-specific needs). As perceived by this participant, the local apps that are not popular in market, may try to earn money in an unethical way, like through blackmailing its customers.

4.2.2 Social Harassment and Physical Danger. Some of our female participants reported concern that the apps collecting their personal information could put them into the risks of social harassment and physical danger. P12 shared an incident of verbal abuse that occurred when the driver of a ride-sharing service (associated with the app) got her phone number when she availed the service, and later kept calling her despite her objection at the first place. P5 and P6 reported a chat application, which shared their contact information with others without taking their consent; P5 also mentioned, *"Due to that [sharing], people around me started to knock me and send me offensive texts and offers."* Participants are worried if the apps share their personal information with unwanted entities, the rate of such incidents would keep increasing.

P31 is concerned that the apps collect a large volume of private information from her smartphone including current geographic location. She is afraid that her safety might be compromised since organizations running the app have constant access to her whereabouts. A few participants have mentioned, they do not worry even if their information are retained by the app for an indefinite period of time, as long as that data are not used to track their physical location. These participants are concerned about their physical safety if their location information are leaked to the adversaries.

4.3 Sense of Indifference

We found instances where participants are indifferent about the apps collecting their personal information. A few participants see information collection by apps as a well-planned multi-step process, where the app collects minimal information from users at the initial stage to make them feel comfortable with using the app. Eventually, as users get used to using the app, it starts collecting more information from them. They think that due to such gradual but slow increase in data collection, it remains unnoticed at user's end contributing to their indifference to this issue. We also found, participants remain indifferent to data collection due to their trust on apps in protecting customer's information, their reliance on caregivers with privacy protection, and believing that general population are safe from the adverse consequences of data leakage.

4.3.1 Users (Except...) Do not Need to Worry. P15 uses his smartphone to keep backup of sensitive personal information, like he stores an image of his National ID Card in his phone. However, he is not worried about the apps collecting data from his smartphone as he considers his information are of little interest to adversaries; he further added, *"I am not an important person, selling my information will not cause that much damage [to me]. But selling those information of a big shot can put him in privacy and security risks big time."* In this context, a few participants think that only the political leaders involved in running the government should be concerned if their information are collected by the apps and shared with unverified entities.

4.3.2 Distant Harm. Participants who do not perceive any foreseeable danger from the information sharing by apps, did not take any step after learning about the privacy leakage through an app they use. They remained indifferent to such incident because they did not face any direct consequence of data leakage before and, thus, considered that as a 'distant' harm. For instance, P29 mentioned, *"Nothing happened to me, so I didn't take any step."*. A few participants believe that an app would ask for explicit permission, e.g., through email, before collecting any personal information from them. Since they did not receive any such email, they are convinced that they do not need to worry about the data leakage incidents related to their apps.

4.3.3 Protecting Business and Reputation. A few participants perceive that information collection through the app is a part of an organization's business policy, where the general population do not need to worry at all. They believe, an app would not exploit the collected information to cause any harm to its users, nor share their information with unverified entities. Because, if the information collection and sharing through an app get its users into trouble they would eventually stop using that app, which in turn, would hurt the organization's business and reputation.

4.3.4 Reliance on Caregiver. Our participants who are relatively older or less educated, reported that they take help from others (e.g., caregivers who are often their friends or family members) in installing an app, who also set the password for them if required. As they reported, they trust their caregivers with protecting their information. They believe that the caregivers would inform them if any privacy risks arise with using an app. Such social reliance contributed to our participants' indifference to information collection and sharing by apps.

4.4 Sense of Necessity and Contribution

Our participants think that the app collects more information than is needed to provide users with its core service, where some of them believe that such information collection is important for financial and security related reasons. They feel contributing to the expansion of app-based business, and law enforcement process by sharing their personal information through an app. P1 commented, *"Applications collect additional information because it is necessary. So, we don't give a second thought before providing our information."*

4.4.1 Improving Usability and Security Features. Usability is an important factor for the success of an app, as perceived by our participants who think that the information collected by an app are leveraged to understand the usability challenges faced by its users. P19 recognizes varying expertise level of users in understanding the features of an app, and thus, considers information collection to be necessary for making the app more accessible to the people with low technical efficacy. P14 believes, information collection helps the authority to identify an app's vulnerability against cyberattack, which in turn, motivates them to enhance its security features.

4.4.2 Business Expansion and Financial Revenue. To open a new wing of business, the organizations may need to identify their opportunities first through market analysis, which include understanding customers' interests and preferences. The information collected by an app could facilitate such market analysis, as perceived by our participants. For example, P4 mentioned, *"Pathao [ride-sharing app] is expanding their business to provide food service. So, they need to know about our interests to provide users with the required services."*; P3 further added, *"If they want to create new applications, they would want to be assured that [new app] is [developed] based on our preferences."*

In process of business expansion, it is important to inform customers about the new products and services [40, 107]. P10 thinks, an app collects users' contact-lists from their smartphone so that the organization could reach out to the users in that list and inform them about their new business endeavors. Also, an organization has to compete with other companies in business, where gaining access to customers' personal information reflecting their interests and preferences could put one in a leading position [99, 108]. P28 believes that information collection through an app is necessary for the survival of a business organization in today's competitive market, where he sees no harm as long as the customers are benefited from their services. Similarly, P32 perceives that information collection through an app is a legitimate way of progressing with business endeavor.

