Privacy Vulnerabilities in Public Digital Service Centers in Dhaka, Bangladesh

S M Taiabul Haque
University of Central Missouri
Warrensburg, USA
haque@ucmo.edu

MD Romael Haque
Marquette University
Milwaukee, USA
mdromael.haque@marquette.edu

Swapnil Nandy
Jadavpur University
Kolkata, India
swapnilnandy2@gmail.com

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

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

Shion Guha
Marquette University
Milwaukee, USA
shion.guha@marquette.edu

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

ABSTRACT

This paper joins a growing body of work within ICTD and related fields studying the privacy challenges in the Global South. While most of the existing work in this area has focused on uses of technology in personal and home settings, a large part of computing in the Global South centers around public places, such as commercial Digital Service Centers (DSCs). In this paper, we present the findings from a six-month-long ethnography studying 19 Digital Service Centers in Dhaka, Bangladesh. We find that infrastructural limitations, local power politics, lack of knowledge, and insufficient protection mechanisms lead to privacy vulnerabilities for the customers of these centers. We apply the lens of informal markets to analyze these vulnerabilities and connect our findings to the broader concerns of ICTD around development, ethics, and postcolonial computing and discuss potential design and policy implications around these issues.

CCS CONCEPTS

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

KEYWORDS

Privacy; The Global South; Ethnography

ACM Reference Format:
S M Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. 2020. Privacy Vulnerabilities in Public Digital Service Centers in Dhaka, Bangladesh. In *Information and Communication Technologies and Development (ICTD '20), June 17–20, 2020, Guayaquil, Ecuador*. ACM, New York, NY, USA, 12 pages. **https://doi.org/10.1145/3392561.3394642**

ICTD '20, June 17–20, 2020, Guayaquil, Ecuador

ACM ISBN 978-1-4503-8762-0/20/06…$15.00
https://doi.org/10.1145/3392561.3394642

1 INTRODUCTION

Like many other countries in the Global South, in recent years, Bangladesh has become a rapidly growing technological nation where almost 100 million people (55% of the total population [15]) now have Internet access [27]. The present government has formulated policies and action plans for transforming the country into "Digital Bangladesh" by improving the nation's digital infrastructure, migrating paper-based activities to online portals, and making Internet accessible to a larger population [46, 72]. However, a recent body of work in ICTD and related fields has demonstrated that despite all these efforts, the majority of the population in Bangladesh still have inadequate knowledge about digital technologies, and depend on others for basic tasks with computing devices [4, 5, 19, 34]. This asymmetry, coupled with a favorable small and medium enterprise (SME) environment in Bangladesh [9], have opened up a business opportunity for Digital Service Centers (DSCs), small commercial shops where a shopkeeper helps customers with various tasks on mobile phones and computers, including facilitating mobile transactions, printing and photocopying, filling up online application forms, and photo editing. Thousands of people, including those with low literacy levels, visit these places everyday to get their intended digital service [73].

Due to the nature of those digital services, these DSCs deal with a large amount of personal information and sensitive documents of the customers. However, there are no adequate policies and laws in Bangladesh to protect the privacy of the customers in these DSCs [44]. Furthermore, due to the lack of resources and training, law enforcement agencies are not well equipped to address the digital threats emerging in these places. As a result, DSCs in Bangladesh are vulnerable to various privacy breaches and potential risks that lead to harassment, blackmailing, and identity theft, some of which have been extensively reported by the local media [45, 54]. These

issues are not limited to Bangladesh because DSC customers in India and Pakistan also encounter similar privacy threats as the governments of these neighboring countries have been establishing numerous one-stop centers for providing digital services to their citizens [42, 51, 74]. Prior work on privacy in the Global South has mainly examined issues related to individual use or shared use among friends or family members [4, 6, 7, 53, 60, 68]. As a result, this important issue of privacy vulnerabilities in public shops has remained understudied in the literature.

Our work intends to fill this gap in the literature with a six-month long ethnographic study in 19 Digital Service Centers (DSCs) in Dhaka, Bangladesh that (a) provides an overview of privacy vulnerabilities in public DSCs in Bangladesh, and (b) analyzes the vulnerabilities through the lens of informal markets or bazaars in developing countries. Through data obtained from our observations, contextual inquiries, and interviews with 44 shopkeepers and 64 customers, we describe how infrastructural limitations, local power politics, lack of privacy knowledge, and insufficient protection mechanisms impact customer privacy in these centers. We borrow the concepts of clientelization, reputation, and situated morality from the literature on informal markets to demonstrate that privacy vulnerabilities in DSCs are associated with broader contexts of development, culture, informality, and postcolonial computing.

Our work contributes to ICTD scholarship on security and privacy by offering a new lens to analyze privacy vulnerabilities in public shops that offer digital services in the Global South. We highlight that in addition to cultural insights, informal market insights are equally important to understand these vulnerabilities as customers and employers develop a personalized relationship over time that is shaped by social regulations, impression management, and an alternative version of morality. These insights are particularly useful for ICTD to formulate better design and policy recommendations in the Global South.

2 LITERATURE REVIEW

2.1 Privacy and the Global South

Studies around privacy have predominantly been influenced by Western liberal values, such as the early work of Warren and Brandeis [81] that advocated for the *'right to be alone'*, or Westin's call for freedom from surveillance [82]. These values were later incorporated into many disciplines including sociology, law, political science, and recently computing technologies [50, 59]. However, such liberal values may not be compatible in many Global South contexts where social structures are community-based, traditional, and hierarchical [36]. Many researchers have suggested that privacy is contextual [58], and a situated understanding of privacy is required to unpack design and policy practices [28, 62]. However, privacy research beyond Western contexts and a liberal framing is still at its inception stage [5].

A few HCI studies that have started looking at privacy outside Western contexts report that local values often contrast with the liberal notions of privacy embedded in current computing systems [3]. For example, Abokhodair et al. discuss how political tensions and conservative cultural norms shape security and privacy concerns [1, 2]. Kumaraguru et al. show how the perception of privacy among Indian users are different from Western users [53]. In a more recent study, Srinivasan et al. highlight the privacy tradeoffs that low-income people face when encountering the state's identity system [75]. Sambasivan et al. describe how women in India, Pakistan, and Bangladesh use shared phones and manage and control their personal privacy on those devices [68]. Along these lines, Ahmed et al. explore the privacy issues that arise when people share devices [4, 6], women use platforms such as social media or mobile phone applications [7, 60]. Haque et al. investigate the social ciphering techniques that are used by different social classes in Bangladesh to exchange confidential and sensitive information [40]. All these works inform us about privacy outside the Western world in the context of individual use or shared use among friends or family members. Privacy concerns in public places has mostly remained understudied.

