2017

Privacy Vulnerabilities in the Practices of Repairing Broken Digital Artifacts in Bangladesh

syed Ishtiaque Ahmed
University of Toronto

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

Mohammad Rashidujjaman Rifat
University of Colorado Boulder

Faysal Hossain Shezan
University of Virginia

Nicola Dell
Cornell Tech

Research Article

Privacy Vulnerabilities in the Practices of Repairing Broken Digital Artifacts in Bangladesh

Syed Ishtiaque Ahmed

University of Toronto, Canada

Shion Guha

Marquette University, USA

Mohammad Rashidujjaman Rifat

University of Colorado Boulder, USA

Faysal Hossain Shezan

University of Virginia, USA

Nicola Dell

Cornell Tech, USA

Abstract

This article presents a study on the privacy concerns associated with the practice of repairing broken digital objects in Bangladesh. Historically, repair of old or broken technologies has received less attention in ICTD scholarship than design, development, or use. As a result, the potential privacy risks associated with repair practices have remained mostly unaddressed. This article describes our three-month ethnographic study that took place at 10 major repair sites in Dhaka, Bangladesh. We show a variety of ways in which the privacy of an individual's personal data may be compromised during the repair process. We also examine people's perceptions around privacy during repair, and its connections with their broader social and cultural values. Finally, we discuss the challenges and opportunities for future research to strengthen the repair ecosystem in developing countries. Taken together, our findings contribute to the growing discourse around post-use cycles of technology.

Introduction

Privacy and computing have been entwined since the inception of computing. For instance, appropriate and rigorous security has been seen as the optimal approach to securing private data and computing systems (Mao, 2003). Initially, this was formulated as a mathematical and engineering problem (Shannon, 2001) and, indeed, cryptographic and other security-based approaches are still popular (Diffie & Hellman, 1976). However, a few decades ago there was a subtle shift away from pure engineering solutions toward a more human-centered approach (Zurco & Simson, 1996). This nascent field of study has at times been called "usable privacy and security" (Cranor & Garfinkel, 2004) and is considered to be at the intersection of computer science,

To cite this article: Ahmed, S. I., Guha, S., Rifat, M. R., Shezan, F. H., & Dell, N. (2017). Privacy vulnerabilities in the practices of repairing broken digital artifacts in Bangladesh. *Information Technologies & International Development* (Special Section)*, 13,* 186–199.

privacy and security, and human-computer interaction (HCI). There have been numerous human-centered studies that aimed to understand privacy in computing, including understanding password construction and use (Chiasson, van Oorschot, & Biddle, 2007), text password alternatives (Chiasson et al., 2007), inferences about privacy preferences from social network behavior and use (Gross & Acquisti, 2005), design recommendations for supporting privacy (Lipford, Hull, Latulipe, Besmer, & Watson, 2009), as well as privacy in mobile computing and other similar systems (Sadeh et al., 2009). However, these studies have primarily been conducted in the Western world and are based on Western ideas of privacy. Since the concept of privacy may vary substantially across cultures, times, and places, much of this existing research is not applicable to developing countries. One notable exception is work by Kumaraguru and his colleagues that recognizes this gap and examines notions of privacy in the Indian subcontinent (Kumaraguru & Cranor, 2006).

In addition, although a growing amount of research in and around computing technologies is generally furthering the agenda of privacy preservation, little attention has been paid to the tensions or privacy challenges that arise when technologies break. Breakdown, maintenance, and repair are inescapable features of the computing technologies we interact with, and people's privacy may become vulnerable during these post-use moments. Our work contributes to a growing body of research that focuses broadly on how maintenance and repair practices constitute a novel platform for development through ICTs in low-income countries (Ahmed, Jackson, & Rifat, 2015; Jackson, Ahmed, & Rifat, 2014; Jackson, Pompe, & Krieshok, 2011). However, to the best of our knowledge, ours is the first article to focus on the challenges and issues surrounding privacy during repair in a non-Western setting.

Our article makes the following contributions. First, we present findings from a three-month ethnographic study conducted at 10 major electronic repair sites in Dhaka, Bangladesh. We focus on understanding the repair process from the point of view of multiple stakeholders, including repairers, apprentices, and customers, and we present several vignettes that highlight privacy concerns and challenges associated with repair. Following this, we present findings from an online survey that sheds light on people's perceptions and prior experiences regarding privacy during repair. We then describe findings from the development and deployment of a mobile application, *Protiraksha,* that we created to explore people's reactions to a software tool that reports if their privacy has been violated during the repair process. Findings from our deployment highlight the connections of the privacy issues with the local law and policy, skepticism regarding a technical solution, and the role of cultural, religious, and social values in privacy practices.