Many of the apps are available for free, to download and use. According to P19, since the organizations do not charge users for using their apps, collecting and selling the information of users is necessary to earn revenue and keep themselves in business. A few participants perceive that information collection might not be directly required for the functionality of an app, however, selling those information helps the organizations to manage their expenditure required for keeping their apps running. P18 sees two-way benefits when an app makes revenue by selling its users' information to a start-up company, which saves the new company from going through resource and time-consuming market analysis and provides them with access to the contact information of a large user-base for promoting their new products and services.

4.4.3 Digital and National Security. It is often challenging to identify the source of a cybercrime [23, 52], which might lead to an innocent person mistakenly accused of being an adversary. A few participants think that the information of users are collected to build an individual profile for each of them. They believe, if a fraudulent activity occurs over the Internet, information collected from innocent users would present the trail of their non-adversary activities and consequently, protect them from being wrongly accused of a cybercrime they did not commit. Also, such exclusion of innocent users would help the law enforcement agency to narrow down the list of potential adversaries.

A few participants believe that information collection through the app is necessary to ensure national security. They are concerned about the rise in crime, and perceive that information collection through apps would help to identify such activities and track down an app user if he is involved with a criminal group. P28 commented, *"In reality, if it [information collection through apps] is needed to control crimes inside a country then it [app] needs to collect the information."* He also mentioned, apps should share the collected information with the government and law enforcement agencies on time to control criminal activities inside a country.

4.5 Sense of Benefit

Some of our participants are in favor of data collection due to the benefits and services they get in return, including personal safety, convenience in transportation, low communication cost, and personalized offer. Because of these benefits, they are found to care less about the privacy compromise they might make in the process. According to P19, *"We are so addicted to using these applications that whatever they are taking from us, including our personal information, we don't really care that much."*

4.5.1 Personal Safety. Our participants think that the app that needs interaction between persons (often a stranger to each other) as a part of its core service, should collect personally identifiable information (e.g., driver's license number, national identification number, etc.) from the entities involved in that interaction. In this case, if any unexpected situation occurs during interaction, the collected information would be used for the purpose of law enforcement. P14 mentioned about an incident she had heard of, where the driver of a ride-sharing app was severely injured by his passenger; according to her, such incidents could be prevented if adequate information are collected from the users of a ride-sharing app to conduct background check before letting them avail the service.

GPS tracking by the ride-sharing app offers a sense of safety to some of our female participants. For instance, P5 mentioned, *"As this [ride-sharing app] keeps track of my route through satellite wherever I go, I feel that I am secure. As a girl, when I roam in the streets of Bangladesh, there arises a question of my security. In that context, ride-sharing app provides me with a clear notion of which street I am on."*

4.5.2 Convenience. Despite learning about the information leakage by a ride-sharing app, participants continued using that app to avail the convenience it provides in a city with heavy traffic and insufficient public transportation, where P4 mentioned, *"For transportation in Dhaka city, it [ride-sharing] is cheap, efficient, and accessible, most importantly time-savvy."*

Most of the mobile phone operators in Bangladesh offer prepaid communication service [82], where the cost of regular phone call is comparatively higher than communicating through an app, as mentioned by our participants. Also, a few participants do not consider the cost of accessing Internet as app-based communication cost, where P27 commented, *"I can socialize with people free of cost [through social networking and communication apps]."*

4.5.3 Personalized Offer. Participants see benefits in data collection as that would help an app to provide its customers with personalized offer. P8 perceives that an app collects its users' financial information, e.g., salary data, to identify a promotional offer that would best fit the economic condition of a customer. He mentioned, *"Pathao [ride-sharing app] has access to my SMS. So, they can easily analyze my banking SMS and have a clear idea about my salary, and based on that they can identify if they should send me any promo [promotional] codes or not."*

According to P4, information collected through location tracking are used to identify the preferences and interests of a user to send him personalized offer: *"Suppose I have visited a fashion-house today and by location tracking, they [apps] can figure out which kind of style I prefer, and based on that, they could start promoting products to me through SMS."*

4.6 Users' Actions

In this section, we report our findings on the steps taken by our participants after learning about the privacy leakage incident involving their apps.

4.6.1 Social Sharing. Most of our participants who perceive no control over their data or have a sense of fear about information collection by apps, started a social discussion after learning about information leakage through their apps. They shared the news with their friends and family members to discuss and understand the risks, or to alert them about possible consequences as per their understanding. For instance, P30 became worried about the privacy of her family members, especially her daughter who used to use the app reported in privacy leakage news. So, she suggested her daughter to stop using that app.

We found different outcomes of social sharing, where a few participants reported uninstalling the app according to the suggestions of their well-wisher. Also, some participants decided to have a closer look into the app's privacy policy. We also found instances where social sharing did not lead to a privacy-preserving behavior. For example, a few participants have learnt from social discussion that there are many people around them who do not understand app's privacy policy, and have not faced any unexpected incident as a result of information leakage through their apps. Consequently, those participants do not feel the necessity of taking any step to protect their privacy.

