Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh

Syed Ishtiaque Ahmed[1], Md. Romael Hoque[2], Shion Guha[3], Md. Rashidujjaman Rifat[4], Nicola Dell[5]
[1] Department of Information Science, Cornell University, Ithaca, NY, USA,
[2]Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh,
[3] Mathematics, Statistics and Computer Science, Marquette University, Milwaukee, WI, USA
[4]Department of Information Science, University of Colorado Boulder, CO, USA
[5]The Jacobs Institute, Cornell Tech, NY, USA
{sa738, nixdell}@cornell.edu, shion.guha@marquette.edu, rashidujjaman.rifat@colorado.edu

ABSTRACT
With the rapid growth of ICT adoption in the Global South, crimes over and through digital technologies have also increased. Consequently, governments have begun to undertake a variety of different surveillance programs, which in turn provoke questions regarding citizens' privacy rights. However, both the concepts of privacy and of citizens' corresponding political rights have not been well-developed in HCI for non-Western contexts. This paper presents findings from a three-month long ethnography and online survey (n=606) conducted in Bangladesh, where the government recently imposed mandatory biometric registration for every mobile phone user. Our analysis surfaces important privacy and safety concerns regarding identity, ownership, and trust, and reveals the cultural and political challenges of imposing biometric registration program in Bangladesh. We also discuss how alternative designs of infrastructure, technology, and policy may better meet stakeholders' competing needs in the Global South.

Author Keywords
Privacy; security; surveillance; HCI4D; ICTD; Bangladesh.

ACM Classification Keywords
K.6.5 Security and Protection; H.1.2 User/Machine Systems

INTRODUCTION
Information and Communication Technologies (ICTs) have often been considered a major vehicle for socioeconomic development in low-resource countries. Today, more than 4.6 billion people around the world have mobile phones, and 52.7% of them browse Internet with their phones [62]. Although mobile technologies have the potential to positively contribute to a range of different development initiatives in the Global South, crimes that make use of these technologies have also become a big concern for these countries. Cybercrimes, including hacking, identity theft, harassment, stalking, and revenge porn, are increasing day by day [35]. At the same time, mobile phones are used by terrorists and other criminal groups to communicate and organize crimes [49]. To combat these crimes, many countries, including Bangladesh, have created surveillance programs that monitor citizens' mobile phone usage [40]. In addition, Bangladesh is the second country in the world (after Pakistan) to deploy nationwide surveillance that relies on citizens' biometric identities: their fingerprints. The collection, storage, and usage of this biometric data has resulted a new set of privacy, security, and safety concerns that are not yet well understood.

The Bangladeshi government initiated this surveillance program in the context of a sudden rise of hate crimes coupled with an alarming rate of terrorism inside and outside the country. The trials of several political leaders for war crimes had created a nation-wide debate [11,57], and caused various political and religious tensions. In addition, militant groups, inter alia, ISIS, JMB, and Ansarullah Bangla announced their violent missions that threatened law and order in the country [8]. Since 2013, extremist groups have killed more than ten progressive writers, bloggers, and publishers in the country [56]. These murders were further punctuated by several violent attacks on religious minorities. When investigating these attacks, the government found that many extremist groups were spreading anti-government news and propaganda, and communicating using the Internet and mobile phones. In August 2013, the government passed an ICT law that enabled them to arrest individuals based on their online activities, which many people considered to be a threat to citizens' freedom of speech [60], and which has since been used to arrest several political activists. In addition to terrorism, other kinds of crimes including political killings, gender violence, corruption, and robbery have also been increasing substantially throughout the country.

Against this backdrop, at a press conference in September 2015, the State Minister of Post and Telecommunication in Bangladesh said, *"We have found that mobile connections*

CHI 2017, May 06 - 11, 2017, Denver, CO, USA

ACM 978-1-4503-4655-9/17/05…$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025961

are the source of all criminal activities like militancy and abduction" [29]. According to the government, in August 2015 more than 130 million of Bangladesh's 160 million people had mobile phone SIM cards, and the Minister announced the launch of a mandatory, nationwide biometric mobile SIM registration program. In 2008, the election commission in Bangladesh created a database of citizens' fingerprints as a part of a project to issue a National ID to every citizen. The new biometric registration program stipulated that mobile phone operators were required to collect the fingerprints of every customer who owned a mobile SIM that connected to their network. This fingerprint data is then sent to the existing database for verification, after which the customer's registration is considered validated. The biometric SIM registration program formally began in December, 2015 [61].

The Minister later explained the objective of biometric SIM registration, "*The biometric verification of the mobile phone SIM has created an opportunity to verify the real owner of the mobile SIM with the information of his own National Identity (NID) and the system would help law enforcement to unearth the real crime perpetrators*" [69]. This statement suggests that the biometric data will enable law enforcement to track down individuals based on their use of mobile phones. However, almost immediately after the launch of the program, it became clear that people were confused and suspicious of the registration process, and protests began to take place across the country. Citizen groups also voiced concerns surrounding the impact that the program had on people's privacy rights [53]. In March 2016, the High Court challenged the legality of biometric SIM registration [63] and, in response, the mobile operators explained that although they were extracting data from people's fingerprints, they were not actually storing the fingerprints themselves. Following this legal challenge, the High Court cleared the way for mobile operators to continue biometric registration of SIM cards [64]. The registration process was scheduled to be completed by April 30, 2016, after which all unregistered SIMs would become non-functional. However, this deadline was subsequently extended for one month since, on the day of the deadline, the majority of SIM cards were still not registered [65].

The main contribution of this paper is to describe findings from a three-month long ethnographic study and online survey that show the tensions, complexities, and challenges surrounding the biometric SIM registration program in Bangladesh. Our findings highlight important nuances in people's conceptual understanding of ownership and identity that further the situated understanding of privacy in Bangladesh. We also show the infrastructural, social, and cultural challenges that impact biometric-based surveillance of mobile phone usage and reveal the political implications of such surveillance for the Bangladeshi people. Taken together, our findings yield valuable new insights that further existing knowledge of digital privacy, safety, and surveillance in the Global South.

RELATED WORK

Privacy, Ownership, and Culture

With the proliferation of computing technologies around the globe, people in all countries are increasingly exposed to risks associated with digital privacy. There have been numerous efforts to understand and mitigate these risks, including password construction and use [14], inferring preferences from social network behavior [24], supporting privacy through design [39], and understanding privacy on mobile devices [48]. However, the majority of these studies focus on the Western world and are based on Western ideas of privacy. In an effort to incorporate other contexts, Nissenbaum [44] argues that notions of privacy change with place, people, culture, and context. Her argument explains why findings of studies done in the West cannot necessarily be extended to non-Western contexts and points out a lack of HCI scholarship investigating privacy outside the West.