Related Work

A rich body of scholarly work has pointed out the necessity to consider repair as a research topic in the study of computing technologies. For example, Lucy Suchman's *Human-Machine Reconfigurations* demonstrates that machines designed to perform certain tasks fail when they experience uncertain or unexpected conditions, and the situated practice of maintenance and repair becomes necessary (Suchman, 2007). Julian Orr's work, *Talking About the Machine,* has further advanced the argument in support of repair. Orr studied how repair workers at Xerox learned repair techniques from their seniors through informal conversations (Orr, 1996). They helped position repair as an important concern in the study of computing technologies. Lately, a growing body of work in HCI and computer-supported collaborative work has started to emphasize the importance of repair and maintenance. For example, Jackson et al. conducted ethnography with electronic repairers in Namibia and found that local repair practices are connected with the global network of knowledge and materials (Jackson et al., 2011). Houston has studied the innovative technical practices associated with repairing mobile phones in Kampala, Uganda (Houston, 2014). Jackson et al. have reported on their ethnography in Dhaka, studying mobile phone repair communities, revealing that the art and craft involved in repair work are often unrecognized in mainstream ICT research (Jackson et al., 2014). Ahmed et al. have also studied repairer communities in Dhaka, documenting different kinds of explicit, tacit, and social knowledges essential to repairing (Ahmed et al., 2015). These ethnographic studies show how the nature of repair is embedded in the socioeconomic fabric of a place, and repair has the potential to play an important role both in strengthening the knowledge around technology and in contributing to national development. Jackson's essay, "Rethinking Repair," depicts a broad picture of repair and its connection with our conceptualization of infrastructure in general (Jackson,

2013). This essay puts forth the experiences around breakdown and repair, and how infrastructures are conceptualized and organized against the constant threat of breakdown. Moreover, scholars have connected repair with global development in other ways. For example, some have depicted repair as a response to postcolonial computing (Irani, Vertesi, Dourish, Philip, & Grinter, 2010), pointing out that technology transfer from the developed western world to developing countries has economic, cultural, and political aspects that may be detrimental to a country's development. Others have seen repair as a tool for sustainable digital consumption that helps reduce electronic wastes (DiSalvo, Sengers, & Brynjarsdóttir, 2010).

Privacy and Repair

Research that examines the relationship between privacy and repair is notably absent in current literature. In a broad sense, privacy during repair communities can be thought of as a transactional and submission process (Nissenbaum, 2004), where a specific commodity or information type is relinquished to a specialized agent for a particular kind of labor or advice. The tensions between privacy and repair are understudied, even in the Western world. It is common for formal service centers to operate according to predefined policies that do not directly address the privacy issue, but that perhaps reduce the motives for repairers to delve into users' private information. However, if a privacy breach occurs, either intentionally or unintentionally, there is currently no effective legal framework in place for how to deal with the breach. For example, a number of recent incidents spurred debates regarding what should happen when the repairer "accidentally" discovers illegal content on a customer's computer or mobile device (CTV News, 2015). In addition, a number of encryption methods have been introduced by computer companies to protect data with passwords that are often intended to protect data privacy even after an electronic object breaks down (Microsoft, n.d.). However, in cases where the repairer needs the password or other essentials to fix a problem, those strategies often do not work.

There are other spheres of life where similar agreements hold true and where there are already precedents in policy and law for preserving the privacy of agents. For example, confidentiality laws protect communication between doctors and patients in medicine. In the United States, medical advice and information are regarded as private and are protected by HIPAA (Health Insurance Portability and Accountability Act) laws (Annas, 2003), which provide standards, conditions, and legislative redress mechanisms for violations of patient data exchange. Similarly, in civil and criminal law, attorney-client discussions are considered privileged and cannot be disclosed to the public except in highly circumscribed situations (Raleigh, 1988). In the realm of higher education, FERPA (Family Educational Rights and Privacy Act; O'Donnell, 2002) manages and protects students' education records, which are respected as private information by U.S. law. However, there are no such protections afforded to repairer-user negotiations. Prior research in usable privacy has shown that not only are people concerned about mobile data privacy (Sadeh et al., 2009), but that they feel embarrassed, deceived, and regretful after disclosures or violations of mobile phone data, which has been shown to have an impact on users' mental and social health (Sadeh et al., 2009). Hence, we argue that this issue is relevant, understudied, and ripe for further investigation in the context of repairing electronic devices.