4.6.2 Uninstalling the App. Among those participants who reported fear about data collection, some of them uninstalled the app reported in privacy leakage news. Among them, P13 emailed the customer service of that app to verify the news of privacy leakage, but did not get any response from them. So, she uninstalled the app as it appeared to be the safest option to her. P22 took similar action, he mentioned, *"I uninstalled it. I would not use it with changing privacy settings. Since I disliked it, nothing could convince me to keep using it."*

A few participants uninstalled the app, followed by a re-installation, which they see as a 'fresh and safe start' with using the app after a privacy leakage incident is reported.

4.6.3 Attempt to Understand Privacy Policy. The news of information leakage made some of our participants aware of privacy issues related to information collection and sharing. They tried to read the privacy policy of app reported in news, however, failed to understand its contents. They mentioned about language barrier why they could not understand the privacy policy.

While Bengali is the native language in Bangladesh, English is taught as a second language in educational institutions [27]. Like many people in Bangladesh [71], some of our participants were not privileged in getting access to education required to understand a foreign language like English. One of our participants commented, *"It [privacy policy] is written in English. For people like us, it is difficult to understand."* Our participants expressed surprise to the fact that the local apps developed in Bangladesh for the people in this country, publish their privacy policy in a foreign language.

Access to Privacy Policy. We found that availing intermediate help limits our participants' access to the privacy policy. Some of those participants who take help from others with app installation are unsure of where to find the privacy policy, and are not aware that the privacy policy is presented at the time of app installation. In this context, our relatively younger participants who often play the role of a caregiver, have reported that they are used to clicking on 'I Agree' button without notifying the person, whom they help with app installation. Further, a few of our participants do not own a personal smartphone and use the apps from other's (e.g., family member) device. In such cases, they were not involved with the app installation process, and reported unawareness about the existence of an app's privacy policy.

5 DISCUSSION

In this section, we discuss about the implications of our findings, and surface recommendations to enhance privacy practices in the social setting of Bangladesh, and Global South.

5.1 Interplay between Urbanization, Digitization, and Privacy

Urbanization, or the growth of urban areas, has seen a rapid increase in the last few decades in the Global South. This has important implications for sustainable development as city infrastructures struggle to keep up with this growth [29]. Rapid urbanization in Bangladesh has led to inadequacy of infrastructural services and challenges related to growing unemployment, traffic congestion, violence and socioeconomic insecurity [60, 78, 80, 98]. It is often difficult for urban authorities to address these issues due to lack of resources, manpower, and planning [78, 80, 96]. As a result, it creates burden on general population to handle urban challenges on their own. The new digital economy is playing an important role here with digital technologies, such as on-demand service apps, slowly becoming crucial to individuals navigating city life in the midst of rapid urbanization. Our paper shows how these apps, and by extension collected user data, relate to how individuals are dealing with urban city life by availing convenience in transportation, getting personalized offer, and believing to contribute to public safety, and economic growth of the country.

In this section, we discuss how the privacy perceptions of people relate to their effort to deal with the issues of urbanization and the opportunities that come with digitization.

5.1.1 Privacy Cost in Digital Economy. Youth unemployment is a major problem in Bangladesh [26, 96], where one in every 10 of 44 million young people is unemployed [75, 111]. Our participants see information sharing as a way to support local business, which in turn, would create job opportunities and contribute to the economic growth of their country. The startup business, especially those based on smartphone apps are getting increasingly popular in Bangladesh [31, 72, 83] and actively encouraged by the government with a motto of thriving in digital sector [9, 49].

The general population in Bangladesh have also started to get the benefits of using these apps in everyday life, like online banking, ride sharing, social communication, ordering food, and purchasing tickets for bus and train [61, 92]. In these contexts, our participants do not want the apps to discontinue, rather, they expect more apps to be launched with new services and features. Many participants believe that the information collected from them contribute to the success of app-based businesses including start-ups, where apps could earn revenue by selling customers' information, expand their business through learning about customers' interests and preferences, and reach out to a larger user-base by collecting the contact-list from customers' smartphone. These perceptions present an interesting contrast to Posner's argument on privacy [74]. While he considers individual privacy to be less of a concern since it is not related to the economic advancement [74], our participants perceive leveraging users' personal information to be necessary and contributing to the advancement of digital economy.

5.1.2 Convenience Gain vs. Privacy Compromise. In the present decade, traffic congestion is recognized as one of the most challenging and complicated issues in city management [63, 98] in Bangladesh. The problem is further alleviated due to inadequate public transport, and lack of planning, infrastructure, and manpower in traffic management [80, 98]. Traffic problem contributes to increasing transportation cost; further, a substantial portion of time is spent navigating urban streets [63]. Under these circumstances, ride-sharing apps are increasingly getting popular through offering convenience in dealing with heavy traffic and inadequate public transport. For many, ride-sharing is not just about convenience, rather it has become a necessity for daily commute. Thus, despite learning about privacy leakage, participants do not see an alternate to continue using the app.

In response to the challenges accompanying urbanization in Bangladesh [2, 63], people have had to be more prudent with balancing their time and effort across work, commute, and personal life. In these contexts, digital merchandise and online shopping have experienced a boom in recent years [35, 47, 94], providing access to large number of products. Targeted advertisements or personalized offers are customizing the shopping experience of people as per their needs and interest [18, 19], along with saving time and being convenient [35, 47, 94]. Interviewed participants seem to appreciate such conveniences and accessibility to shopping even if it came at the privacy cost of sharing financial information (e.g., salary data) or allowing location tracking.