One of the notable exceptions to this is Ahmed et al's work in the informal repair market in Dhaka, Bangladesh [3]. In that work, the authors have documented how the digital data stored in broken mobile phones are often accessed by repairers, and how their conception of privacy is influenced by ignorance and religious beliefs. For example, some repairers think that looking at the media content stored on customers' phones is fine as long as they do not publish somebody's secret photos, while others believe that fear of God prevents them from accessing customers' contents. Although these issues are common among the businessmen in most informal markets in Bangladesh, their findings do not capture the broader social, political, and economic factors that contribute to the practices in those places. In another paper, Ahmed et al. documented the biometric SIM registration process that took place in DSCs in Bangladesh [5], and connected the privacy vulnerabilities there to government-imposed public surveillance. While that paper shows how privacy practices in DSCs can be influenced by national politics, it still misses the social dynamics within the DSCs and between the businessmen and the clients that heavily influence the privacy practices there. Thus, there still remains a gap in conceptualizing the privacy vulnerabilities in DSCs in Bangladesh from their cultural context. Another study around the idea of "privacy in public" was conducted by Best and his colleagues where they interviewed cybercafe users in Ghana and reported the privacy concerns that are associated with voyeuristic learning [16].

2.2 Hybridity and Decolonization of Privacy

In a more recent work, Ahmed et al. demonstrated how both Western and local values of privacy co-exist in urban Bangladesh [6]. The findings of the study resonate with the concept of "hybridity" by Homi Bhabha [18], which refers to the mixing of Western and local cultural values. In a recent qualitative study on the appropriation of social media by urban Indian women, Karusala and her colleagues unpack the relationship between the individual and the collective by showing how being on social media becomes a balancing act between personal and collective values [48]. In her recent work, Arora takes a radical approach and calls for decolonizing privacy studies in the Global South by focusing on traditional periphery of local techno-oligarchs [11]. In Bangladesh, there has been a growing concern of privacy violations from start-up giants such as Pathao and Shohoz that resulted in public backlash [49, 71].

Against these backdrops, individual privacy violations in public places seem to be an important issue even in the Global South.

2.3 Informal Markets, Reputation, and Situated Morality

For developing a deeper understanding of the privacy and security concerns in DSCs, it is important to understand the functioning of such informal markets. A key characteristic of informal markets is how local social relationships play an important role in enforcing rules and contracts [23, 31]. Previous research has captured how informal communities around the world coordinate in the absence of external laws or formal regulations [33, 38]. These studies show how actors resolve disputes through informal rules and social norms that are a consequence of historical social ties and personalized exchanges [61]. These informal institutions, often unwritten, encode rich local knowledge and play a crucial role in reducing information uncertainty and noise in markets [25, 26].

Geertz captures this in his analysis of the "bazaar economy" [37]. He identifies information scarcity as the key identifying feature of informal markets and highlights two intersecting practices of information search: clientelization and bargaining. In clientelization, buyers and sellers cultivate long-lasting relationships and trust through repeated interactions. This practice minimizes search costs for market actors: rather than searching for better deals, buyers negotiate the price with trusted sellers [25]. Similarly, bargaining allows market actors to determine the reservation prices of other actors, a process that is both influenced by social relationships and builds them. We observed similar practices in the DSCs we studied.

The importance of such personalized relations along with ethnic ties have been documented in business communities around the world, especially in South Asia [47]. These relationships play an important role in structuring market ecosystems and are deeply intertwined with the local reputation of market actors. Reputation, here is a function of not just economic activity, but also cultural and social activities. Reputation of merchants is a consequence of how they manage their impressions through mechanisms of self-presentation – for example, a carefully cultivated public persona that is religiously devout [77] is deemed more trustworthy. Subsequently, the trust relations found at these informal markets are a direct consequence of informal reputation mechanisms [39]. In this paper, we analyze the relationships between DSC owners in Dhaka and their clients with this lens – privacy (or its breach) is thus situated within how relationships at the market are not just limited to commercial dealings.

With the informal thriving in the interstices of the formal economy [24], social and economic life here is disconnected from existing legal mechanisms or formal regulation [12]. Galemba [35] argues that Western perspectives have linked "legality" and "the economy" by criminalizing economic practices that do not fit into static "legal" categories. However, in reality, these concepts are fluid and continuously challenged in everyday life. Informal market communities are subsequently able to create alternative visions of legitimacy and morality. In this paper, we use the term "situated morality" – morality embedded in local social contexts – to drive our analysis. We relate it to the notion of "ordinary ethics" [29], which argues that the practices of everyday life are the source of ethics, rather than any universalist legal frameworks.

3 METHODS

We conducted a six-month long ethnography in Dhaka, Bangladesh, from October, 2018 to March, 2019. During this period of time, our ethnographer, who is born and raised in Dhaka, and a native speaker of the Bengali language, visited two types of Digital Service Centers (DSCs) that are prevalent in Bangladesh: Computer Service Shop (CSS) and FlexiLoad Shop (FLS). We briefly describe them below:

3.0.1 Computer Service Shop (CSS). Computer Service Shops (CSSs) are larger shops that offer a comprehensive range of digital services including photocopying, printing and scanning, filling out forms, document editing, and graphic designing. Most of the owners of these shops started with a single photocopy machine or two and gradually expanded their business to meet the digital need of their customers. We collectively refer to the owners and employees of these shops as "shopkeepers".

3.0.2 FlexiLoad Shop (FLS). FlexiLoad Shops (FLSs) are typically small-scale shops that offer digital services to customers in addition to their primary business of selling household goods and grocery shops. Due to the proliferation of mobile phones in Bangladesh, the owners of these shops decided to act as middlemen to offer mobile-based digital services such as *FlexiLoad* (balance recharge service) and bKash/Rocket (financial transaction service) [13, 14]. Some FLSs are simply road-side tiny booths where an agent sits with a chair and a table to offer mobile-based digital services only. We collectively refer to the owners and employees of FLSs as "agents".

Figure 1 shows different types of Digital Service Centers we observed.

3.1 Data Collection

The sample population for our ethnography was generated through convenience and snowball sampling. Our ethnographer (also a co-author of this paper) is familiar with the CSSs in Nilkhet area, a university hub in Dhaka, where he frequently visited shops when he was an undergraduate student. He reached out to those shops and began his observation sessions there. Next he started running a snowball sampling and expanded his field site by visiting CSSs and FLSs in other localities after being recommended by the Nilkhet shopkeepers and agents. This allowed him to gain access to four different diverse neighborhoods (DSCs around universities, commercial places, foreign embassies, and government offices) in Dhaka. He continued visiting new DSCs in these neighborhoods until theoretical saturation was achieved [69].

In total, our ethnographer visited twelve CSSs and seven FLSs. The frequency of visits to each shop in six months ranged between one to six, with two being the average. The owners of these shops were aged between 23 and 60 and their academic background ranged from high-school dropout to bachelor's degree. The average number of daily customers is around 40, with roughly a quarter of them being a returning customer. Table 1 provides an overview of the specific types of services offered by these shops. Our ethnographer arranged prolonged observation sessions (roughly two to four

Figure 1: From left, the first picture is of a Computer Service Shop in Nilkhet area, one of the largest Digital Service Center hubs in Bangladesh. The second picture is of a small road-side FlexiLoad Shop. The third one is an example of a spacious Computer Service Shop with multiple computers.