Privacy and Development

Although some prior work relates the idea of privacy to the liberal definition of development (Westin, 1968), we have found no direct relationship between general development theory and privacy discourse in information technologies. In this article, we draw two separate connections between privacy in broken technologies and development. First, we build connections between ICTD (information and communication technologies for development) and privacy. To this end, we turn to Nobel laureate economist Amartya Sen, who has defined *development* as "freedom"—achieved through both instrumental and constitutive means (Sen, 1999). As seen in other studies, lack of privacy often discourages people from using a technology, thus affecting their instrumental freedom. At the same time, the issue of privacy also has a constitutive aspect. A person, being a part of a society and culture, develops their own definition of privacy that must be nurtured and protected by that society. Without support from the society about "self," "ownership," and "security," a person may not achieve the constitutive capability to obtain their freedom. In addition to this conceptualization, privacy is also a democratic right that is essential to protect a citizen's voice. Without assuring citizens' privacy, democratic development is impossible (Ahmed, Hoque, Guha, Rifat, & Dell, 2017; Raab, 1997).

Second, Ahmed et al. have suggested that repair can be considered a potential and novel venue for

sustainable development (Ahmed et al., 2015). Their argument was based on the optimism around building a repair and recycling infrastructure in parts of the world that are not usually the developers of computing technologies. We argue that such repair infrastructure cannot be imagined without securing the privacy of data stored in broken and discarded devices. If repair services remain insecure and unreliable in those places, many users may prefer not going there—resulting in a failure of the attempt to expand a practice that offers an extended longevity of electronic devices and, thus, an overall reduction in electronic production and, in turn, electronic waste. Hence, we argue that understanding and addressing privacy issues in repair constitute an important research agenda for ICTD. Our work contributes to this important, yet often ignored, area of research by reporting empirical evidence from Bangladesh.

Methods

Our study was conducted in Dhaka, the capital of Bangladesh. Our investigations into repair and privacy were conducted in three phases between June 2013 and May 2015. In the first phase, we conducted a three-month ethnographic study in Dhaka to understand the practice of repairing mobile phones from the repairer community's point of view. From June to September 2013, we visited 10 major electronic repair sites in Dhaka. In addition, during this period, one researcher on our team learned to repair mobile phones from a senior repairer. Following this, that researcher worked for three weeks in another repair shop as an apprentice. This allowed him to become deeply engaged with the repairer community and to learn their norms and values. While working as an apprentice, he also conducted semiformal interviews with the individual repairers working in standalone workshops or as a part of a group in a large workshop, including senior repairers who owned their own businesses, apprentices, repair customers, and electronic waste collectors. He gathered notes documenting a huge amount of observational data, took photographs, and made videos. Between December 2013 and January 2014, he conducted another round of ethnography at the same 10 sites. In that round he studied 70 negotiations between the customers and the repairers at several repair workshops. In addition to documenting their conversations, he separately interviewed both parties after the negotiations about the privacy of the data stored in those broken phones.

Following this ethnographic work, we conducted an online survey that asked people about their experiences while having their broken personal electronic devices repaired. In addition to collecting demographic data about the participants, we asked them about their use of electronic technologies, experiences with repairs, and privacy concerns. We made the questionnaire available online using Google Forms by sharing an invitation and link to the questionnaire publicly on Facebook. The invitation explicitly solicited participation from Bangladeshi citizens. Forty-eight participants responded to our online survey.

To further investigate people's perceptions and opinions regarding privacy during repair, we created a mobile phone application (app) called Protiraksha. It allowed users to track the history of apps accessed on their phone. That app essentially enabled people to monitor if or what apps somebody had accessed on their phone. To understand users' perceptions around privacy through this app, we circulated an advertisement on the Facebook groups of three universities in Dhaka and, from this, recruited 23 university students as our participants (12 of them were female). We began by conducting an initial interview that asked our participants about their ideas, experiences, and suggestions regarding privacy and repair. Next, we asked participants to use Protiraksha for two weeks. After two weeks, we interviewed the participants a second time and asked about their experiences using the app. We inquired about the challenges they perceived regarding different privacy-preserving measures and invited them to share their ideas with us regarding technology or policy design for preserving privacy.

Three of our five team members were born and raised in Bangladesh. One of these three members conducted the ethnography. All the field notes were written in Bengali. All the interviews were voluntary and lasted approximately 15 minutes. The interviews were later translated into English and transcribed.

Privacy and Repair in Dhaka

To provide a better understanding of privacy among repair communities in Dhaka, we first present a picture of the repair ecology from our ethnography. The electronic repair ecology in Bangladesh consists of a complex

combination of actors and activities. *Brand repairers* are the formal repair units found mainly in modern shopping malls and at stand-alone shops on the side of busy streets in wealthy neighborhoods. Well-known companies like Nokia, Samsung, and Siemens have their own "repair and service" stalls spread across the city. The repairers working in these service centers are usually educated and have formal certificates from government-registered universities. In our study, we found that the type of repair work they do for broken mobile phones consists mainly of replacement rather than actual repair. Fixing mobile phones at these service centers is often free if the warranty period still covers the device. However, in other cases, repairs done in these centers can quickly become expensive because the repairers demand both the price of the new components to replace the faulty ones and a high price for their labor. Hence, most of the customers who use these brand name service centers are wealthy.