5.1.3 Individual Privacy vs. Public Safety. While Blousetin [20] describes privacy as aspects of personal autonomy and independence, our participants perceive that individual privacy needs to be sacrificed for the greater good, like public safety. This is supported by research that describe Bangladesh as a collectivist society [44, 79], where the interests of the community or society take precedence over individual interest. Collectivism in Bangladeshi society manifests itself as strong intra-community bonds, where individuals take responsibility for other members of their group and think about the collective 'we' rather than the individual self. In our study, we consequently find that participants placed higher importance on public safety than their individual privacy.

Rapid urbanization has often posed challenges for law enforcement authorities having to deal with an increase in crime and violence. The lack of resources and manpower makes the situation even worse, adding to the concern of general population [78, 80, 91]. The participants believe that data collection by apps would equip

the government with resources to maintain peace and order within the society. They see the collection of digital information as a potential way to support law enforcement, alleviate injustice, and catch criminals by tracking their activities through apps. The larger expectation is that collected information would be shared by apps with the government and law enforcement agencies on time, so as to prevent the crime from being committed.

5.2 Privacy Dependency, Concerns, and Control

Our participants never developed privacy perceptions from the privacy notice of an app, rather it was from different sources, including browsing experiences on the Web, social discussion and sharing, and personal experiences in the physical world. However these sources are often inadequate, leading to many possessing misconceptions of their control over privacy, and a lack of awareness of how to protect their digital information. The problem is further exacerbated due to their dependency with technology use.

Our relatively younger participants often played the role of a caregiver to help their older family members with app installation and use. The older participants consequently trust their caregivers to inform them about privacy vulnerabilities (if any exist). However, the expectations from a caregiver might not always match with reality. We found that our participants, including the caregivers, discuss about privacy issues only when they perceive no control over their data or have a sense of fear about information collection by apps. The perceptions of caregivers thus shape how some individuals think about privacy issues.

Privacy preservation is important to protect and control social relationships [76], where blackmailing and harassment could harm people's dignity, reputation, and social relations [90, 109]. Participants reported concern about such incidents as a possible consequence of data collection by apps. They are also worried about physical danger as a result of information collection. Here, participants feel little, or no control at all over their information as collected and shared by the apps. An app could gain control over any type of personal information as perceived by the participants. They see the data collection by apps as a well-structured process, controlled by the top organizations, with a networked communication system including local apps where data collected by an app are shared with other apps and organizations. Also, participants do not realize their control over deletion provision, rather consider the deletion of collected information being possible only at the administrator's end. Such perceptions resulted in their consensus that they have nothing to do with their digital privacy protection, which made several participants indifferent to the information leakage incidents related to their apps.

5.3 Towards Informed Privacy Decision

The majority of our participants were not worried about information leakage through apps, however, even when participants were concerned, they were unsure of how to protect their digital privacy. This indicates the need for an effective and organized approach to raise the privacy awareness to help individuals realize their control over personal information. This would help them make informed decisions on sharing their data along with learning to adjust privacy settings for protecting their information. Below, we provide recommendations to achieve the goals in the context of Bangladesh, and Global South.

5.3.1 Social Discussion and Story-telling Sessions. Social discussion plays an important role on the privacy perceptions of people in Bangladesh. People ask for suggestions and help from their social circle when they hear of privacy leakage news, and share their privacy concerns and recommendations with friends and family members. To leverage the power of social sharing in raising privacy awareness, workshop and discussion session could be arranged in schools and colleges, public libraries, and local club in the neighborhoods.

The younger participants help the users who are relatively older or less educated with the installation and use of apps. So, educating our caregivers through the workshop in schools and colleges would channel the privacy awareness to the people from varying age and literacy level. Also, the security and privacy workshops in educational setting will help to create a local workforce involving teachers and students who would then disseminate the knowledge to the people in their family, social circles, and neighborhoods.

The discussion and storytelling sessions in public libraries and local neighborhood clubs will let the experts reach out to broader population, and inform them about information leakage incidents and techniques to enhance their digital privacy. These sessions will let people share their security and privacy stories, followed by open discussion and suggestions from the experts on how they could react to those instances in a more secure and privacy-preserving way. In this way, the social discussion will create a communication bridge between experts and general population, and help the educators and researchers to alleviate people's privacy misconceptions.

5.3.2 Leveraging News Media. Although the circulation of printed newspaper has experienced a decline in USA and Europe in recent years [41, 53], the picture in the Global South is not as bleak as in the west [15, 36, 84]. Newspapers played a historic role in the politics, culture, and democracy of Bangladesh, where the traditional print media remains influential and plays a crucial role in building public opinion [8, 36]. Despite the widespread use of Internet and online social media, many in both urban and rural areas in Bangladesh still depend on newspapers for stories and information [8, 84]. Our participants reported newspaper as one of the notable sources of learning about privacy leakage news.