Recently, a small amount of HCI research has started looking at privacy in the Global South. Abokhodair et al. [1,2] reported that privacy in the Middle East is dominated by religious practices around intimacy and freedom of speech. Kumaraguru et al. described notions of privacy among Indian populations using communication media [38]. Ahmed et al. reported on notions of privacy in mobile repair markets in Bangladesh [4]. Our work builds on this nascent literature by examining concepts of ownership and identity, two of the core components of privacy [54].

Existing notions of identity and ownership are based primarily on an individualistic Western value system that often conflicts with the values of many collectivist societies in the Global South [26]. Several studies have demonstrated how technologies that are considered to be 'personal' in the West have shared and intermediated usage models in collectivist societies that challenge Western notions of 'personal computing' [13,22,37,46,50]. In addition, the prevalence of informal second-hand markets further complicates the one-to-one relationship between a user and a device [4,6,30,31]. Thus the concepts of identity and ownership often take on a different meaning in the Global South. Our paper contributes to this literature by developing a nuanced understanding of identity and ownership in Bangladesh, and their impact on digital privacy and safety.

Surveillance, Voice, and Democracy

Lyon [41,59] defines surveillance as a "*focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction*". Our focus in this paper is on government-imposed mass surveillance. In recent years, these kind of surveillance programs have focused primarily on monitoring communication media to track suspicious activities. China, Russia, Germany, Australia, the United Kingdom, the United States, India, and many other countries have dedicated projects for eavesdropping on their citizens' Internet traffic and mobile communication [70]. To be effective, many of these programs need to collect and monitor citizens' private

information. Biometric identifiers are one of the most effective ways to uniquely identify a person. For example, fingerprints and retina have been used to track individuals crossing national borders or to register people for citizenship [9]. At least 25 countries in sub-Saharan Africa and South Asia have already held elections that use biometric voter IDs [18]. However, biometric surveillance of mobile phone usage is fairly new. Only Pakistan, Bangladesh, Nigeria, UAE, and a few other countries have recently launched these programs, and there has thus far been little work that seeks to understand their impact.

Regardless of how important surveillance is for national security, from the citizens' point of view these programs can be interpreted as being authoritarian or exploitative [20,23,51,58]. In addition, surveillance programs can be used to diminish political voice [23]. A person develops a political opinion through their social values, observations, readings, discussions, and debates. Surveillance can curtail the freedom with which people are able to share their ideas and opinions and reduce the diversity of public opinion and competing voices [20]. Thus, privacy is considered important in most democratic theories [12,25,42], suggesting that democratic governments need to draw and maintain a line between what data should or should not be collected. In many Western countries, constitutions have also been established that protect certain privacy rights [15]. Similarly, different citizen groups monitor and criticize government surveillance programs [45]. However, many countries in the Global South are struggling to maintain a stable democracy and are embarking on mass surveillance programs with little external oversight.

Aadhar, India's biometric identification project, is one of the most studied biometric identification schemes in the Global South. From the inception of this project, it received harsh criticism from activists who pointed out the potential risks regarding security, privacy, and corruption [21,34,43,47]. Johri et al. reported how Aadhar's narrow focus on data forcefully aligned technology and people and ignored many important broader aspects of identity by "viewing citizens as numbers" [33]. Jacobson reported that the Indian government is more interested in controlling citizens than ensuring their security [32]. Despite these concerns, Aadhar's data has not (yet) been used by the Indian government to track citizens' communications. Our study on the biometric mobile phone registration program in Bangladesh contributes to the growing amount of research that focuses on biometric data and further adds important elements of privacy and security in the context of the Global South.

METHODS

We conducted a three-month ethnographic study in Dhaka, Bangladesh to study the biometric mobile registration program. The first author was born and raised in Dhaka and is a fluent speaker of Bengali. From March to June 2016, he visited 30 biometric registration points in a variety of Dhaka neighborhoods. Although the neighborhoods were chosen based in part on convenience and the ethnographer's familiarity with the area, we ensured that we covered a wide variety of registration points, including formal service centers, local shops, and temporary booths, that serviced a diverse range of people. At each of the registration points, the researcher conducted two hours of observation, resulting in a total of 60 hours of observational data. The researcher also conducted semi-structured interviews with people in charge of the registration points and in situ interviews with customers who were willing to participate in the study. In total, we performed 30 interviews with registration operators and 34 interviews with customers. All interviews were voluntary, roughly 15 minutes long, and audio recorded. Observational data was recorded in the researcher's notebook. We also took over 200 photos during our observations.

The first and second authors (both of whom are Bangladeshi) also visited the homes of 30 families in Dhaka and conducted semi-structured interviews with 52 participants at these homes. We used snowball sampling, starting with a set of families that we knew, and expanding based on suggestions for participants, stopping when we reached theoretical saturation. We tried to visit families from different socioeconomic classes to achieve diverse viewpoints. Ten families were selected from each of low, middle, and high income ranges (low-income is <10,000 Taka/month, middle-income is 10,000-20,000 Taka/month, and high-income is >20,000 Taka/month)[1]. Each of the home visits lasted approximately one hour and discussed the participants' backgrounds, mobile phone use, their experience with the biometric registration process (if any), and their thoughts on the program. Finally, we also posted flyers at three local universities and invited interested students to participant in interviews. A total of 30 students (15 males, 15 females) were recruited through this process. All interviews were voluntary, 10 to 15 minutes long, audio-recorded, and they were conducted in Bengali. All interview data was later translated into English, and transcribed by two different coders, both of whom have bilingual expertise in Bengali and English.

In addition to our ethnographic and interview data, we also conducted an anonymous online survey. The survey was in Bengali and asked questions regarding participants' demographic information, biometric registration, and their opinions about the registration program. Although most of the questions were structured checkboxes or multiple-choice questions, the survey also included an optional open-ended textbox where participants could freely express their opinions, concerns, or suggestions about the biometric SIM registration. The survey was publicized through two public posts on the ethnographer's Facebook page between March

[1] 80 Bangladeshi taka is roughly equivalent to 1.00 USD.

1st and 10th 2016. The survey was left open until April 30, 2016. A total of 606 participants completed the survey.

In total, our ethnography produced 60 hours of observational data and over 150 hours of interview data. The data was separately translated to English by two native Bengali speaking researchers and cross-checked for validation. The translated data was then coded by the team following the Grounded Theory method [16], and labeled with emerging themes. The survey data was processed similarly but separately from the ethnography data.

THE BIOMETRIC REGISTRATION PROCESS

The biometric SIM registration process took place in three main settings: a) formal service centers, b) informal shops, and c) temporary registration booths. We discuss each of these contexts before describing the registration process.