In addition to the formal brand repair and service centers, many repairers work individually or under a master repairer. In most cases, these repairers are not well-educated and they lack formal certificates that document their repair skills. They learn the repair trade from master repairers through an apprenticeship. Gulistan Underground Market is one place where many such repairers work. The market is located underground at a busy intersection in the Gulistan area of Dhaka. About 500 mobile phone repairers work there. Almost all these shops either offer mobile phone repair services or sell parts used to repair mobile phones. There are also shops that sell second-hand mobile phones, and some repairers work in those shops. However, most repairers set up a desk in front of those shops and offer repair services as their sole business. The Gulistan market is almost always crowded, hot, and full of dirt and mud. Most customers who frequent the market are from low-income communities and want to have their mobile phones fixed cheaply.

Repair Transactions

The following vignettes illustrate some of the privacy threats that arise during the repair process. Although each case is situated within a specific context, none of them is a discrete incident. Rather, they represent a general pattern and common activities associated with mobile phone repair practices in Dhaka. To protect the privacy of our participants, real names have been replaced by pseudonyms.

Case 1

Mr. A is a 40-year-old businessman living in the Shantinagar area. He bought a smartphone last year that is giving him trouble. The mobile phone often fails to transmit his voice to the person he is speaking to so he has brought the phone to Mr. R's shop for repair. He did not previously know Mr. R. Mr. A was simply looking for a repair shop in the mall and found Mr. R's shop.

Mr. R first examined Mr. A's mobile phone and then demanded 500 Taka (~US$6.20) to fix it. After a round of bargaining, they settled on 300 Taka (~US$3.90). Mr. R kept Mr. A's phone and asked him to return in three days.

When Mr. A left the shop, we approached him and asked what sort of documents he had stored in his mobile phone. Mr. A informed us that he often took pictures with his phone since he did not like to carry a separate camera. His phone contained photographs of family members and other private and important moments in his life. He had shared some of his pictures on Facebook, but there were also many photos on his phone he did not want to share with people outside his family.

Case 2

Ms. Y is a 22-year-old undergraduate at a local private university who lives with her parents on Elephant Road. She recently bought a new mobile phone because her previous phone was very old; however, the new mobile started giving her trouble right from the beginning. She heard from several sources that Mr. B was a well-reputed repairer so she has brought her phone to him today.

After examining her phone, Mr. B demanded 700 Taka (~US$9) to fix it. Mr. B told the young woman there was no chance of bargaining, and she agreed to the price with little argument. Mr. B told her to return in four days.

We talked to Ms. Y as she left Mr. B's shop. She told us that she often used her phone to take photos with her boyfriend and she never shared them on Facebook. She said she would not feel comfortable if other people saw these photos. The photos were stored on the mobile phone she left with Mr. B.

These two cases represent the general pattern we observed with many of the repair customers whom we interviewed: They stored private photos and videos on their mobile phones that they would feel uncomfortable

sharing with others. However, all of them left their mobile phones with the repairer, who then had full access to those phones. As we can see here, the customers did not refuse the repair services even after knowing the possible risk to their private data. Although this observation engenders questions around the value of the private data to these customers, we require further study to learn the reasons that impact such decisions.

Inside a Repair Shop

We now describe three incidents that took place in a repair shop, drawing on our ethnographic field notes from the researcher who spent three weeks working as an apprentice in a workshop. These incidents highlight the vulnerability of private data stored on broken mobile phones in repair workshops.

Case 3

Two senior students are practicing at Mr. C's training center. They have already graduated from the training program and are now practicing the skills to gain some practical experience. One of the students is 18-year-old Mr. K; the other student is 25-year-old Mr. D. Today, Mr. C left them with seven mobiles, each of which had a problem that could be solved by *jumpering,* a technique that connects two points on a motherboard with a wire.

Mr. K is looking at a smartphone he is supposed to fix. He turns the phone on and says to Mr. D, "Look, this is a phone of the latest model. Mr. C said that the phone's speaker is not working. Look at the screen and the speed! This is a great phone." Mr. K continues to look at various features of the phone. Mr. D is less interested, saying of his phone, "This is a cheap Chinese phone. These phones are loaded with features, but all of those features are weak and full of viruses. These phones are of no use." Mr. K has just found a game on the phone. He shouts, "I saw this game on a phone that my friend has. I played this game; it is so much fun. Do you know if I can transfer this game to my phone? Both my phone and this one are Android." Mr. K starts playing the game and laughing. Mr. D warns, "You don't have all day. Stop playing, and let's get these tasks done. I have to leave early today." Mr. K says, "You can go whenever you want. I will return the phone to Mr. C in the evening. Don't worry." Mr. D exclaims, "Kids!"