We found instances where the news of information leakage through apps contributed to enhance participants' privacy awareness. However, they are unsure of how to address the privacy issues in the reported apps. The news media could help in these instances through publishing privacy solutions from the experts. Our participants reported their needs of having privacy notice in Bengali. Most of the newspapers in Bangladesh are published in Bengali [36, 110], which could contribute to raising awareness through publishing the summary and implications of privacy policy of the popular and widely-used apps in Bangladesh. While many newspapers in Bangladesh now have digital version and online presence in social media [36, 97], it provides an opportunity to reach out to diverse groups of population and help with enhancing their privacy awareness and practices.

5.3.3 Customer Service Infrastructure. We found that many of the users - irrespective of age or tech literacy - are unsure of how to handle privacy issues or react to news reporting information leakage through the app they use. One of our participants ended up uninstalling the app as she did not hear back from the customer service after contacting them to verify the privacy leakage news. In such instances, clarification and support from customer service could play a vital role in a user's decision to continue using the app while taking appropriate steps for privacy protection.

Participants reported their concerns about blackmailing and harassment, and risks of location tracking by unwanted entities. The app's role and steps required by a user could be disseminated through the customer support center. In this regard, the employees in customer service should be trained not only to fix the technical problems in apps, but also to help users with the privacy issues.

5.3.4 Accessibility of Privacy Notice. A secondary channel for delivery, and multi-user environment due to the sharing of smartphone should be taken into account to increase the accessibility of privacy notice.

Secondary Channel for Delivery. While privacy policy of an app is generally shown during installation, we identified a lack of awareness of participants about where to find the privacy policy. A secondary channel for privacy notice delivery, e.g., through email, should be considered by the apps, so that people who take help from others with app installation, would get an opportunity to go through the privacy notice by themselves instead of depending upon caregivers. Also, it would enable users to access the privacy policy from their email-inbox whenever they want, like in cases where they would like to verify the information collection and sharing policy of an app after learning about a privacy leakage incident.

Multi-User Environment. In the social setting of Bangladesh, people are expected to share their smartphone with family members [4, 6]. Our participants reported using apps from other's (e.g., family member) device without being notified of privacy policy. Here, multi-user access privilege should be provided at the app level, so that users (like, members in a family) could access an app from the same device, but through different accounts. In this regard, one of our researchers looked into (i.e., accessed as a user) some of the most popular local apps in Bangladesh [61, 92] and found that a majority of them do not offer multi-user access from the same phone. While a few of these apps [61, 92] provide multi-user access feature, they present privacy notice only at the time of installation. We suggest, when a new user would create an account in an already-installed app, she should be presented with the privacy notice first, before using the app.

6 LIMITATIONS AND CONCLUSION

In our qualitative study, we interviewed 32 participants. Our sample size is relatively small, where we followed the widely-used methods for qualitative research [16, 21, 22], 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. In addition, self-reported data might have limitations, like recall and observer bias.

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 [46, 65, 88], and the literacy rate is generally higher in urban areas as compared to that in rural areas [71], we speculate that the privacy perceptions and behavior of users reported in this paper represent an upper bound in the context of Bangladesh.

Despite these limitations, we unveil the participants' perceptions of data collection and sharing by the app reported in privacy leakage news. Our analysis sheds light on the relation between users' privacy perceptions, local infrastructure, and social practices in Bangladesh, where we unpack the situated issues that influence people's privacy behavior. Based on our findings, we provide recommendations on how we could develop situated and sustainable strategies for local people in Bangladesh to make informed privacy decision. We encourage HCI, Privacy, and ICTD research communities to extend the findings of this work in the contexts of different domains and field sites, and use other methods as well, if required.

7 ACKNOWLEDGEMENT

We thank our participants in this study. We are thankful to the anonymous reviewers for their thoughtful suggestions in improving the paper. This research was made possible by the startup fund provided to Mahdi Nasrullah Al-Ameen by Utah State University, and the generous grants from Natural Sciences and Engineering Research Council (#RGPIN-2018-0), Social Sciences and Humanities Research Council (#892191082), Canada Foundation for Innovation (#37608), Ontario Ministry of Research and Innovation (#37608), National Institute of Health (#1R21MH116726-01), and International Fulbright Centennial Fellowship of Syed Ishtiaque Ahmed.

REFERENCES

[1] 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

[2] AI Ahmed and Mahbub Uddin. 2004. Weber's perspective on the city and culture, contemporary urbanization and Bangladesh. *Bangladesh e-journal of Sociology* 1, 1 (2004), 1–13.

[3] Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (Ann Arbor, MI, USA) *(ICTD '16)*. ACM, New York, NY, USA, Article 11, 10 pages. https://doi.org/10.1145/2909609.2909661

[4] 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 (Dec. 2017), 20 pages. https://doi.org/10.1145/3134652

[5] 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* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 906–918. https://doi.org/10.1145/3025453.3025961

[6] Syed Ishtiaque Ahmed, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. "Everyone Has Some Personal Stuff": Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, Article 180, 13 pages. https://doi.org/10.1145/3290605.3300410

[7] Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md Rashidujjaman Rifat, ASM Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A platform for fighting sexual harassment in urban Bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2695–2704.

[8] Mortuza Ahmmed. 2014. Impact of Mass Media in Creating Political Concern in Bangladesh. *Online Journal of Communication and Media Technologies* 4, 2 (2014), 1.

[9] Nayeema Akbar. 2017. 37 Startups Receive Funding From Startup Bangladesh-iDEA Of ICT Division. https://sdasia.co/2017/12/11/43950/.