Formal Service Centers

The formal service centers were usually located in shopping malls and were owned and operators by large mobile phone companies. The primary goal of the centers was to provide customer service and assistance to people who were experiencing issues or having trouble with their mobile phone service. Since SIM card registration was not their main function, we found that staff at the service centers would only help people to register their SIM cards if the SIM cards were from the network of that operator.

All of the staff at the service center were highly educated (possessing at least a college degree) and well-trained on the registration process. They were also experienced with technology and capable of using computers, laptops, and tablets. They were dressed in uniforms and communicated with customers in accordance with established rules laid out by their employers. These staff reported that the majority of the customers they served were from middle or upper class communities, with one telling us:

"Everybody knows that these places are for gentlemen. Also, people who come here … they don't want to take risk by going to a roadside shop and doing their registration in a sloppy fashion. They want confirmation from a reliable authority." – (Formal Service Provider, male, 32 years)

The customers at the service centers shared similar views, with one saying, *"Here you don't have to encounter foul people. Also, I don't want to risk my registration, my business is relying on this."* (Businessman, male, 45 years)

Informal Shops

In contrast to the formal service centers, the informal shops were typically local, road-side shops that were frequented by a diverse range of people from a variety of backgrounds. These shops, which included grocery stores, laundromats, hair dressers, pharmacies, and CD/DVD shops, offered SIM card registration service in addition to their usual business. Nine out of the ten shopkeepers that we interviewed had low levels of education, with four completing elementary school and five not finishing elementary school. Only one

Figure 1. A grocery shopkeeper is helping a customer with biometric SIM registration.

shopkeeper was currently studying at a local university for an undergraduate degree in accounting. None of the shopkeepers were familiar with computers or the Internet. However, they all used mobile phones for sending money.

The shops were chosen to be biometric registration points by agents who worked for the mobile phone operators, often based on their existing relationship with the agents or following a previous contract with the operators for mobile-money transfers. The shopkeepers were given the equipment necessary to do the registration and received one day of training at the operator's office. Since the device used to do the registration was different for each operator, a shopkeeper could only register customers for the specific operators that had trained them. The shopkeepers would often post flyers that indicated the operators that they were authorized to serve. For each registration, the shopkeepers would receive 1.80 Taka (approx. 0.01 USD) before tax.

Temporary Registration Booths

Temporary registration booths took a variety of different forms. Some of these booths consisted simply of a colorful umbrella on the side of the road under which a person would sit with a chair and table offering a registration service. Frequently, these booths would be located in a public place, like a road-crossing or the corner of a market. The mobile phone operators employed temporary staff to provide the registration service at these booths, with the length of the employment contract ranging from two to six months. All the staff employed had a minimum of high school education and were trained on registration process by the operators. These temporary booths aimed to serve customers from a variety of socioeconomic backgrounds. The booths would open as early as 7am and stay open until 10pm, with the staff taking only short breaks for meals.

Completing the Registration Process

Completing the registration process would typically take about 10 minutes. Although different mobile phone operators used different equipment for the registration, they were all tablet-based systems. Some operators provided a

separate fingerprint reading device that needed to be connected by wires to the tablet, while others augmented the tablet with fingerprint reading capabilities. Figure 1 shows how a customer providing his fingerprints on a tablet device for biometric SIM registration at an informal grocery shop in Dhaka.

To begin the registration process, the customer had to provide their mobile phone number and national ID document. The registration person would then give the customer a paper form to fill out that required them to provide their name, age, gender, date of birth, etc. The customer filled out the form and gave it to the registration person, who then entered relevant information into an app running on the tablet and set up the fingerprint equipment. Next, the customer had to provide fingerprints of their thumb and index finger of each hand. The device provided a notification that indicated when each fingerprint was successfully captured, prompting the customer to move on to the next fingerprint. After the fingerprints had been captured, the device would send, via text message, a unique passcode to the customer's phone. The customer then needed to enter the passcode into the system (or the registration person would help them to enter the passcode). If the passcode was correct, the registration was complete and the customer would receive confirmation that they had completed the registration process. However, after completing the registration process, the customer had to wait up to two days to know whether the registration was actually successful. During this time, the customer's data was transmitted to a central database and analyzed. The customer would then receive a text message that informed them if the registration was successful.

Although the cost of registration process was borne by the mobile phone operators and was supposed to be free for customers, during the last week of mandatory SIM registration, we found 5 informal and temporary registration centers who were illegally charging customers 20 Taka (0.25 USD) to complete the registration process.

TENSIONS SURROUNDING BIOMETRIC REGISTRATION

This section discusses several major themes, challenges, and complexities associated with the biometric registration process that emerged during our analysis of our data.

Ownership

Our findings reveal that the concept of ownership of the mobile phone and the SIM card was complex and not well-aligned with the 'one SIM card, one owner' model that the registration process assumed. In addition, there were many occasions where tensions surrounding ownership resulted in additional challenges for both customers and registration booth staff. For example, the separate identity of the phone and the SIM card was not clear to many customers. Seven of the people that we talked to at the registration booths said that they had come to register their "mobile phone", which they had bought somewhere else. However, it turned out that their SIM card was already registered to another person that the customer usually did not know. One told us:

"I bought this phone 2 months ago … in exchange for my own money, my hard-earned money. You can ask my fellow rickshaw drivers in the garage about this. They all know I bought this. Now, this registration guy is saying that this is not my phone. Why? Because I am poor?" (Rickshaw driver, male, 40 years).

Another of our interview participants, who worked as a domestic helper, explained how she would always buy phones from other people or from the second-hand mobile phone market. She knew about the difference between the body of the mobile phone and the SIM card, but said that her husband and son did not understand this difference. She had to explain the difference to them before they went for the biometric registration. Moreover, since the SIM card in her mobile phone was not originally registered in her name, she had to buy a new SIM card, which cost her 50 Taka (approx. 0.7 USD). She said, *"I find this a new kind of business by the phone company. All they want is to drink our blood"* (Domestic helper, female, 45 years). It quickly became clear to us that the majority of mobile phone users in Bangladesh depend on the second-hand mobile phone market, where they not only trade their old phone, but also their SIM cards. As a result, associating one's identity with a SIM card is challenging. One of our participants asked us, *"What will happen when I will sell this phone to someone else, and buy a new phone?"* (Night Guard, male, 35 years)

Further tension concerning ownership arose due to the hierarchical power structure of the society, and our findings showed that in many communities the ownership of mobile phones (and SIMs) is determined by power relationships. For example, we encountered nine cases, where the senior male person of a family came to register all the SIMs for his family members in his name. One of these participants said:

"I am the person who earns money and buys things for my family. I am responsible for anything that happens with these phones. So, who else do you think will register the SIMs?" – (Service holder, male, 52 years).