Types of Services	Digital Service Center (DSC)																		
	Computer Service Shop (CSS)												Flexi Load Shop (FLS)						
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7
Photocopy	✓	✓	✓	✓					✓			✓	✓			✓			✓
Printing and Scanning	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓				✓			
FlexiLoad													✓	✓	✓	✓	✓	✓	✓
Mobile-based Financial Transaction										✓			✓	✓	✓	✓	✓	✓	✓
Filling out Forms & Other Internet Jobs	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓				✓			
Academic Needs		✓	✓			✓	✓	✓			✓	✓							
Document Tampering					✓	✓	✓	✓			✓								
Graphic Design & Other Services	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓							

Table 1: An overview of the specific types of services offered in the Digital Service Centers we observed (n=19)

hours at each DSC) at these places where he took notes and photographs. He conducted semi-structured interviews and contextual inquiries [17]. In total, he interviewed 44 shopkeepers and agents and 64 customers.

Our ethnographer asked shopkeepers and agents questions about their demographic information, educational backgrounds, challenges in their profession, and perceptions and practices around privacy. Interviews with them stretched out throughout the whole duration of his stay at the DSCs. He conducted contextual inquiries as they were doing various tasks related to digital services [17]. The customers were recruited and interviewed at the DSCs. Usually they were in a hurry, so he interviewed those who agreed to give him a few minutes after they had received their services. The interview with each customer usually lasted between 10 to 15 minutes on average. He asked them about their privacy concerns and their prior experiences of privacy breach in these digital service centers.

All the interviews were voluntary and the participants were not paid any compensation (according to the prevalent social norms of Bangladesh, they were offered tea instead of monetary compensation). The responses were written down by the ethnographer in most of the cases, while in a couple of cases, those were audio recorded with the permission of the participants. All the interviews were conducted in Bengali, the observational field notes were written down in Bengali as well.

The protocol of this study was examined and approved by the ethics review boards of the author's institution.

3.2 Data Analysis

All the recorded interviews were directly translated into English by our ethnographer and then analyzed by three members of our research team. It should be noted here that all the members of the analysis team are male, born and raised in Bangladesh, and they are well-familiar with the DSC culture. They are all professional researchers below the age of 35. The data was anonymized before the analysis. Then we used thematic analysis to analyze our data [57]. We followed an inductive approach and did not try to fit the data into an existing framework or any general area of interest in advance of conducting the coding. Three members of the group individually coded each piece of data and labeled them with different themes. Next the labels added by different members were compared. If they matched, they were accepted. When the labels did not match or a fragment of data was associated with multiple labels, the three team members discussed on that piece of data and a consensus was achieved through the discussion to best fit the

data into a single label. In this way, the whole data was grouped in different themes. The team then worked together to group the related themes and find the final set of broader themes that can best illustrate our findings.

Our analysis showed that both infrastructural limitations and lack of knowledge lead to privacy vulnerabilities in public DSCs. There was limited evidence of shopkeepers adopting protection mechanisms to mitigate vulnerabilities. More importantly, the broader themes that emerged from our findings were clientelization, reputation, and situated morality – concepts that are associated with the organization of informal markets or bazaars in developing countries.

4 AN OVERVIEW OF PUBLIC DIGITAL SERVICE CENTERS

4.1 Infrastructural Limitations

Like many other places in a developing country, the DSCs of Dhaka have a lot of infrastructural limitations. These include absence of a privacy policy, lack of robust technologies, and adherence to paper-based bookkeeping.

4.1.1 Absence of a privacy policy. Our ethnographer categorically asked the owners of each DSC if they had any formal or legal privacy policy for their customers. None of them could answer anything about it and the concept of privacy policy was quite foreign to them. None of the shopkeepers or the FLS agents was formally trained about customer privacy either.

4.1.2 Lack of robust technologies. Most of the CSSs that our ethnographer visited had old 32-bit desktop computers, running pirated old versions of Windows operating system, without software updates being installed regularly. The processors and the RAMs had a much lower configuration. As a result, those computers were operating very slowly. During his observation sessions, the ethnographer saw multiple cases when the computer got hung and the shopkeeper had to reboot, which also took a lot of time. The shopkeepers were often "refreshing" the desktop with a hope to make the computer run faster.

4.1.3 Adherence to paper-based bookkeeping. As mentioned before, FlexiLoad is the primary service offered in FLSs, and this entire process adheres to a paper-based bookkeeping method. When customers want to FlexiLoad to their number, the agent usually notes down the number in his notebook, or at times asks the customers to write down the number by themselves. The amount of money is recorded beside each number and the agent uses this notebook entry to load the required amount to the corresponding number from his own phone.

During his observations, the ethnographer saw that these notebooks are always exposed. When one customer's phone number is being written down, others could easily track and see that number if they want to. The agents do not have any concern about this and they allowed us to take pictures of these notebooks. Figure 2 shows an exposed notebook that contains important information like mobile banking account numbers, phone numbers etc.

4.2 Local Power Politics

During his observation sessions, our ethnographer noticed that the FLSs were occasionally affected by local goons, politicians, and other kinds of external powers. Some of these people take services for free and the agents often do not resist them as they are "powerful". While the exercise of power itself is a big concern, at times their power also invades other people's privacy. One agent said:

> "The local political leader makes me disclose the phone numbers of all the residents in this locality. He wants to use that list to call/text people as a part of his election campaign. At times, local goons forcefully take the mobile phone numbers of local girls and harass them over phone. Recently, some of the "Chatro League" (local student union supported by the current government in power) leaders are maintaining a list of people whom they want to leave the society. They gave me a list (he showed the list). These leaders harass me to give them information about the people on this list. These leaders also take information about other customers illegally to use for other purposes".

The agents also mentioned that they are afraid of these local goons and prefer to avoid any chaos. They think that there is no hope in complaining against them because they are often connected with political leaders and the law enforcement agency wouldn't take any action against them.

4.3 Lack of Knowledge

The shopkeepers and agents working at the DSCs lack knowledge regarding digital privacy and computer. In many cases, our ethnographer found that they were not careful enough to protect the privacy of the customers. Customers, on the other hand, are in a rush usually, and as such, neither party pays enough attention to privacy.

In one of the Computer Service Shops, a customer came to print the admit card for his entrance exam to Bangladesh Army. The card was required to be downloaded from his online account where he registered for the exam. The shopkeeper asked for the account credentials and the customer responded by saying out loud the username and the password of his account. This was overheard by our ethnographer and another customer standing nearby. After the printing was done, the customer quickly left the shop without deleting the card from the computer.

In another Computer Service Shop, he saw a 52 years old private company employee coming to fill up an Indian visa application form. The shopkeeper opened a browser, downloaded the form, and opened it with Microsoft Word. He then asked the customer to start filling up the form. After a few minutes, when the customer needed help for filling up a field in the form, he consulted the shopkeeper. The shopkeeper then started searching on the same computer to find another visa form that had previously been filled up by another customer. After finding one such form and resolving the issue, he didn't close the form and asked the customer instead to check it whenever he needed help rather than consult him every time. The customer then started filling up his form again while the other form was kept open the whole time.