[10] Mahdi Nasrullah Al-Ameen, Kanis Fatema, Matthew Wright, and Shannon Scielzo. 2015. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 185–196.

[11] Mahdi Nasrullah Al-Ameen, Matthew Wright, and Shannon Scielzo. 2015. Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2315–2324.

[12] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security practices for households bank customers in the Kingdom of Saudi Arabia. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 297–308.

[13] Hala Assal and Sonia Chiasson. 2018. Security in the software development lifecycle. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 281–296.

[14] Anonymous Author. 2017. *Bangladesh Population 2019.* Retrieved March 31, 2019 from http://worldpopulationreview.com/countries/bangladesh-population/

[15] M. Abul Kalam Azad. [n.d.]. Bangladesh: Media Landscapes. https://medialandscapes.org/country/bangladesh/media/print.

[16] Kathy Baxter, Catherine Courage, and Kelly Caine. 2015. *Understanding your users: A practical guide to user research methods.* Morgan Kaufmann.

[17] M Bhuiyan. 2010. E-government applications in Bangladesh: status and challenges. In *Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance*. ACM, 255–260.

[18] Alexander Bleier and Maik Eisenbeiss. 2015. The importance of trust for personalized online advertising. *Journal of Retailing* 91, 3 (2015), 390–409.

[19] Alexander Bleier and Maik Eisenbeiss. 2015. Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science* 34, 5 (2015), 669–688.

[20] Edward J. Bloustein. 1964. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review* 39 (1964), 962.

[21] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development.* sage.

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

[23] Cameron SD Brown. 2015. Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9, 1 (2015), 55.

[24] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana.. In *Symposium on Usable Privacy and Security*. 129–142.

[25] Abhishek Choudhary. 2019. Smartphone Market in Bangladesh Grew 45% YoY in Q1 2019. https://www.counterpointresearch.com/smartphone-market-bangladesh-grew-45-yoy-q1-2019/.

[26] Mohammad Chowdhury, Md Hossain, et al. 2014. Determinants of unemployment in Bangladesh: A case study. *Developing Country Studies* 4, 3 (2014).

[27] Raqib Chowdhury and Ariful Haq Kabir. 2014. Language wars: English education policy and practice in Bangladesh. *Multilingual Education* 4, 1 (2014), 21.

[28] Camille Cobb, Samuel Sudar, Nicholas Reiter, Richard Anderson, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer security for data collection technologies. *Development engineering* 3 (2018), 1–11.

[29] Barney Cohen. 2006. Urbanization in developing countries: Current trends, future projections, and key challenges for sustainability. *Technology in society* 28, 1-2 (2006), 63–80.

[30] Bangladesh Telecommunication Regulatory Commission. 2019. *Internet Subscribers in Bangladesh.* Retrieved March 31, 2019 from http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-february-2019

[31] Digiology Content. 2018. 7 Startups which are shaping Dhaka's digital ecosystem! http://digiology.xyz/top-startups-in-bangladesh/.

[32] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. *Comput. Supported Coop. Work* 26, 4-6 (Dec. 2017), 453–488. https://doi.org/10.1007/s10606-017-9276-y

[33] Nicola Davinson and Elizabeth Sillence. 2014. Using the health belief model to explore users' perceptions of 'being safe and secure'in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies* 72, 2 (2014), 154–168.

[34] Leslie L Dodson, S Sterling, and John K Bennett. 2013. 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*. ACM, 79–88.

[35] Jonathan Doerr. 2017. Revolutionising the Digital Marketplace. https://www.dhakatribune.com/opinion/op-ed/2017/09/12/214778.

[36] Hamida El Bour, Elsebeth Frey, and M Rahman. 2017. Media landscape in Bangladesh, Norway and Tunisia. *Negotiating Journalism: Core Values and Cultural Diversities, Göteborg: Nordicom* (2017), 23–37.

[37] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 59–75.

[38] Dinei Florêncio and Cormac Herley. 2010. Where do security policies come from?. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 10.

[39] Yuri V. Gankovsky. 1974. The Social Structure of Society in the People's Republic of Bangladesh. *Asian Survey* 14, 3 (1974), 220–230. http://www.jstor.org/stable/2643011

[40] Kamala Gollakota, Vipin Gupta, and James T Bork. 2010. Reaching customers at the base of the pyramid—a two-stage business strategy. *Thunderbird International Business Review* 52, 5 (2010), 355–367.

[41] Elizabeth Grieco. 2020. Fast facts about the newspaper industry's financial struggles as McClatchy files for bankruptcy. https://www.pewresearch.org/fact-tank/2020/02/14/fast-facts-about-the-newspaper-industrys-financial-struggles/.

[42] SM Taiabul Haque, Pratyasha Saha, Muhammad Sajidur Rahman, and Syed Ishtiaque Ahmed. 2019. Of Ulti,'hajano', and" Matachetar otanetak datam" Exploring Local Practices of Exchanging Confidential and Sensitive Information in Urban Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–22.

[43] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2647–2656.

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

[45] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 209–223.

[46] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[47] Ahmed Ishtiaque, Abdul Baten, and Adib Sarwar. 2017. How E-commerce is Transforming in Bangladesh. *Australasian Journal of Business, Social Science and Information Technology* 3, 4 (October 2017), 166.