There were six adult members in his family including his wife, three sons, and daughter. Each of them used a separate mobile phone. His elder son even paid for his phone from his own salary. However, all of the phones were 'owned' and registered in the father's name since, as he said, *"As long as they are staying in my family, I am responsible for everything they do."*

Our visits to other local families revealed many similar stories regardless of the socioeconomic status of the families. For example, we encountered five low-income families in which the women did not own their SIM cards and their husbands were in charge of registration. In three other middle-income families, the women identified the registration as the *"men's task"*, while in two more the women did not know who owned the SIM cards. In four

high-income families, the women did not own their SIM cards. In total, we found only one family in which the wife had done her own registration by herself. One senior male member of a middle income family told us:

"When you are a grown up man and you have a family, you need to know what your responsibilities are. Whenever you buy something, that may cause legal trouble at some point, and you may need to run here and there. It is always safe that men take that responsibility"- (Pharmacist, male, 68).

Beyond families, we also encountered issues of ownership in informal business settings. For example, one customer that we spoke to at a registration booth had brought about 70 mobile phones with him, wanting to register all the phones in his name. However, the national rules say that each person can only register a maximum of 20 SIM cards. This scenario resulted in a big discussion between the customer and the registration person. The customer described himself as the owner of a rickshaw garage who had bought the mobile phones for the rickshaw drivers that worked under him. He argued that the registration needed to be in his name because he was the one who had paid for the phones. He further said that he often discharged his workers and needed to keep the phones for the new workers. The registration person argued that the situation could only be handled under "corporate registration" of the garage, which the customer did not have since the garage was his informal family business. Finally, they decided that the customer would bring his wife, brother, and son to the booth the next day and have them register 20 SIM cards each. Similar issues of ownership arose in several other cases, including owners of other informal businesses, leaders of religious institutions, or leaders of local sports teams that wanted to register SIM cards for the people working under them. In general, the power hierarchy associated with these informal organizations was not well aligned with the concept of 'ownership' that the registration process assumed.

Identity and Identification

Another major set of challenges that were revealed by our analysis concerned the concept of identity and the process of identification. For example, the registration system required that the owner of a SIM card identify themselves with a valid ID, which could be their national ID card or passport. However, in several cases we found that people came to the registration booth with the ID of another person, and the registration person had to explain them that they should bring their own ID. One such customer told us:

"I do not remember if I ever had an ID. Some people came to our village before the election and gave us some cards. That happened several years ago. Now I have moved to Dhaka and I do not know where those are." – (Rickshaw Driver, male, 25 years)

Since he did not have his own ID, he brought the ID of his aunt who lived nearby, arguing, *"This is a genuine ID. Why doesn't he use this for registration? I took my aunt's permission. She considers me as her son. What is the problem?"* In addition to this participant, we found 15 other people at different booths who did not have their own IDs. Unable to register these customers, the registration person suggested that they go and talk to their Ward Commissioners[2] to obtain new IDs. However, several people reported that they had already talked to their Ward Commissioners but had failed to get new ID cards since they were not originally registered in their current Wards. Instead, they were told to travel to their villages to collect their new IDs, which they were unable to do at that time of the year. Five people said that they had never received an ID card. All of these stories highlight the challenges associated with requiring that people possess valid ID cards before they are able to register their SIM cards.

A serious challenge associated with the identification and registration process arose when several customers did not have clear lines on their fingerprints. We observed four cases where, even though the registration agents were forcefully pressing the thumbs of the customers against the machine's surface, no fingerprint lines were being captured. At one point, the agent had to apologize to the customers. When we checked the fingers of the customers in question, we found that the lines were not very clearly visible on their fingers. All four of the people that this happened to were day laborers. One explained that he did not have lines on his fingers because he regularly used hard hammers to break bricks. Another said that he burnt his hand working with hot oil. We also found one participant who had lost his thumb in an accident, and the lack of a thumb made it impossible for him to complete the registration.

Finally, we encountered a number of issues associated with identity and gender. For example, many women were concerned that the registration process would allow them to be identified as women. In one of these cases, a woman showed us her earlier registration papers, that had a man's name written on the form that did not match her name on her ID card. She argued that she had preferred to use a male name to avoid being harassed over the phone. She asked, *"Why do I have to tell them if I am a man or a woman? So that they can arrange harassments for me?"* - (University student, female, 23 years). In another case, one woman came with her husband's ID and refused to show her own ID for the SIM registration, saying, *"I do not trust these people with my information."* - (House wife, female, 30 years). Many more of our interview participants reported that the registration booths were operated by male staff members who would need to touch the customers' hands to take their fingerprints. However, the women did not like to be touched by an unknown male person, which prevented many female participants from doing the registration.

[2] Commissioners are elected public representatives in Wards, the smallest administrative units in Bangladeshi cities.

Exploitation

Many of our participants were concerned that the biometric registration system would be used to facilitate exploitation of people by the Government and mobile phone operators. For example, several participants expressed that the justification for the biometric registration process – to enable the Government to track criminal behavior – was a farce. One participant described:

"Do you think police do not know who the criminals are in a neighborhood? Of course, they know! Everybody knows. Even the children of the neighborhood know. But they will never arrest the criminals, because they take bribes from them. And now they have made this excuse of identifying the criminals for taking our fingerprints?!"- (Retired Banker, male, 68 years).

The concern that the system would be used to exploit people was reinforced when many participants were forced to purchase new SIM cards because the SIM cards that they had bought on the second-hand market turned out to already be registered to other people. Moreover, although it was illegal, we found several registration people who were charging customers extra money to perform the registration. When we asked the customers why they paid this extra money, all of them replied that they did it because they felt that they had no other option.

The decision by the informal registration staff to risk punishment by charging extra money for the registration process [68] stemmed in part from the fact that the staff also felt exploited by the system. In particular, the staff felt that the amount of money that they earned from registering people was not sufficient to justify the amount of work that they were doing. The minimum commission that the staff were paid was 1.80 Taka excluding tax (approx. 0.016 USD) for each biometric SIM registration. Since each SIM registration took them approximately 15 minutes, if they worked solidly for 8 hours in a day, they would only be able to register about 33 SIMs for which they would earn a total of about 66 Taka (approx. 0.8 USD), which they claimed was exploitative. In response to these concerns, Bangladesh Tele Recharge and Mobile Banking Business Association held a press conference in April 2016 to present their case for increasing the commission paid for each biometric registration. They stated that they were strictly opposed to the minimum commission paid by mobile phone operators for biometric SIM registration.