Figure 2: An exposed notebook inside a FLS.

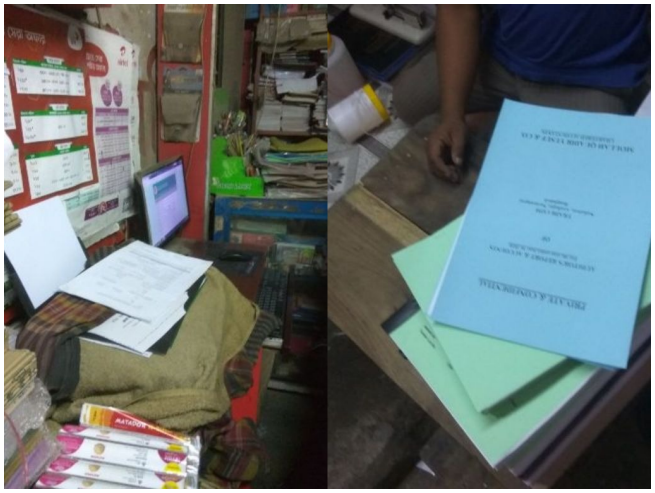

Figure 3: On the left, documents that are in the queue for photocopy have been put in an open space. On the right, the shopkeeper is doing the binding of a "private and confidential" document, which is clearly visible to other customers.

When the shopkeepers were asked about the possible vulnerabilities that can arise from poor handling of private data, they did not take that seriously. In several other cases, we found that the computers were affected with malware. The shopkeepers acknowledged their presence but claimed the threat to be "not very serious" and "not harmful for the customers". They were also not aware about specific malware such as keyloggers. While they agreed that antivirus software would make their computers safer, they did not want to spend money for purchasing those software.

The ethnographer also noticed huge stacks of paper scattered around the shops, ranging from thesis papers and class notes to applications forms and utility bills. These documents contained private information such as name, address, salary, location, and phone numbers. These documents are kept exposed and the shopkeepers did not seem to have any concerns about this. Similarly, when he checked the computers of these shops with the shopkeepers, he found a huge collection of photos, certificates, visa forms, job applications, utility bills, wedding cards, school assignments, air tickets, and CVs, just to mention a few. Figure 3 shows a couple of examples where documents are put in an open space.

4.4 Insufficient Protection Mechanisms

There was limited evidence of shopkeepers and agents adopting privacy protection mechanisms for their customers.

4.4.1 Technical Means. Some DSCs claim that they adopt technical means to protect their computers, but none of those appeared to be sufficient in our analysis. For example, they think that using a pirated, outdated antivirus software is enough to keep their computers secure. Only two CSSs were using original and updated antivirus software. They also use passwords that are weak and guessable (simple patterns such as "12345") to lock their computers. In one shop, the ethnographer found a CCTV camera and the shopkeeper told him that they put the camera to watch over the customers so that they wouldn't do "bad stuff". When he further asked if the camera was good enough to capture the computer monitor and what kind of "bad stuff" they wanted to stop, it turned out that they were more interested in ensuring that customers were not stealing any hardware device from the shop.

4.4.2 Content Deletion. Shopkeepers extensively use older documents as templates so that new customers can view them and customize. One shopkeeper who offers graphic designing services in his computer shop mentioned that this is a standard practice for designing wedding cards. The ethnographer then told him to show some samples, which he did. When asked if any customers request to delete the files after the job is done, the shopkeeper replied that very few do so, that too for exclusivity of design rather than for privacy concerns.

However, if customers explicitly ask to not store their contents, shopkeepers delete those contents. In fact, a couple of shopkeepers told us that their default strategy is deletion and one of them doesn't store customers' contents even if he is requested to do so. "Why would I fill my own hard drive with customers' documents?", he said. He acknowledged that documents downloaded from emails are not deleted though.

Other shopkeepers periodically delete older contents that they consider non-reusable, usually at the end of the day or at their free time. They understand the difference between simple delete and Shift delete. One shopkeeper follows a particular strategy to delete older contents:

> "If customers ask me to store their documents, I follow a pattern and save them in a folder that is named on the current date. Once in every 7-10 days, I review these folders and delete the relatively older ones. In this way, I never store customers' contents for a long term, unless a frequent customer makes any special request."

This response indicates that frequent or regular customers are an important consideration for many shopkeepers, which is a significant aspect of informal market. In fact, the privacy vulnerabilities in DSCs can be better understood through the lens of informal market because these centers share a lot of common elements with other informal markets in developing countries. We offer a detailed analysis of these vulnerabilities in the next section.

5 PRIVACY VULNERABILITIES - AN ANALYSIS THROUGH THE LENS OF INFORMAL MARKETS

5.1 Clientelization

As mentioned above, DSCs, especially the CSSs contain a lot of sensitive customer documents, both digitally and on paper. It turned out that clientelization, or repeated interactions between shopkeepers and customers, is the major reason these documents are stored and exposed in such manner. Shopkeepers tend to offer special services to their "regular customers". If a document of such a customer needs to be copied every now and then, the shopkeeper would eventually scan and store it in his computer, and then print from the scanned copy as this would make life easier for the customer. One such customer, a 25 years old male said:

> "I have been applying for jobs for some time now. It takes me a lot of time to wait at the shop for getting the papers photocopied. So, I have decided to leave the scanned copy at the computer of the shop. In the future, every time I will need a copy, I will call ahead the shopkeeper to get that printed for me, and I will just pick up at my convenient time. It is also better than carrying the papers every time, because I may lose them during commuting".

The shopkeepers mentioned that this is indeed a common practice. Some regular customers even do not have a computer so they ask the shopkeepers to store these documents for them. There was a vast amount of private information in some computers that are stored in different folders without any password protection. The shopkeepers said that they keep storing the documents until the hard drive is full, and then they delete the older documents. The paper-based documents are periodically trashed when the customers leave them for a prolonged period of time.

This practice of clientelization is extended to public figures too. During one observation session, a female Member of Parliament (MP) came to the shop to photocopy 1000 pages of documents, seven copies for each, and asked if it could be done immediately. The shopkeeper was visibly busy with other customers but he did not want to refuse the MP as she was a regular customer. He politely asked her to leave the documents there till the next morning to have them copied overnight. The shopkeeper put them in a visible place and our ethnographer could see that those documents contained TIN certificate, 37 case files, property papers, and income certificates.

Our ethnographer observed a similar trend in the FLSs he visited. A personalized relationship is developed between customers and agents in those shops. A lot of customers like the informal atmosphere of a neighborhood FLS and they don't want to commute to formal and professional Customer Service Centers for their mobile phone related services. One such customer said:

> "The representatives at Customer Service Centers are usually more educated and they might laugh at me if I visit them for a trivial issue. It might seem 'lame' to them. I would like to go to my local FLS agent instead as he is a known and friendly guy. It's easier to talk to him".