[48] Jannatul Islam. 2018. Pathao Violates Users' Privacy. https://www.daily-sun.com/arcprint/details/348905/Pathao-violates-users%E2%80%99-privacy/2018-11-09.

[49] Muhammad Zahidul Islam. 2019. Govt to set up firm to fund startups. https://www.thedailystar.net/business/news/govt-set-firm-fund-startups-1774672.

[50] Shariful Islam. 2018. *Digital Bangladesh a reality now.* Retrieved March 31, 2019 from https://www.dhakatribune.com/bangladesh/2018/07/11/digital-bangladesh-a-reality-now

[51] Elida KU Jacobsen. 2012. Unique Identification: Inclusion and surveillance in the Indian biometric assemblage. *Security dialogue* 43, 5 (2012), 457–474.

[52] Yunsik Jake Jang et al. 2013. Harmonization among national cyber security and cybercrime response organizations: new challenges of cybercrime. *arXiv preprint arXiv:1308.2362* (2013).

[53] J. Johnson. 2019. Newspaper market in Europe - Statistics & Facts. https://www.statista.com/topics/3965/newspaper-market-in-europe/.

[54] Ruhul Kader. 2019. The Mobile And Internet Penetration Growth Continues, Internet's Deployment Phase. https://futurestartup.com/2019/01/31/mobile-and-internet-penetration-updates-internets-deployment-phase/.

[55] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 39–52. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

[56] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 39–52.

[57] Md Abdul Karim. 2010. Digital Bangladesh for good governance. In *Bangladesh Development Forum*. 15–16.

[58] Allan J Kimmel. 1988. *Ethics and Values in Applied Social Research.* SAGE Publications, Inc, Thousand Oaks, CA. https://doi.org/10.4135/9781412984096

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

[60] Serajul Islam Laskar. 1996. Urbanization in Bangladesh: some contemporary observations. *The Bangladesh Development Studies* 24, 1/2 (1996), 207–216.

[61] Nurun Nahar Liya. 2018. The Most Popular 5 Android Apps of Bangladesh. https://dhrubokinfotech.com/popular-android-apps-of-bangladesh/.

[62] Faisal Mahmud. 2018. Dhaka Ride-Sharing App Accused of 'Stealing Users' Phone Data'. https://www.asiatimes.com/2018/11/article/dhaka-ride-sharing-app-accused-of-storing-users-phone-data/.

[63] Khaled Mahmud, Khonika Gope, and Syed Mustafizur Rahman Chowdhury. 2012. Possible causes & solutions of traffic jam and their impact on the economy of Dhaka City. *J. Mgmt. & Sustainability* 2 (2012), 112.

[64] Mahdi Mashrur Matin. 2018. How Ride-hailing app Pathao is dangerously close to malware. https://medium.com/@mashrur123/how-ride-hailing-app-pathao-is-dangerously-close-to-malware-1459dbc1d93e.

[65] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 173–186.

[66] Susan E McGregor, Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Kelly Caine, and Franziska Roesner. 2017. When the weakest link is strong: Secure collaboration in the case of the Panama Papers. In *26th USENIX Security Symposium (USENIX Security 17)*. 505–522.

[67] Papreen Nahar, Miranda Van Reeuwijk, and Ria Reis. 2013. Contextualising sexual harassment of adolescent girls in Bangladesh. *Reproductive health matters* 21, 41 (2013), 78–86.

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

[69] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA.

[70] Fayika Farhat Nova, MD. Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed, and Shion Guha. 2019. Online Sexual Harassment over Anonymous Social Media in Bangladesh. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development* (Ahmedabad, India) *(ICTD '19)*. ACM, New York, NY, USA, Article 1, 12 pages. https://doi.org/10.1145/3287098.3287107

[71] Bangladesh Bureau of Statistics. 2008. *Literacy Assessment Survey 2008*. http://www.un-bd.org/Docs/Publication/Bangladesh_Literacy_Assessment_Survey_2008.Pdf.

[72] Martin Pasquier. 2015. Top 11 startups to watch from Bangladesh. https://www.techinasia.com/talk/top-11-startups-to-watch-from-bangladesh.

[73] Andrew Patrick and Steve Kenny. 2003. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-computer Interactions. In *Privacy Enhancing Technologies*. Springer, 107–124.

[74] Richard A. Posner. 1981. The Economics of Privacy. *The American Economic Review* 71, 2 (1981), 405–409. http://www.jstor.org/stable/1815754

[75] Johura Akter Pritu. 2018. 4.4 million youths face unemployment in Bangladesh. https://www.dhakatribune.com/bangladesh/2018/09/25/4-4-million-youths-face-unemployment-in-bangladesh.

[76] James Rachels. 1975. Why Privacy Is Important, 4 Phil. & Pub. *Aff* 323 (1975), 326.

[77] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 6.

[78] Md Motiar Rahman. 2012. Urbanization and Urban crime in Bangladesh.

[79] Taiabur Rahman. 2006. Problems of democratic consolidation in Bangladesh: A cultural explanation. *Network of Asia-Pacific Schools and Institutes of Public Administration and Governance (NAPSIPAG)* 569 (2006).