Security, Safety, and Resistance

Our analysis also revealed a wide variety of concerns and issues surrounding the safety and security of the biometric SIM registration process. For example, the security of the biometric data relied heavily on the integrity and honesty of the registration staff. However, the registration staff in the informal shops were chosen based on their relationship with the mobile phone operators, which resulted in a potential threat to the system. Although the software that they were using for data entry was not necessarily compromised, a dishonest registration person could run separate software in the background to surreptitiously capture the fingerprint data that could then be used to register duplicate SIM cards in a customer's name without informing them. Although not part of our study, such an incident was reported in June 2016 in Mymensingh, a large city in Bangladesh. A registration person was arrested with two thousand illegal duplicate sims [66]. Similarly, in May 2015 the police arrested two people who had been collecting duplicate copies of other people's SIM cards from retailers, saying that they had lost their original ones [67]. In reality, they had been collecting mobile money sent to those numbers.

In addition to the potential threat posed by the registration staff, many of our participants expressed confusion and suspicion regarding the registration process, and our conversations with participants revealed that this lack of trust was in part due to a scarcity of information that explained the process. Many participants were concerned about where their fingerprint data would be stored and how it might be used in the future. One participant said:

"*Once the Government said that the fingerprints would not be saved anywhere. Now they are saying that they will fine the mobile phone operators if they leak the fingerprints. This means, our fingerprints are being saved somewhere by the mobile phone operators. This is very unfortunate.*" - (Businessman, male, 42)

Another participant was concerned about the technical knowledge of the Government saying:

"I don't think our Government is aware of the technical flaws that may occur. I even don't think that any system is safe to keep those biometric data. Government is overconfident, but they don't even know any of the technical aspects of biometric data collection and its safety. It's undoubtedly a violation of human rights." – (Service holder, female, 38 years)

These suspicions were accompanied by people's fear that their stolen fingerprints could be used to harm them. One participant said, *"If you have somebody's fingerprints, you can basically make papers to grab all their properties."* – (Night Guard, male, 40 years). However, other participants were less concerned about this, with one describing:

"I know that it is possible to snatch away one's properties with their fingerprints, but I am not afraid. Because, I am a poor man and I do not have anything to lose. The rich people should be bothered about this." – (Rickshaw Driver, male, 35 years).

In addition to theft of property, several participants raised concerns regarding their responsibility for whatever their phone might be used for. One housewife explained,

"My husband uses my phone all the time. If he does something wrong, or talks to a criminal over my phone, why should I be responsible for that?" - (Housewife, 55 years).

A local rickshaw garage owner expressed a similar fear concerning the phones that he provided to his drivers,

"Look, I give my phones to the rickshaw drivers so that they can communicate with me while they are out to work. How do I know why else they are using those phones? Now, if police arrest me for that, is this a justice?" – (Rickshaw Garage owner, male, 40 years)

A total of seven participants reported that they did not feel comfortable sharing their personal data with the government, and felt pressured to do so, with one saying,

"*I feel pressurized to share my personal information, because if I don't give away my biometric data, I have to stop using mobile phones."* (Student, male, 22 years)

Another participant called the program a breach of privacy saying, "*Why do I have to tell them everything anyway? Then where is my privacy?*" (Housewife, female, 40 years)

In general, the security concerns, suspicions, and fears associated with the process often led people to resist the requirement to participate in the biometric registration system. Ten of our participants said that they would not register their SIM, believing that the project would finally fail. Eleven participants said they would wait until the end of the deadline to see what happened to other people who did not register. They all believed that it would be impossible for the Government to register all mobile phone users in Bangladesh, and hoped that the project would fail so that they would not have to register their information.

FINDINGS FROM THE ONLINE SURVEY

Our online survey was designed specifically to further the understanding of our ethnographic findings. Our anonymous online survey asked participants about their demographic data and whether they supported the biometric SIM registration [71]. In addition, we provided an optional, open-ended comment box that enabled participants to share their opinions. We received 606 survey responses, from which a number of themes arose.

First, the majority (77%) of our survey participants said that they did not like the biometric SIM registration system. Only 15% supported the program and 4% said that they did not care (the rest preferred not to comment). The survey asked participants why they were dissatisfied with the biometric registration, and three answers stood out. 62% participants said they were not happy with the biometric registration because they believed that they were going to lose their personal security through this process. 55% participants said that they did not like the fact that they were being forced to give away their fingerprints. 15% thought the system could probably improve national security, but they still did not like the process of registration. Out of our 606 survey responses, 172 participants chose to use the open-ended comment box to tell us their personal opinions regarding biometric registration. We summarize the main findings from these responses below.

Support for the Biometric Registration System

A total of 36 people (20.9% of comments in the open-ended box) said that they supported the biometric registration program. They acknowledged the infrastructural challenges associated with implementing the program, but said that such systems were necessary to reduce crime. One participant wrote:

"*If you go to USA, you don't mind giving your fingerprints to the embassy, but here you don't want to give those to your own Government. This is hypocrisy.*" – (Businessman, male, 30 years).

Another participant said, "*The Government already has our fingerprints. We gave those to them when they made the voter registration cards. If they wanted to do any harm to us, they could do that by now.*" - (Student, female, 22 years).

Some people who supported the registration process not only defended the biometric registration system, but also attacked the people who were protesting the program. For example, one comment said,

"*Some people do not like the Government, and they will protest any Government initiative. To be honest, only the people who do illegal things will be concerned of such a surveillance system.*" – (Software engineer, male, 32 years).

Concern about Government or Political Exploitation

Of the 172 comments that we received, 73 (42.4%) did not support the biometric registration system because they thought that the Government would exploit this system later for their own political interest. One participant connected biometric surveillance with the Section 57 of ICT Law that the Bangladesh Government had imposed a few years ago, to control people's online behavior. According to the rule, the Government has the power to punish a citizen for their online activities if they are deemed to be threatening to the Government, and the Government have arrested a number of political activists in last few years through that rule [27]. The participant wrote:

"*The Government just does not want us to criticize them. The ICT law suppressed our voice online, and now this biometric surveillance will suppress our voice even over day-to-day communication. We are slowly moving to a police state.*" – (University professor, male, 54).

Many other participants also expressed fear that the system could be used for political exploitation. Some participants believed that the Government would be able to listen to their conversations and track who they talked to, saying:

"Now you have to be careful whenever you talk to somebody through your mobile phone. Because if the (Government) don't like him, you are going to jail." – (University student, male, 23 years).

Another participant pointed out that even if the current Government did not exploit the system, future Governments would still be able to do so:

"Even if this Government is so good that they are not going to exploit this information, how do you know the next Government will not do that? This system is going to exist forever. The Government has just given birth to a monster." – (University professor, male, 42 years)

Exploitation by the Mobile Phone Operators

Of the 172 comments that we received, 28 (16.3%) said that they did not like the biometric registration process because the mobile phone operators would be able to obtain and keep their fingerprint data. One participant wrote,

"What is the point of giving our fingerprints to some commercial company? So that they can make a business out of those?"- (Housewife, female, 31 years).