Case 4

Mr. R has become my friend. He shares a lot of things with me as we work together in the workshop. Today Mr. R was asking me how to open a Facebook account. I said it was easy. I told him all he needed was an email account. He said he had heard it was even possible to open a Facebook account without an email account. I was surprised because I didn't know that was possible. He said he wanted to open a Facebook account because he had heard there were many pretty women on Facebook. He seemed to be excited about that and asked me if I had a Facebook account. I told him I did, and it was true that there were many beautiful women there. I asked him why he wanted to meet those women online. He said he wanted to have some fun. I jokingly said, "Then you have to present yourself as an attractive guy. Women won't like you otherwise." Mr. R said, "You will take some beautiful pictures of me around that corner of the mall. I will post those. You will write something smart for me." I laughed and said, "Well, I can do that for you if that helps, but I don't think your mobile phone has a good camera for that." Mr. R promptly replied, "Don't worry, my friend. I have a latest model Nokia phone here in my workshop. If you look at the pictures of that camera, you will be surprised." I asked, "How do you know? I heard their camera was not that good." He said, "The phone is on the middle shelf. You can just check the pictures stored on it. I was looking at those pictures yesterday, and thinking about if I had one such mobile phone . . ."

Case 5

Mr. BD was a student of Mr. E. He trained at Mr. E's mobile repair training center for three months and then he returned to his village to start a mobile phone repair business. Although he learned most of the techniques needed to fix basic problems that occur with mobile phones, he often gets more complex problems that he cannot fix himself. In those cases, he brings the mobile phones to Dhaka and meets Mr. E, who helps him fix them. In such cases Mr. E gets half the service fee, and Mr. BD keeps the rest.

Today Mr. BD brought 12 mobile phones from Chandpur (a district three hours from Dhaka). Mr. E was showing the phones to his students and asking them to do the necessary repairs. The most senior student in his workshop is Mr. M. Mr. M took one of the mobile phones in his hand and said, "Wow! Somebody in Chandpur uses an iPhone! That is very surprising. Let's see what he does with it." Mr. M switched on the phone and checked a variety of apps on the phone. He said, "I bet the user only uses this phone for taking selfies. Those are the only things I found on this phone. Such a waste of money."

Cases 3, 4, and 5 show that repairers often look at the private contents of customers' phones. Moreover, we directly observed many incidents of repairers using their customers' phones for the repairers' own purposes. They also frequently judged the financial and social circumstances of their customers by evaluating the mobile phones and the devices' data or contents. However, although repairers often talked among themselves about their customers' devices and data, we did not directly observe the repairers selling the private contents of customers' mobile phones to others.

Mobile Pornography Market

Above the Gulistan Underground Market, street hawkers sell CDs and DVDs that contain movies in various languages, including Bangla, Hindi, and English. When we asked one of the hawkers about those movies, we were asked if we would be interested in some "real spicy thing." On further inquiry we discovered that (at least) one of the hawkers had some private pornographic videos in MMS (multimedia messaging service) format available on CDs that he would sell. When we asked about the source of these videos, the hawker in question reluctantly answered, "Somewhere from the underground repair market." When we asked the hawker to introduce us to the repairer who was selling these videos to the hawkers, the hawker said he did not know any specific repairer and quickly left the area. We then approached three other such hawkers. All of them said the source of the pornographic videos was the underground repair market. However, none of the hawkers was willing to introduce us to any repairer who was selling these videos.

When we interviewed the repairers in the underground market and asked them about the market for mobile pornographic photos and videos, they agreed they had heard these kinds of stories, but none admitted to knowing anybody involved with it. However, one repairer told us, "In such a big market with so many people, if you leave a phone here, how can you trace who is taking your data where? So it is better to delete all sensitive data before giving the phone to a repairer here."

This case was not unique to the Gulistan Underground Market. Six of 10 major repair sites that we visited had similar CD/DVD markets nearby, and each of those markets would sell pornographic contents in MMS format. At these sites the hawkers informed us that the source of the pornographic content was the repair workshops at nearby markets, but no hawker was willing to introduce us to a repairer who sold such content. In addition, all the repairers we interviewed admitted to being familiar with such incidents, but denied involvement in the practice.

Takeaways

We learned several lessons from our observations and interviews in Dhaka's repair markets. First, private customer data stored on broken mobile phones is often leaked during the repair process. This private data may be converted to MMS and then copied and sold by many CD/DVD businesses.