[80] Md Masud Parves Rana. 2011. Urbanization and sustainability: challenges and strategies for sustainable urban development in Bangladesh. *Environment, Development and Sustainability* 13, 1 (2011), 237–256.

[81] Sabina Faiz Rashid, Hilary Standing, Mahrukh Mohiuddin, and Farah Mahjabeen Ahmed. 2011. Creating a public space and dialogue on sexuality and rights: a case study from Bangladesh. *Health Research Policy and Systems* 9, 1 (2011), S12.

[82] Mike Rogers. 2014. Country Overview: Bangladesh: Mobile Industry Driving Growth and Enabling Digital Inclusion. https://www.gsmaintelligence.com/research/?file=a163eddca009553979bcdfb8fd5f2ef0&download.

[83] Jon Russel. 2019. A Young Entrepreneur is Building the Amazon of Bangladesh. https://techcrunch.com/2019/05/21/deligram/.

[84] Maria Salam. 2011. Role of Mass Media in Enhancing Education in Bangladesh. http://www.digital-development-debates.org/issue-04-media--education--role-of-mass-media-in-enhancing-education-in-bangladesh.html.

[85] 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.

[86] Nithya Sambasivan, Nimmi Rangaswamy, Ed Cutrell, and Bonnie Nardi. 2009. Ubicomp4D: infrastructure and interaction for international development–the case of urban indian slums. In *Proceedings of the 11th international conference on Ubiquitous computing*. ACM, 155–164.

[87] Nithya Sambasivan, Julie Weber, and Edward Cutrell. 2011. Designing a phone broadcasting system for urban sex workers in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 267–276.

[88] Sovantharith Seng, Mahdi Nasrullah Al-Ameen, and Matthew Wright. 2018. Understanding users' decision of clicking on posts in Facebook with implications for phishing. In *Workshop on Technology and Consumer Protection (ConPro 18)*.

[89] Abul K Shamsuddin. 2018. *The real scenario of internet access*. Retrieved March 31, 2019 from https://www.thedailystar.net/opinion/perspective/the-real-scenario-internet-access-1611499

[90] Henry E Smith. 1997. Harm in Blackmail. *Nw. UL Rev.* 92 (1997), 861.

[91] Paris Sociales. 2001. Crime as a social cost of poverty and inequality: a review focusing on developing countries. *Facets of Globalization* (2001), 171.

[92] Saad Solaiman. 2017. 10 must-have apps in Bangladesh! https://travel.jumia.com/blog/bd/10-must-apps-bangladesh-455.

[93] 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.

[94] Jubayer Suhan. 2015. Acceptance of Online Shopping in Bangladesh: Consumer's Perspective. *Journal of Business and Management* 17, 1 (2015), 14.

[95] Sharifa Sultana and Syed Ishtiaque Ahmed. 2019. Witchcraft and HCI: Morality, Modernity, and Postcolonial Computing in Rural Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–15.

[96] Rayhan Ahmed Topader. 2018. Unemployment a big problem for Bangladesh.

[97] Saifur Rahman Tuheen. 2016. Online Newspapers: The Bangladesh Perspective. http://www.theindependentbd.com/arcprint/details/35640/2016-03-01.

[98] Mohammed Forhad Uddin and Kazushi SANO. 2011. Transportation problem urban city of the developing country Bangladesh. In *Proceedings of the Eastern Asia Society for Transportation Studies Vol. 8 (The 9th International Conference of Eastern Asia Society for Transportation Studies, 2011)*. Eastern Asia Society for Transportation Studies, 177–177.

[99] Wolfgang Ulaga, Arun Sharma, and R Krishnan. 2002. Plant location and place marketing: understanding the process from the business customer's perspective. *Industrial marketing management* 31, 5 (2002), 393–401.

[100] Kami E Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2671–2674.

[101] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 25.

[102] Samuel D. Warren and Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4, 5 (1890), 193–220. http://www.jstor.org/stable/1321160

[103] Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Franziska Roesner, Kelly Caine, and Susan McGregor. 2017. 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 17)*.

[104] Elizabeth Anne Watkins, Franziska Roesner, Susan McGregor, Byron Lowens, Kelly Caine, and Mahdi Nasrullah Al-Ameen. 2016. Sensemaking and Storytelling: Network Security Strategies for Collaborative Groups. In *2016 International Conference on Collaboration Technologies and Systems (CTS)*. IEEE, 622–623.

[105] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L Mazurek, and Blase Ur. 2019. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 149–166.

[106] Alan F Westin. 1968. Privacy and Freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[107] Hugh Wilson, Elizabeth Daniel, and Malcolm McDonald. 2002. Factors for success in customer relationship management (CRM) systems. *Journal of marketing management* 18, 1-2 (2002), 193–219.

[108] Ji Young Woo, Sung Min Bae, and Sang Chan Park. 2005. Visualization method for customer targeting using customer map. *Expert Systems with Applications* 28, 4 (2005), 763–772.

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

[110] Ananta Yusuf. 2015. Story of the Bangla Press. https://www.thedailystar.net/the-star/cover-story/story-the-bangla-press-3161.

[111] Azaz Zaman. 2019. How the digital economy is shaping a new Bangladesh. https://www.weforum.org/agenda/2019/06/how-the-digital-economy-is-shaping-a-new-bangladesh/.

[112] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. " 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)*. 197–216.