Agents in FLSs eventually establish a deep friendship with these regular customers as they grow older. In one of his visits to a FLS, the ethnographer saw the agent receiving a call from a customer, requesting him to FlexiLoad to that customer's number. The agent retrieved the number from his notebook, loaded the mentioned amount, and called back the customer to confirm. Later the agent described his relationship with the customer:

> "This customer is a 70 years old retired bank officer whom I respect a lot and call 'uncle'. He frequently visits my shop for FlexiLoad and grocery purposes. His phone number is stored in my notebook. I offer this special service to a few older regular customers like him out of respect and friendship and they pay the money next time they visit the shop".

The ethnographer saw agents at other FLSs also giving special attention to older regular customers. One specific incident drew his attention where an agent spent almost half an hour with an older customer to fix several issues in his Android handset.

5.2 Reputation

Reputation plays an important role in the daily business of the FlexiLoad Shops. Agents tend to be helpful and create a positive image among customers there. Some of them provide extra attention to protect the privacy of female customers. One such agent said,

> "Whenever a female customer doesn't feel comfortable to put her number on my notebook for FlexiLoad purposes, I understand her privacy concerns and give her my phone instead, to input her number directly. I also let her delete the confirmation message from the mobile phone operator about the successful transaction, as that message also contains her number. I put a symbolic entry (the last two digits, for example) on my notebook, so that no trace of her (the female customer's) number exists anywhere".

There were many other instances where both male and female customers visited the shop for FlexiLoad purposes, but then asked the agent to help them with other issues on their phones. We saw customers asking for help with checking balance (FLS1), deleting some photos to clear up the gallery (FLS2), installing and setting up Uber (FLS3), finding a number from the message inbox (FLS6), fixing battery issues (FLS6) etc. In some cases, the agents were in possession of the phone for an extended period of time but they didn't seem to misuse this privilege in any way. One agent said:

> "I have been doing this business for the last 20 years in this neighborhood. Everybody here knows me by my name. They all know what kind of a person I am, and what I can and cannot do. They all know that I

> am not a person to do a dirty thing. This required a lot of work to build this reputation and I cannot just ruin that by doing a cheap thing".

The customers that were interviewed also said that in general, agents care about their reputation and do not invade customer privacy. All these findings inform us how agents shape their reputation through careful impression management [20, 77].

However, not all agents are concerned about their reputation. For example, one female customer shared her story of being harassed by an agent:

> "It was 2-3 months back, I used to get a call from a number frequently. It was a male voice and the guy wanted to make friendship. I refused as I was not interested but he kept harassing me time and again. By some means, I was able to identify the location from which the call had been coming and eventually I realized that it was the neighboring shop from which I regularly FlexiLoad to my number. I confronted the agent and finally he stopped harassing me".

Some shopkeepers and agents are also afraid of being the subject of public rage and mob justice. As one agent said:

> "You don't do anything bad because you fear public beating. If public become angry with you, they will kill you".

5.3 Situated Morality

Situated morality emerged as a recurring theme during our analysis of the participant responses. On the one hand, shopkeepers and agents feel that they have a moral obligation to keep customers' trust. As one agent said:

> "I am aware that customers' personal files should not be accessed, including gallery, call logs or messages. But some customers are less educated or unaware of technology-related stuff, especially the middle aged low-income people (guards, housemaids, etc.), so I need to help them. Sometimes customers ask to send money to a specific number which they cannot tell clearly. Then they give their handset to me and I find out the number from their call logs, following their instructions. If they ask to find out the number from a stored photo, then I need to access their gallery. Sometimes I come across some private photos, which I think should not be exposed, but I just ignore them. I complete my task and then I return the phone to the customer".

On the other hand, our ethnographer found shopkeepers and agents offering services that are while clearly illegal, were morally acceptable to them (and often the customers).

5.3.1 Assignment Plagiarization. In Nilkhet, a university hub area, he saw students looking for "thesis/project writing assistance" in multiple DSCs. One student came for assistance for his Bachelor of Business Administration (BBA) degree project who did not know how to write the objectives, findings, and discussion sections of the project. The shopkeeper pulled up a folder that had all the previously completed thesis/project documents in that shop. By mixing and matching from several such documents, the shopkeeper wrote those sections for the student. In exchange for his "assistance", the student paid 2,000 BDT (1 BDT = 0.012 USD approx.) to the shopkeeper and took the electronic document in a flash drive.

The shopkeepers there even developed a skill to bypass plagiarism detection software. One customer, who is a student of a local university, told the ethnographer:

> "Our university has a software to detect if the assignment is copied or not. If the paper scores less than 40 in the software, it passes the plagiarism check. The shopkeepers here are talented enough to prepare papers that score below 40".

5.3.2 Statement of Purpose Preparation. The ethnographer even observed customers soliciting for writing their Statement of Purpose (SOP) for graduate applications to foreign schools. He saw a man bringing his daughter for such service and the shopkeeper helping them by collating a few sample SOPs.

5.3.3 Document Forgery. In one of the CSSs, one customer came to make some illegal edits to a medical certificate. The shopkeeper initially told the customer that the font would look exactly the same as the original document in the edited part but later could not deliver it that way. As a result, he took a smaller amount of money, about 100-150 BDT (1-2 USD). Later the shopkeeper told the ethnographer that DSCs in Nilkhet area are more efficient in offering these kinds of service and those centers prepare illegal and duplicate documents that look so real and can't be differentiated from the original. He saw another instance of document forgery in another CSS where some central board examination certificates were being altered.

During the interviews, the shopkeepers and the customers in those computer service shops said that document forgery is a pretty normal job there and the local law enforcement agency is not concerned about such illegal activities. A couple of shopkeepers also said that the local police probably do not understand the "digital stuff".

6 DISCUSSION

In the sections above, we have presented our findings around the privacy vulnerabilities in informal DSCs in Bangladesh.

Our findings show that DSCs in Dhaka, Bangladesh, share a lot of common elements with informal markets or bazaars of Egypt, Kenya, Ghana, Iran and India [25, 37, 55, 56, 77]. In order to formulate a comprehensive privacy policy in these developing nations, it is therefore important to gain an understanding of how these local informal markets or bazaars operate. The liberal Western values of privacy, including privacy in public places, do not incorporate this informality and therefore it is necessary to conceptualize "privacy in public" in a different way in the Global South. Furthermore, our study of public places illuminates new findings that have not been reported in prior studies in the Global South that focused on private spaces [4, 6, 7, 53, 60, 68]. Our findings demonstrate that any discourse on privacy in public places in the Global South should incorporate informal market issues (clientelization, reputation management, and situated morality) and the role of associated external factors (mob justice, local politics, etc.).

We note that many practices that have been reported in our study, including cut-and-paste and plagiarism services, are ubiquitous and not exclusive to the Global South. The contexts within which these activities take place, however, are significantly different. These phenomena cannot be explained by a cultural lens alone; instead we use the conceptual socio-economic and political framework of informal markets to analyze existing market practices that are built on reputation and trust, and the inherent vulnerabilities related to privacy. We discuss some of these perspectives in relation to our findings below.