Other participants mentioned how their fingerprints could be potentially be exploited for profit-making purposes and described how companies would be able to exercise power over them by having their fingerprint data. Eight participants were further concerned because five out of six mobile phone operators in Bangladesh were actually foreign companies, with one participant commenting,

"This means we are basically selling our fingerprints to other nations. No sane person can support this." (Software engineer, male, 30 years)

Concerns about Privacy Rights

Finally, 41 out of our 172 comments (23.8%) did not like the biometric registration system because they thought that it was violating their right to privacy. Participants in this group described how they viewed their fingerprints as their personal property, that the Government had no right to force them to give that away. Several participants expressed grief, frustration, and fear regarding this issue. One participant wrote, *"This is my fingerprint, and I do not want to give this to anyone. This is my right"* (College student, female, 20 years). Another participant said, *"I am just not comfortable sharing my personal information with some people I do not know. I don't want to hear whether they are good or bad, I just don't like this."* -(Businessman, male, 54 years). Several participants also did not like the fact that they were being forced to participate in the process. One of them said, *"I just don't like to be forced. Is this why we live in an independent country?"* - (Banker, male, 38 years).

DISCUSSION

The sections above present a qualitative analysis of our ethnographic findings and key observations from our online survey. In addition to developing a rich, field-level understanding regarding the implementation of the biometric SIM registration program in Bangladesh, our ethnography has demonstrated how the local and situated values and practices around ownership, identity, exploitation, and security and safety concerns challenged the biometric registration program. Furthermore, our online survey revealed substantial dissatisfaction with the biometric SIM registration process. Our participants expressed their fear of political exploitation, commercial use, and invasion into their privacy. These findings help us conceptualize some of the core challenges associated with imposing a biometric surveillance in Bangladesh.

However, before synthesizing our findings into a set of key takeaways, we want to acknowledge that there are a number of limitations to our study. The biometric SIM registration program is a nation-wide campaign in Bangladesh, and our research only reveals a subset of the challenges encountered in part of the capital city, Dhaka. The registration points and the families that were studied were chosen based on convenience and participant availability. Hence, the findings of our study should not be generalized over the entire country. Instead, our study relies on the strength of ethnography that, instead of capturing a general picture, reveals rich nuances and a deep understanding of situated practices. In addition, the participants in our online survey represent only a small portion of the Bangladeshi population, and those that have Internet access. As such, the survey should be viewed as collecting data to validate findings from our ethnography and to accumulate a diverse set of opinions. Combining two different kinds of data (ethnography and an online survey) was also a methodological challenge that we confronted in this study. However, we decided that both kinds of data were important in explicating the nuances associated with the biometric registration program. Despite these limitations, our research offers several key insights and takeaways that will be beneficial for the HCI community at large.

First, the core idea of biometric SIM registration was based on an assumption of individual ownership and personal use of mobile phones, which conflicted with local practices in several ways. Our ethnography revealed how mobile SIM cards frequently changed owners over time without any formal records, how the ownership of a phone in a family or a group was dominated by power relationships rather than use, and how a single device was shared among multiple people in a variety of settings. Those practices not only complicated the process of biometric SIM registration, but also challenged its main objective: that the person who 'owns' a SIM is responsible for its use. Furthermore, the mismatch between the assumptions of the registration system and local practices also created fear among the people who were being forced to register their SIM cards. Our findings suggest that a more successful registration model might focus more on actual use of the SIM card rather than relying on ownership of a SIM.

Second, the success of creating and implementing a surveillance system like Bangladesh's biometric registration program largely depends on having a functioning and robust infrastructure that is difficult to guarantee in a developing country. As we have seen in our

ethnography, the informal registration points were vulnerable to data leaking, corruption, and exploitation. There were gender and economic concerns that affected the success of the registration system. In light of these concerns, we observe that securely collecting, transmitting, and storing large amounts of sensitive biometric data requires infrastructural strength that may quickly become a burden for a Government in a low-resource country. The complications that arose during the implementation of the biometric registration system suggest that biometric surveillance is resource-hungry, and without having proper infrastructural support, launching such a program should not be recommended.

Third, the success of a surveillance program may be heavily dependent on the extent to which people trust the entity responsible for the surveillance. Our ethnography and online survey both demonstrate that many people were suspicious of the motives of the Government and mobile phone operators. Although people's political beliefs undoubtedly shape part of this suspicion, it is undeniable that such a surveillance tool provides the Government with substantial power that could be used to exploit people. Many developing countries suffer from poor governance, and such surveillance tools have the potential to make the situation worse. We suggest that any action based on surveillance be made transparent to the country's citizens, so that the government cannot lie or misuse people's data. This would require that every access to the biometric database be publicly logged and justified. At the same time, an autonomous and unbiased civil society needs to be developed that will monitor and sanction access to the biometric database.

Beyond these implementation-level challenges, there are also several broader lessons from this study that are important to HCI scholarship in the "developing world". The growing enthusiasm for ICT-based "development" programs around the globe often ignores the potential negative consequences of introducing ICTs in low-resource settings. However, the prevalence of ICT-based crimes has already been a big concern for many countries, including Bangladesh, and these countries are now taking steps launch costly monitoring and surveillance systems that, due to technical, cultural, and infrastructural challenges, are likely to fail. Although we are not advocating that ICT-based solutions in these countries be discouraged, we do highlight the need for carefully considered policies, laws, and robust security infrastructure before embarking on large-scale, public ICT initiatives. Although recent HCI scholarship has critically analyzed ICT-based development programs through the lenses of postcolonial computing [28], residuality [7,52], and sustainability [17], we suggest that HCI and ICTD scholars consider the issues of infrastructural breakdown, and potentially negative consequences as important aspects for evaluating technology in development contexts. At the same time, our study highlights a need for innovations in low-cost technologies to fight ICT-based crimes in the Global South.

Another key issue that our work raises is the need for notions of privacy that better fit the contexts, values, and local practices that are prevalent in the Global South. Our data shows that the situated idea of privacy among participants often made them resist the biometric registration program. However, the origin, nature, and characteristics of privacy in the Bangladeshi context has not been studied enough to explicate this resistance. The challenges in aligning the Western notion of privacy with notions of shared use, complex ownership, and communal identity, as reported in this paper, demonstrate the dearth of knowledge in this area. With the rapid adoption of technologies worldwide, people of different cultures are exposed to technologies that are embedded with Western privacy values [19] and this issue is becoming increasingly important. Our study reveals tensions between the shared use of mobile phones and individual privacy, and between ownership and gender – both of which are culturally constructed but technology mediated. Several studies on technology and gender in the Global South have shown how the relationship between technology and women is affected by the male-dominated cultural norms [3,5,36]. However, we know little about their impact on the notion of privacy and implications for biometric identification. Hence, the gender, power, and economic dynamics that we reveal in this paper open a new space in which HCI designers can create mechanisms that preserve privacy in contexts outside the West.