Second, the repairers often use customers' mobile phones for the repairers' personal use. In addition, they often look at the media content stored on customers' mobile phones. When we asked the repairers how they felt about looking at such content, we found that none felt he was doing anything wrong. For example, one repairer told us,

> I did not see anything bad in that phone. If I found anything wrong, I would not show it to anybody. I would just keep quiet. So, I don't think I have done anything wrong. It would be wrong if I would publish somebody's secret photos.

Third, repair ecology in Dhaka involves complex networks of sharing, assistance, and exchange. Thus, it often becomes difficult for a repairer to track who is working on a phone at any given time in the workshop. In a typical repair shop, expert repairers and apprentices work together, and the mobile phones move around from one hand to another, both to fix and to teach apprentices how to fix the phones. In other cases, as in Case 5, mobile phones often travel from one workshop to another, some of which are not even in the same locality. During these travels, the phones are handled by many people, and the original repairer may not have control over who has access to private data stored in the phone.

Online Survey

The objective of our online survey was to better understand privacy threats during repair from the user perspective. Forty-eight people responded to our survey (33 male, 15 female). Of the 48 participants, 37 were students, seven had official jobs, and four owned a business. The majority (87%) were between 20 and 30 years old, while 11% were younger than age 20. The other 3% were older than 30 years.

The survey results revealed several interesting findings about repair and privacy. Laptops, desktops, and mobile phones were the three main electronic devices participants took to repairers. Of the content identified as personal, 42% was stored in image files, 19% was stored in text files, and 16% was stored in video files. The other 23% was too varied and insignificant. When choosing a repairer, 21% said they preferred to use a trusted friend, 21% said they chose a reputable repairer, 23% said they did not mind going to an unknown repairer, and 21% said they stayed with the repairer during the entire process. The rest of the participants adopted some other means (see Figure 1).

Almost half the participants (46%) suspected that their private data had been accessed during the repair process, and five participants were sure of it. One participant wrote that the repairer had erased all the personal data from his father's phone, which was a sure sign of accessing personal data. Another participant wrote,

> During repairing, the technician was checking out my photos folder. In one folder, there were some pictures of one of my female friends taken when we were vising a place as a group. He kept on looking at those pictures. Although the pictures were very typical tourism pictures, it made me feel really uncomfortable. I watched his activities from the reflection in the showcase mirror. He was unaware that I noticed his activities.

In addition to sharing their frustration regarding data privacy violations, our participants made a few suggestions about how to protect privacy during repair, such as locking personal data with authentication, using online storage and monitoring, watching repairers while they worked, and more. These findings suggest a need for design interventions that better protect privacy during repair.

Protiraksha

In the next phase of our study, we designed and developed a mobile phone application, Protiraksha, to explore what users would think about a software intervention to approach the problem of privacy during repair. In Bangla, *protiraksha* means protection or security. The mobile phone app was built on the Android operating system and was designed to track and display app access and use.

The rationale for developing this app is two-fold. First, many of the customers and repairers we encountered did not know that a technical solution was a possible approach to combating privacy threats. Hence, we wanted to create a simple app customers could easily understand that would generate further insights and additional thoughts or opinions about new applications and systems that could improve digital privacy. Second, we wanted to involve our participants in thinking about ways to combat privacy threats. An encryption-based solution would be challenging to explain in layperson's terms, and we concluded that presenting computation-heavy ideas might discourage users from using the app. Thus, we focused on designing an app that would be user-friendly and motivate participants to provide us with additional ideas and concerns.

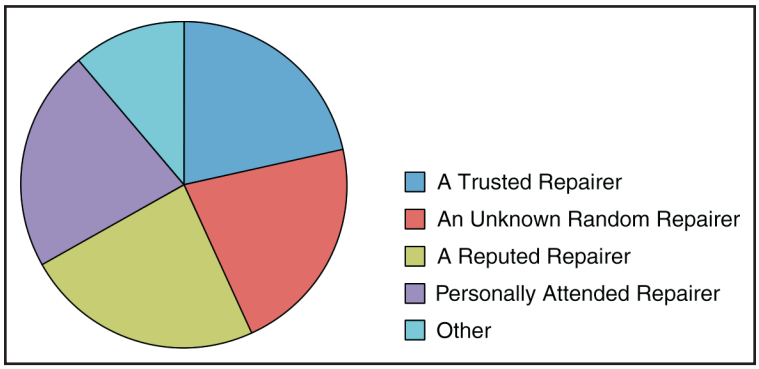

Figure 1. Repairer selection strategies.

Once a user would activate the Protiraksha app, it would work in the background without interrupting other operations. Every time an app was accessed, Protiraksha recorded a timestamp of the

Figure 2. Screenshots of the Protiraksha application. Left: The application prompts the user to turn on tracking. Right: The application shows the log of timestamps of when different applications were accessed.

access. When the user opened the app, they could see the "last access time" for all apps since Protiraksha had been turned on.