6.1 Personalized Relationships and Awareness

We begin by discussing clientelization in this regard. With clientelization, or repeated transactions with familiar customers, the DSC becomes a hub for information storage for these customers. The DSC stores their information – paper copy or digital versions – so that the customers can use or collect them later. These regular customers are also the most vulnerable group as they entrust a huge amount of private data to the DSC, which, in most cases, lack the basic protection mechanisms. We also observed that employees and regular customers eventually establish deep social ties and friendships, and as such, these personalized relations could be leveraged to make the employees more aware so that they adopt better mechanisms to protect the privacy of the people whom they consider as friends. An important strategy here would be educating the employees about the potential consequences their actions might bring to their customers.

The personalized relationship between the employees and customers, however, operates within a broader political context and can get disrupted by the exercise of external political power. While the employees are often forced to share the vulnerable information of their customers with the local goons, they still maintain their impressions before the customers both for the sake of their personalized relationship and their business with them [77]. We argue that both design and policy interventions are required here for protecting the private information of general people in such contexts. The government should ensure the support of law-enforcement entities to secure these DSCs. At the same time, there should be social awareness and protest against such privacy breaches. The lessons from existing ICTD and HCI work around social movement can be extended to this context to develop an effective measure to secure the private data of the general people at DSCs.

We offer a few concrete suggestions in this regard. To re-design privacy mechanisms in these DSCs, designers and policy makers could focus on reputation-based accountability [22], communal surveillance [83], and empowerment of DSCs [70]. In addition, CVE and IVR tools can be used for creating awareness about privacy breaches among people as both have been demonstrated to be successful technologies in the Indian subcontinent [52, 80]. Finally, to unite people and record their grievances in the Global South, we recommend using mobile-phone based reporting [7] and citizen journalism [32].

6.2 Social Regulation and Legitimacy

We also observed that many DSC employees are afraid of being the subject of public rage and mob justice if they do something bad. This fear of mob justice is often common in the Global South [10, 65], and still understudied in ICTD and HCI. Although law enforcement agencies are often weak there, employees often refrain themselves from doing anything unethical out of their fear of mob justice. A few recent incidents of mob justice and public beating consolidate this sentiment [76, 78].

The ineffectiveness of law enforcement agencies and the absence of a robust legal infrastructure result in market actors developing an alternative vision of legitimacy and morality among employees and customers, which is similar to the trend observed in informal markets around the world [56]. Thus while many of the services offered here might be illegal, they are still acceptable to market actors – both shopkeepers and customers. Borrowing from Schendel and Abrahams's [79] analysis of "illegal" activities around the world, we propose using the contracted term "(il)licit" to describe such activities that are prohibited by existing laws and yet licit, in that they correspond to socially acceptable informal activities. For example, contents of older customers are reused to assist new customers. These contents include visa application forms and wedding cards that contain private information including name, address, and monthly salary. This has the potential to create a serious breach to the privacy of older customers. However, shopkeepers usually delete contents if customers explicitly ask to do so, indicating a capacity for the market to self-regulate. Customers should thus be made more aware of the risks they face so that they can leverage their social connections and become more proactive in making their contents get deleted.

Assignment/thesis and SOP plagiarizing is another major service provided by some of the shops around university areas. While we concede that some of these activities, such as document forgery, might require legal interventions, from the perspective of understanding privacy, we argue that these practices problematize our notions of what activities count as "illegal". To understand informal activities in such markets, we need to think beyond the existing legal/illegal dichotomy, and instead study how the (il)licit is shaped by everyday interactions. Thus, even with respect to privacy and security, we need to focus on what community believes is socially legitimate rather than rigid definitions derived from Western constructs of legality.

At the same time, we discourage any attempt to morally justify these activities as this can lead to total relativism in ethical reasoning to the point where it might become very difficult to draw the line between "right" and "wrong". We note that these actions of academic plagiarism and certificate forgery impose a "negative externality" [21] on people who are competing in similar exams or applications – people who are not present when these actions are taken. When the employees and customers of DSCs engage in these il(licit) activities, the interests of these competing groups are compromised, which should not be overlooked during any discourse on situated morality.

Further, we stress on the importance of understanding the relationship of the state to informality and illegality. As we discuss, legal actors often choose to turn a blind eye to informal practices, but this is heavily contingent on local politics and the priorities of resource-constrained law enforcement agencies. For example, law enforcement agencies give greater weight to protecting communal

harmony than protecting individual privacy. The morality of everyday life emerges out of this tense equilibrium at the market; the contours of what is acceptable and what is not are shaped by the fluidity of informal relationships and formal constraints.

6.3 Local Strategies Supporting Privacy

When users encounter privacy and security challenges, their practices are often influenced by their risk perceptions [41] and past experiences [30, 64]. We see this reflected in our study in different ways. For instance, we observed gender-specific privacy challenges at the DSCs in Bangladesh. From interviews with agents and customers, we came to know about several past incidents where female customers' phone numbers were leaked from DSCs to other people, and were used as a means of harassing those customers. In a recent study on online abuse experiences and coping strategies of South Asian women [67], it has also been reported that female customers receive unwanted phone calls after they visit phone recharge (top-up) shops and employees of these shops sell their phone numbers in bulk packages to strangers. Consequently, to enhance their reputation, many agents have started taking different strategies for protecting their female customers' information and credentials, although it might conflict with their usual information storage and customer service procedure. This can be connected with prior work on harassment and gender-specific privacy challenges in Bangladesh where digital platforms and technologies, combined with the lack of specific privacy policies have put women in vulnerable situations, often making them a victim of personal and social harassment [7, 60].

To thwart such issues, agents in some shops do not ask the female customers to write down their phone number in the notebook; rather they hand over their phone (with agent/admin privilege for FlexiLoad) to those customers to complete the FlexiLoad by themselves. Such strategies protect female customers' phone numbers from being exposed to adversaries through DSC's notebook. However, they introduce risks in other dimensions – for example, if the customers fail to duly complete the FlexiLoad process by themselves, it might cause issues for the agents, potentially even leading to business loss if female customers mistakenly load an incorrect mobile phone account. The strategy of not keeping the log of female customers' phone numbers also compromises the agent's usual bookkeeping procedure in resolving future disputes with customers. Furthermore, handing over their phone to customers could lead to privacy leakage and misuse of information stored in that phone [3]. Thus, while ad-hoc strategies might address a particular privacy concern, they introduce risk in other dimensions. Any design solution tackling privacy and security concerns will need to address the complex ecosystem of social practices, instead of expecting a user to perform privacy and security tasks.

6.4 Information Asymmetry

We would like to stress that these DSCs are commercial places and people are paying for the services. Therefore, there is a tacit expectation that DSCs will maintain customer privacy and protect personal and sensitive information. While there is an absence of law enforcement in informal markets, there is little recourse even in the formal markets with respect to privacy. Legal procedures related to privacy are relatively new in Bangladesh [5]. The Information and Communication Technology (ICT) Act of 2006 allows individuals to bring criminal proceedings against perpetrators of such intrusion and unauthorized access [66]; what it fails to take into account is that these perpetrators carry out their operations anonymously and thus, in most cases, it is difficult to identify them. In other words, a preventive framework at the pre-breach level is simply nonexistent. There is no comprehensive data protection for consumers and general public for their non electronic data provided to various organizations, companies, and corporations [66]. The absence of possible legal recourse suggests that interventions need to leverage social and cultural norms, and involve market actors at public places such as the DSCs.