Finally, our analysis reveals a tension between notions of voice and surveillance in Bangladesh. The historical conflict between surveillance and privacy in the Western world has been shaped by laws that preserve an individual's privacy rights [10,41,55,59]. However, many countries in the Global South, including Bangladesh, do not have these privacy rights protected by their constitutions. As a result, enactment of a surveillance law carries the risk of suppressing individuals' voices, and may eventually destroy the democratic environment in a country. Hence, an individual's right to privacy is inevitably associated with the democratic development of a country. This broad conceptualization of privacy allows us to perceive how the design of different privacy features in our day-to-day devices actually "function" in the Western world because of the stable democratic environment. However, when the devices leave these stable environments, a whole new set of designs and policies are required to understand "privacy" in different scenarios. As a result, in addition to understanding privacy as it relates to different social and cultural norms, it also needs to be studied in a diverse range of political environments and settings.

REFERENCES

1. Norah Abokhodair. 2015. Transmigrant Saudi Arabian Youth and Social Media: Privacy, Intimacy and

Freedom of Expression. 187–190. Retrieved from http://dx.doi.org/10.1145/2702613.2702629
2. Norah Abokhodair and Sarah Vieweg. 2016. Privacy & Social Media in the Context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems.*, 672–683. Retrieved from http://dx.doi.org/10.1145/2901790.2901873
3. Syed Ishtiaque Ahmed, Nova Ahmed, Faheem Hussain, and Neha Kumar. 2016. Computing beyond gender-imposed limits. In *In Proc. LIMITS'16*, Article No. 6.
4. Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Md. Foysal Hossain, and Nicola Dell. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *In Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, Article No. 11. Retrieved from http://dx.doi.org/10.1145/2909609.2909661
5. 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 *In Proc. CHI'14*, 2695–2704.
6. Syed Ishtiaque Ahmed, Steven J Jackson, and Md. Rashidujjaman Rifat. 2015. Learning to fix: knowledge, collaboration and mobile phone repair in Dhaka, Bangladesh. In *In Proc. ICTD'15*, 4:1-4:10.
7. Syed Ishtiaque Ahmed, Nusrat Jahan Mim, and Steven J Jackson. 2015. Residual Mobilities: Infrastructural Displacement and Post-Colonial Computing in Bangladesh. In *In Proc. CHI'15*, 437–446.
8. Joseph Allchin. *The Rise of Extremism in Bangladesh*. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/bangladesh/2016-06-09/rise-extremism-bangladesh
9. Louise Amoore. 2006. Biometric borders: Governing mobilities in the war on terror. *Political geography* 25, 3: 336–351.
10. George J Annas. 2003. HIPAA regulations-a new era of medical-record privacy? *New England Journal of Medicine* 138, 15: 1486–1490.
11. BBC News. *Bangladesh war crimes trial: Key accused*. Retrieved from http://www.bbc.com/news/world-asia-20970123
12. Seyla Benhabib. 2002. *The claims of culture: Equality and diversity in the global era*. Princeton University Press.
13. Jenna Burrell. 2010. Evaluating Shared Access: social equality and the circulation of mobile phones in rural Uganda. *Journal of Computer Mediated Communication* 15, 2: 230–250.
14. Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *In Proc. Computer Security-ESORICS*, 359–374.
15. Julie E. Cohen. What privacy is for. *Harvard Law Review* 125: 1904.
16. Juliet Corbin and Anselm Strauss. 1994. Grounded theory methodology. *Handbook of qualitative research*: 273–285.
17. Carl DiSalvo, Phoebe Sengers, and Hrönn Brynjarsdóttir. 2010. Mapping the landscape of sustainable HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1975–1984.
18. Kevin P. Donovan and Aaron K. Martin. 2014. The rise of African SIM registration: The emerging dynamics of regulatory change. *First Monday* Speccial Issue. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820
19. Mary Flanagan, Daniel C. Howe, and Helen Nissenbaum. 2008. Embodying Values in Technology: Theory and Practice. In *Information Technology and Moral Philosophy*, John Weckert (ed.). Cambridge University Press, 322–353. Retrieved from http://www.nyu.edu/projects/nissenbaum/papers/Flanagan,%20Howe%20&%20Nissenbaum%20-%20Embodying%20Values.pdf
20. Michel Foucault. 1977. *Discipline and punish: The birth of the prison*. Vintage.
21. Mehboob Geelani. 2011. Numbers and NREGA. *The Caravan*.
22. Koushik Ghosh, Tapan S Parikh, and Apala Lahiri Chavan. 2003. Design considerations for a financial management system for rural, semi-literate users. In *In Proc CHI EA'03*, 824–825.
23. Henry A Giroux. 2015. Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies* 29, 2: 108–140.
24. Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71–80.
25. Jürgen Habermas. 1991. *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. MIT Press.
26. Geert Hofstede. 1984. The cultural relativity of the quality of life concept. *Academy of Management Review* 9, 3: 389–398.
27. Faheem Hussain and Mashiat Mostafa. 2016. Digital Contradictions in Bangladesh: Encouragement and Deterrence of Citizen Engagement via ICTs. *Information Technologies & International Development* 12, 2: 47.
28. 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*, 1311–1320.
29. Muhammad Zahidul Islam. 2015. *SIM re-registration a must in Bangladesh*. The Daily Star. Retrieved from