The benefit of using the Protiraksha app was that the owner would know if another person had accessed any of the phone's apps. During the repair process Protiraksha would record when the repairer accessed personal information through an app on the device. When the user retrieved their mobile phone from the repairer, they would be able to see any privacy breaches by analyzing the timestamps.

The objective of developing this app was not to impose surveillance to preserve the privacy of personal data stored on broken devices. It was obvious that if the software part of the phone was nonfunctioning, then Protiraksha itself might not work either. In addition, it would be possible for the repairer to turn off the app or find other ways to access private data that bypassed this kind of surveillance. However, we designed the app to understand, if such monitoring software existed, how users and repairers would react to such a tool and if technical interventions like this might aid privacy during repair. After deploying the app, we conducted several interviews, described in the following section.

Evaluation and Feedback

Our participants provided us with a wealth of feedback regarding their opinions about privacy during repair, their suggestions for preserving privacy, and their ideas about both technology- and policy-based solutions. From their feedback we have distilled a few important themes that both represent participants' thoughts on these topics and are relevant to our ongoing discussion of privacy and repair. These themes are meant to conceptualize some of the challenges associated with privacy during repair.

Ignorance, Uncertainty, and Confusion

A lack of understanding about privacy and repair was common to all participants. We found different levels of familiarity with privacy threats. For example, half our participants were unaware of the danger to data privacy on their mobile phone, only realizing this when we asked them questions about the topic. A few participants knew about data privacy, but did not realize their privacy could be vulnerable during repairs. Four participants were aware of privacy threats during repairs, but were unaware of ways to combat these threats.

We encountered a range of hypotheses and strategies and a general confusion surrounding data privacy. For example, three participants said they had asked for help from their friends and relatives instead of going to a professional repairer, and simply decided not to repair their mobile phones if they were unable to have the repair done by people close to them. Five participants relied on the reputation of the repairer, assuming a good reputation meant the repairer was trustworthy. Three others stayed with the repairer for the entire time to prevent a privacy breach. Another two participants took the memory card out of the phone before handing their device over to the repairer. However, they understood the repairers could still see any pictures saved on the

phone's built-in memory or access their email and Facebook accounts. All our participants expressed concern over these issues, but none knew any way to successfully combat the problem.

Beside these, it is often unclear to us whether our participants were more concerned about their private data being leaked to the repairers or to a broader audience through the repairers. Although we have observed several cases where the repair clients were uncomfortable about leaving their phones with the repairers, with some participants deciding not to repair their phones because of this, it requires further investigations to understand why some other clients left their phones with the repairers, even after understanding the potential risks.

Skepticism of Technical Solutions

We asked participants if they would like a technical solution that would preserve the privacy of their personal data during a repair. In general, we found participants to be skeptical about the effectiveness of any technical solution. When we asked them about Protiraksha, all participants expressed their satisfaction with the software's usability, describing how the app could help them protect their privacy during repair as well as at other times. However, they also shared concerns about using the software. For example, one participant told us,

> This software demonstrates a distrust. You don't trust the people around you and, hence, you have installed this. If you find somebody around you checked something on your phone, you will be more hurt than happy. So this software is risky.

We asked them about other potential mechanisms related to data encryption. It is worth noting that most participants were unfamiliar with these technical terms so we explained to them how encryption worked. We encountered a range of arguments against and concerns over encryption mechanisms. Most participants said they shared passwords, screen-locking keys, and other credentials with the repairers so they would be able to operate the phone as necessary. All participants mentioned they were always online on email and social media so they did not see how encryption could help them. In addition, most participants did not use external memory cards so the strategy of taking out the memory card was not helpful to them either.

Challenges Around Law and Policy

We asked participants if they would support laws or policies to preserve personal data privacy during repairs. We asked if they thought it would be a good idea to introduce punishments for repairers who intruded into personal data saved on a customer's phone. All participants vetoed this idea. We uncovered two primary reasons for their disagreement. First, all participants said they would be uncomfortable sharing such stories with others. For example, one participant told us,

> If they see something like a secret photo or video on my mobile phone, I am not going to call other people and talk about that because the other people, be they police or not, would want to check those secret files again. That is kind of a double insult.

Second, all participants were skeptical that it would be possible to implement such laws or policies in Dhaka. Several participants highlighted the weakness of Bangladesh's law enforcement agencies, while others pointed out their familiarity with police corruption and said it was common for police to silently support the perpetrators.

Trust, Religion, and Cultural Values

When we asked participants how a privacy-preserving environment could be developed within the repair ecosystem, they expressed a desire for an increased level of trust between customers and repairers. To achieve this increased level of trust, participants appealed to a range of social, religious, and cultural values. For example, one participant told us,

> It can be completely eradicated when the man who is repairing [the phone] is originally a good man. It will happen when he will have the knowledge about what he should access or what he should not. When he will have those ethics, that fear [of Allah], then he will not access it.