6.5 Postcolonial Computing and Privacy

Beyond these implications, we also argue that our study contributes to the postcolonial computing literature of ICTD and related fields [8, 43, 63] that shows how a foreign technology that travels from the West to the Global South often struggles for cultural and infrastructural mismatches. Digital Computing, which has its root in the West is often shaped by Western assumptions where, in many cases, issues such as "clientelization" or "local goons" are not relevant. However, these are everyday reality in many places in the Global South. Now, as digitization is happening in the Global South, the countries are confronting a series of challenges that were unforeseen. We argue that the countries need to be careful to develop a robust infrastructure before introducing a new digital service. Otherwise, many citizens may suffer from a technology breakdown. At the same time, the countries need to be careful that, in making a room for a robust technological infrastructure, they do not drive away their cultural resources such as community bond, trust, faith, and respect.

7 CONCLUSION

The findings from our study reveal the privacy vulnerabilities posed to users due to insecure storage of their private information, and reuse of their personal documents and artifacts in DSCs. We identified the social and political challenges, and the lack of policy, awareness, and resources that hinder the privacy practices at DSCs. We also investigated the reciprocal relationship between customers and employees through the lens of informal market and showed how practices such as clientelization and impression management regulate privacy behaviors. We highlighted an alternative version of morality as well, which generates new insights on ethical implications of privacy. Taken together, our work offers a new orientation to analyze privacy vulnerabilities in public shops that offer digital services in developing nations.

8 ACKNOWLEDGMENTS

This research was made possible by 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), and International Fulbright Centennial Fellowship of Syed Ishtiaque Ahmed.

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

[4] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017a. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (Dec. 2017), 20 pages. DOI: **http://dx.doi.org/10.1145/3134652**

[5] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017b. 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 (CHI '17)*. ACM, New York, NY, USA, 906–918. DOI: **http://dx.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 (CHI '19)*. ACM, New York, NY, USA, Article 180, 13 pages. DOI: **http://dx.doi.org/10.1145/3290605.3300410**

[7] 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 *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2695–2704. DOI: **http://dx.doi.org/10.1145/2556288.2557376**

[8] Syed Ishtiaque Ahmed, Nusrat Jahan Mim, and Steven J. Jackson. 2015. Residual Mobilities: Infrastructural Displacement and Post-Colonial Computing in Bangladesh. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 437–446. DOI: **http://dx.doi.org/10.1145/2702123.2702573**

[9] Md. Alauddin and Mustafa Manir Chowdhury. 2015. Small and Medium Enterprise in Bangladesh-Prospects and Challenges. *Global Journal of Management and Business Research* 15, 7 (2015).

[10] Arifur Rahman Rabbi. 2019. Child-abduction rumour: Woman among three lynched in 3 districts. (July 2019). **https://www.dhakatribune.com/bangladesh/crime/2019/07/20/2-suspected-kidnappers-killed-in-dhaka-narayanganj-mob-beating**

[11] Payal Arora. 2019a. Decolonizing privacy studies. *Television and New Media* 20, 4 (2019), 366–378.

[12] Payal Arora. 2019b. General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. *Surveillance & Society* 17, 5 (2019), 717–725.

[13] Anonymous Author. 2010. bKash. (Mar 2010). Retrieved March 31, 2019 from **https://www.bkash.com/**

[14] Anonymous Author. 2011. Rocket - Dutch Bangla Bank. (Mar 2011). Retrieved March 31, 2019 from **https://www.dutchbanglabank.com/rocket/rocket.html**

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

[16] Michael Best, Bence Kollanyi, and Sunil Garg. 2012. Sharing in Public: Working With Others in Ghanaian Cybercafes. In *Proc. ICTD'12*. ACM, 211–220.

[17] Hugh Beyer and Karen Holtzblatt. 1998. *Contextual design: Defining customer-centered systems*. Morgan Kaufmann Publishers.

[18] Homi Bhabha. 1994. *The location of culture*. Routledge, London.

[19] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. 2017. When the Internet Goes Down in Bangladesh. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 1591–1604. DOI: **http://dx.doi.org/10.1145/2998181.2998237**

[20] D. B. Bromley. 1993. *Reputation, Image and Impression Management*. John Wiley and Sons.

[21] James Buchanan and Craig Stubblebine. 1962. Externality. *Economica* 29, 116 (1962), 371–384.

[22] Madalina Busuioc and Martin Lodge. 2016. The reputational basis of public accountability. *Governance* 29, 2 (2016), 247–263.

[23] Miguel Angel Centeno and Alejandro Portes. 2006. The informal economy in the shadow of the state. *Out of the shadows: Political action and the informal economy in Latin America* (2006), 23–48.

[24] Priyank Chandra. 2017. Informality and invisibility: Traditional technologies as tools for collaboration in an informal market. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4765–4775.

[25] Priyank Chandra, Syed Ishtiaque Ahmed, and Joyojeet Pal. 2017. Market Practices and the Bazaar: Technology Consumption in Informal ICT Markets in the Global South. In *Proc. CHI '17*. ACM, Forthcoming.

[26] Priyank Chandra and Joyojeet Pal. 2019. Rumors and Collective Sensemaking: Managing Ambiguity in an Informal Marketplace. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 333.

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

[28] 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. DOI: **http://dx.doi.org/10.1007/s10606-017-9276-y**

[29] Veena Das. 2012. Ordinary ethics. *A companion to moral anthropology* (2012), 133–149.

[30] 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.

[31] Hernando de Soto. 1989. *The Other Path: The Invisible Revolution in the Third World*. Harper & Row.

[32] Hira Ejaz, Syed Ali Hussain, and Agha Ali Raza. 2018. The case for IVR-based citizen journalism in Pakistan. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 87–94.

[33] Robert C Ellickson. 1991. *Order without law*. Harvard University Press.

[34] Fayika Farhat Nova, Mohammad Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed, and Shion Guha. 2019. Online sexual harassment over anonymous social media in Bangladesh. 1–12. DOI: **http://dx.doi.org/10.1145/3287098.3287107**

[35] Rebecca B Galemba. 2008. Informal and illicit entrepreneurs: Fighting for a place in the neoliberal economic order. *Anthropology of Work Review* 29, 2 (2008), 19–25.

[36] 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**

[37] Clifford Geertz. 1978. The bazaar economy: Information and search in peasant marketing. *The American Economic Review* 68, 2 (1978), 28–32.

[38] Avner Greif. 1993. Contract enforceability and economic institutions in early trade: The Maghribi traders' coalition. *The American economic review* (1993), 525–548.

[39] Avner Greif. 1997. *Informal contract enforcement: lessons from medieval trade*. Number 145. John M. Olin Program in Law and Economics, Stanford Law School.