http://www.thedailystar.net/frontpage/sim-re-registration-must-139189
30. Steven J Jackson, Syed Ishtiaque Ahmed, and Md. Rashidujjaman Rifat. 2014. Learning, innovation, and sustainability among mobile phone repairers in Dhaka, Bangladesh. In *In Proc. DIS'14*, 905–914.
31. Steven J Jackson, Alex Pompe, and Gabriel Krieshok. 2012. Repair worlds: maintenance, repair, and ICT for development in rural Namibia. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, 107–116.
32. Elida KU Jacobsen. 2012. Unique Identification: Inclusion and surveillance in the Indian biometric assemblage. *Security Dialogue* 43, 5: 457–474.
33. Aditya Johri and Janaki Srinivasan. 2014. The role of data in aligning the "unique identity"infrastructure in India. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, 697–709.
34. Reetika Khera. 2011. The UID Project and Welfare Schemes. *Economic and Political Weekly* XLVI, 9.
35. Nir Kshetri. 2015. Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management* 18, 4: 245–249.
36. Neha Kumar. 2015. The gender-technology divide or perceptions of non-use. *First Monday* 20, 11.
37. Neha Kumar and Tapan Parikh. 2013. Mobiles, music, and materiality. In *In Proc. CHI'13*, 2863–2872.
38. Ponnurangam Kumaraguru and Lorrie F Cranor. 2006. Privacy in India: Attitudes and awareness. *Privacy Enhancing Technologies*: 243–258.
39. Heather R Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer, and Jason Watson. Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. In *In Computational Science and Engineering, 2009. CSE'09. International Conference*, 985–989.
40. David Lyon. 2003. Technology vs "terrorism": circuits of city surveillance since September 11th. *International Journal of Urban and Regional Research* 27, 3: 666–678.
41. David Lyon. 2007. *Surveillance studies: An overview*. Polity.
42. Jane Mansbridge. 1983. *Beyond adversary democracy*. University of Chicago Press.
43. Arindam Mukherjee. 2011. *Aadhar, A Few Basic Issues*. Outlook.
44. Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash L. Rev* 79, 119.
45. Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press. Retrieved from https://mitpress.mit.edu/books/obfuscation
46. Nimmi Rangaswamy and Sumitra Nair. 2010. The mobile phone store ecology in a Mumbai slum community: Hybrid networks for enterprise. *Information technologies & international development* 6, 3: pp–51.
47. Aruna Roy. 2011. *Aadhaar Bound to Fail*. The Hindu, Kochi Edition.
48. Norman Sadeh, Jason Hong, Lorrie F Cranor, Ian Fette, Patrick Kelley, Madhu Prabakar, and Jinghai Rao. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* 13, 6: 401–412.
49. Yasar Guneri Sahin and Tuncay Ercan. 2008. Detection of hidden hostile/terrorist groups in harsh territories by using animals as mobile biological sensors. *Sensors* 8, 7: 4365–4383.
50. Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated technology use in developing communities. In *In Proc. CHI'10*, 2583–2592.
51. Daniel J. Solove. 2011. Why privacy matters even if you have "nothing to hide." *Chronicle of Higher Education* 15. Retrieved from http://www.chronicle.com/article/Why-Privacy-Matters-Even-if/127461
52. Susan Leigh Star and Geoffrey C Bowker. 2007. Enacting silence: Residual categories as a challenge for ethics, information systems, and communication. *Ethics and Information Technology* 9, 4: 273–280.
53. Arifuzzaman Tuhin. 2016. Fear around filgerprints for SIM registration. *NTV Opinions*. Retrieved from http://www.ntvbd.com/opinion/39175/%E0%A6%B8%E0%A6%BF%E0%A6%AE-%E0%A6%A8%E0%A6%BF%E0%A6%AC%E0%A6%A8%E0%A7%8D%E0%A6%A7%E0%A6%A8%E0%A7%87-%E0%A6%86%E0%A6%99%E0%A7%81%E0%A6%B2%E0%A7%87%E0%A6%B0-%E0%A6%9B%E0%A6%BE%E0%A6%AA-%E0%A6%A8%E0%A6%BF%E0%A7%9F%E0%A7%87-%E0%A6%AD%E0%A7%9F
54. Samuel D Warren and Louis D Brandeis. 1890. The right to privacy. *Harvard Law Review*: 193–220.
55. Alan F Westin. 1968. Privacy and Freedom. *Washington and Lee Law Review* 25, 1: 166.
56. Wikipedia Aricle. *Attacks by Islamic extremists in Bangladesh*. Retrieved from https://en.wikipedia.org/wiki/Attacks_by_Islamic_extremists_in_Bangladesh
57. Wikipedia Article. *International Crimes Tribunal (Bangladesh)*. Retrieved from https://en.wikipedia.org/wiki/International_Crimes_Tribunal_(Bangladesh)
58. David Murakami Wood. 2007. Beyond the Panopticon? Foucault and surveillance studies. *Space, knowledge and power: Foucault and geography*: 245–263.
59. Bauman Zygmunt and David Lyon. 2013. *Liquid Surveillance: A Conversation*. John Wiley & Sons.
60. 2013. *Bangladesh's ICT Act Stoops to New Lows*. Global Voices. Retrieved from https://advox.globalvoices.org/2013/09/18/bangladeshs-ict-act-stoops-to-new-lows/

61. 2015. *Trial biometric SIM registration begins Wednesday*. Dhaka Tribune. Retrieved from http://www.dhakatribune.com/bangladesh/2015/oct/20/trial-biometric-sim-registration-begins-wednesday
62. 2016. Statistics and facts on mobile internet usage. *Statista: The Statistical Portal*. Retrieved from https://www.statista.com/topics/779/mobile-internet/
63. 2016. *HC questions legality of biometric SIM registration*. The Daily Star. Retrieved from http://www.thedailystar.net/country/hc-questions-legality-biometric-sim-registration-791002
64. 2016. *HC okays biometric SIM registration*. The Daily Star. Retrieved from http://www.thedailystar.net/country/hc-okays-biometric-registration-sim-1208071
65. 2016. *Deadline for biometric re-registration of SIM cards extended by a month*. bdnews24.com. Retrieved from http://bdnews24.com/bangladesh/2016/04/30/deadline-for-biometric-re-registration-of-sim-cards-extended-by-a-month
66. 2016. *"Biometrically registered Robi SIMs" used in fraud, money stolen from bKash accounts: Chittagong police*. bdnews24.com. Retrieved from http://bdnews24.com/bangladesh/2016/05/23/biometrically-registered-robi-sims-used-in-fraud-money-stolen-from-bkash-accounts-chittagong-police
67. 2016. *Retailers bio-metrically registering SIMs without users' knowledge: BTRC*. The Daily Ittefaq. Retrieved from http://www.clickittefaq.com/retailers-bio-metrically-registering-sims-without-users-knowledge-btrc/
68. 2016. *BIOMETRIC SIM REGISTRATION : Retailers to face punishment for fee collection*. New Age. Retrieved from http://newagebd.net/197633/biometric-sim-registration-retailers-to-face-punishment-for-fee-collection/
69. *"Biometric SIM registration to help identify criminals."* The Daily Samakal. Retrieved from http://www.samakal.net/2016/05/02/5392
70. Mass Surveillance. *Wikipedia Article*. Retrieved from https://en.wikipedia.org/wiki/Mass_surveillance
71. *Online Survey on Biometric SIM registration in Bangladesh*. Retrieved from https://docs.google.com/a/csebuet.org/forms/d/1H3EhWnmAS1tgbrFKNYilpqNH4RaNtwMCqFp7CDeXpq8/edit?usp=drive_web