[40] S M Taiabul Haque, Pratyasha Saha, Muhammad Sajidur Rahman, and Syed Ishtiaque Ahmed. 2017. 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* Vol. 3, CSCW (2017), Article 173.

[41] 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.

[42] Ihsan Qadir. 2017. Lack of facilities at e-Khidmat Markaz irks citizens. (Oct. 2017). **https://www.pakistantoday.com.pk/2017/10/03/lack-of-facilities-at-e-khidmat-markaz-irks-citizens/**

[43] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E. Grinter. 2010. Postcolonial Computing: A Lens on Design and Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1311–1320. DOI: **http://dx.doi.org/10.1145/1753326.1753522**

[44] Md. Toriqul Islam. 2018a. Urge to enact privacy and data protection law. (Jan 2018). Retrieved March 31, 2019 from **https://www.thedailystar.net/law-our-rights/urge-enact-privacy-and-data-protection-law-1527220**

[45] Md. Toriqul Islam and Dr. Md. Ershadul Karim. 2018. Protecting privacy in biometric data. (july 2018). Retrieved March 31, 2019 from **https://www.thedailystar.net/law-our-rights/rights-advocacy/protecting-privacy-biometric-data-1602577**

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

[47] Gopalkrishnan R Iyer. 1999. The impact of religion and reputation in the organization of Indian merchant communities. *Journal of Business & Industrial Marketing* 14, 2 (1999), 102–121.

[48] Naveena Karusala, Apoorva Bhalla, and Neha Kumar. 2019. Privacy, patriarchy, and participation on social media. In *Proc. DIS'19*. ACM, 511–526.

[49] Wasif Jamal Khan. 2019. Can the government keep our data safe? (Sep 2019). Retrieved December 19, 2019 from **https://www.dhakatribune.com/opinion/op-ed/2019/09/25/can-the-government-keep-our-data-safe**

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

[51] Kritti Bhalla. 2020. IT Ministry Seeks Permission To Run 3.7 Lakh Rural Kiosks For Digital Services. (April 2020). **https://inc42.com/buzz/it-ministry-seeks-permission-to-run-3-7-lakh-rural-kiosks-for-digital-services/**

[52] Neha Kumar, Trevor Perrier, Michelle Desmond, Kiersten Israel-Ballard, Vikrant Kumar, Sudip Mahapatra, Anil Mishra, Shreya Agarwal, Rikin Gandhi, Pallavi Lal, and Richard Anderson. 2015. Projecting Health: Community-led Video Education for Maternal Health. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development (ICTD '15)*. ACM, New York, NY, USA, Article 17, 10 pages. DOI:**http://dx.doi.org/10.1145/2737856.2738023**

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

[54] Nuruzzaman Labu. 2018. Fraud continues as pre-registered SIMs easily available. (May 2018). Retrieved March 31, 2019 from **https://www.dhakatribune.com/bangladesh/crime/2018/05/19/fraud-continues-as-pre-registered-sims-easily-available**

[55] Fergus Lyon. 2000. Trust, networks and norms: The creation of social capital in agricultural economies in ghana. *World Development* 28, 4 (2000), 663–681.

[56] Fergus Lyon and Gina Porter. 2009. Market institutions, trust and norms: exploring moral economies in Nigerian food systems. *Cambridge Journal of Economics* 33, 5 (2009), 903–920.

[57] Moira Maguire and Brid Delahunt. 2017. Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education* 9, 3 (2017).

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

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

[60] 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 (ICTD '19)*. ACM, New York, NY, USA, Article 1, 12 pages. DOI:**http://dx.doi.org/10.1145/3287098.3287107**

[61] John Nye. 2008. Institutions and the institutional environment. *New Institutional Economics, a guidebook', Cambridge University Press, Cambridge* (2008), 67–81.

[62] 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.

[63] Kavita Philip, Lilly Irani, and Paul Dourish. 2012. Postcolonial Computing: A Tactical Survey. *Science, Technology, & Human Values* 37, 1 (2012), 3–29. DOI:**http://dx.doi.org/10.1177/0162243910389594**

[64] 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.

[65] Star Report. 2019. Mobs beat five dead for 'kidnapping'. (July 2019). **https://www.thedailystar.net/frontpage/news/mobs-beat-2-dead-kidnapping-1774471**

[66] Himaloya Saha and Saquib Rahman. 2015. Personal Data Protection Laws Concerning Bangladesh. *IOSR Journal Of Humanities And Social Science* 15, 8 (Aug. 2015), 34–43. DOI:**http://dx.doi.org/10.9790/0837-20823443**

[67] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Senley Gaytan-Lugo, David Nemer, Elie Burzstein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proc. CHI'19*. ACM, 1–14.

[68] 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.

[69] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity* 52, 4 (01 Jul 2018), 1893–1907. DOI:**http://dx.doi.org/10.1007/s11135-017-0574-8**

[70] Amartya Sen. 1999. *Development as Freedom.* Oxford University Press.

[71] Shaikh Shahrukh. 2019. Dmoney and Shohoz breaches user data. (Nov 2019). Retrieved December 19, 2019 from **https://www.observerbd.com/details.php?id=229125**

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

[73] Khondoker Md Shoyeb. 2010. Tiny business, shiny prospect. (feb 2010). Retrieved March 31, 2019 from **https://www.thedailystar.net/news-detail-124282**

[74] Snigdha Poonam. 2017. Stalkers' delight: Mobile numbers of girls for sale in UP recharge shops. (Feb. 2017). **https://www.hindustantimes.com/india-news/girls-mobile-numbers-up-for-sale-in-uttar-pradesh-price-rs-50-to-rs-500/story-5lYPcav12h7rnW6A6UDLLI.html**

[75] 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.

[76] Syed Samiul Basher Anik. 2019. Alarming spike in mob justice. (July 2019). **https://www.dhakatribune.com/bangladesh/2019/07/22/alarming-spike-in-mob-justice**

[77] Soheil Torkan. 2017. *The bazaar. Embedded Alternative to Globalization?* Ph.D. Dissertation. Baarn: Real Life Publishing De Weijer uitgeverij.

[78] Unknown Author. 2019. Mobs lynch eight over child abduction rumours. *BBC News* (July 2019). **https://www.bbc.com/news/world-asia-49102074**

[79] Willem Van Schendel and Itty Abraham. 2005. *Illicit flows and criminal things: States, borders, and the other side of globalization.* Indiana University Press.

[80] Aditya Vashistha and William Thies. 2012. IVR Junction: Building Scalable and Distributed Voice Forums in the Developing World. In *Presented as part of the 6th USENIX/ACM Workshop on Networked Systems for Developing Regions*. USENIX, Boston, MA.

[81] 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**

[82] Alan F. Westin. Alan F. Westin. *Washington and Lee Law Review* 25 (????), 166. Issue 1. **https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20**

[83] Nils Zurawski. 2004. "I Know Where You Live" - Aspects of Watching, Surveillance and Social Control in a Conflict Zone (Northern Ireland). *Surveillance and Society* 2, 4 (2004).