Similar suggestions were made about social and cultural values. One participant pointed out that local and known repairers would never do anything bad because their reputation would be damaged, explaining that

local repairers cared about their social reputation for their own business; therefore, they would not breach their customers' privacy. The repairers also expressed concerns around their professional and social status. One repairer told us, "No good repairer will do that. We need to fix the phone and we don't need to check what data are there inside the phone."

The customer participants emphasized a need to teach the repairers about social, cultural, and religious values. However, one senior and educated repairer blamed the inflow of uneducated and illiterate repairers into the repair market for these privacy problems, saying,

> The laptop and mobile repairing markets were confined to university graduates in the past. At that time, the quality of fixing was high. Plus, you would not hear any such case [of privacy breaches] then. As soon as the Chinese mobile phones and cheap accessories started to come into the market, the market started to be flooded with illiterate repairers. Many of them did not have moral teaching and they started doing all kinds of illegal things.

Another experienced, yet illiterate, repairer later refuted that argument, saying,

> Morality has nothing to do with literacy. You learn this from your family, from your friends, and from your neighborhood. We may be poor, but we are honest. But yes, there are some immoral repairers, and they cause all kinds of problems.

Discussion

This section synthesizes our findings into several key takeaways. We present these results as the first step in a larger research agenda that aims to better understand privacy during repair. We hope our work will encourage future scholarly discussions in this space.

The findings presented in the previous sections point to many important concerns around privacy during repair. First, following Nissenbaum's notion of privacy (Nissenbaum, 2004) as contextual integrity, we have obtained a local interpretation of privacy threats through our study. Our participants' responses clearly demonstrate that their privacy is often endangered at the repair workshops. Our investigation also reveals that people often lack the technical knowledge to combat such privacy threats, which often results in frustration, anxiety, and even non-use of technologies. For some customers, privacy concerns constitute a threat large enough to prevent them from being willing to get their electronic devices repaired in the market. Thus, we identify the problem of privacy during repair as a critical challenge for a country like Bangladesh, where the repair ecosystem has the potential to support sustainable ICT use.

Second, we reveal that technological interventions are not necessarily appropriate solutions to privacy-related problems during repair. Our study shows people are skeptical about encryption-based solutions, and they believe tech-based solutions are unworkable in the Bangladeshi context, both because of the practice of sharing passwords with the repairers and because users prefer to avoid tech-heavy solutions. Our software, Protiraksha, further revealed that some participants do not want to appear untrusting of the repairers (and others) by installing and using the software. Those participants who did react favorably to the Protiraksha liked it because of its silent mode of operation and its potential to work in a variety of settings in addition to repair.

Third, we reveal several challenges associated with drafting laws and policies to apply to the repair process, with participants expressing a reluctance to report a privacy breach. These findings are further supported by similar culturally sensitive findings in Bangladeshi contexts, such as Ahmed et al.'s findings that people are reluctant or unwilling to report sexual harassment (Ahmed et al., 2014). The barriers and limitations that affect both technical- and policy-based interventions create challenges for the privacy of mobile repair in Dhaka. Most existing privacy-related design interventions depend heavily on these two ideas—designing technologies or creating policies—but our study suggests a need for reimagined approaches that can overcome these limitations.

Fourth, our study indicates that possible solutions to the problem of preserving privacy during repair could come from leveraging the religious and cultural values of Bangladeshi society. Almost all participants stated that repairers need to be taught ethical behavior in addition to their technical lessons. Participants frequently mentioned how fear of "Allah," their deity, could discourage a repairer from accessing information stored on

customers' broken devices. On the other hand, many repairers said they considered ethical practices to be a part of good repairing. For them, doing anything that would breach customers' privacy would be bad for the repair community. Both conceptualizations indicate there are both religious and cultural values that affect the privacy-during-repair ecosystem and that could, even without technical or policy measures, help prevent privacy breaches.

Beyond these immediate implications, our study also uncovers opportunities to think about privacy in a wider context and its connection to development. The privacy vulnerability associated with information and communication technologies has not yet been extensively researched, particularly when technologies are deployed in developmental contexts. In addition, technology transfer from the Global North to the Global South also carries threats associated with privacy in the developing world. For example, in postcolonial literature, technology transfer has been seen as a major conveyor of cultural imperialism through technical means (Irani et al., 2010). Since privacy is culturally situated in a locale, privacy becomes vulnerable when foreign practices of interaction intrude into the community through technologies. In the Western world, privacy vulnerabilities are often combated through technical- or policy-level solutions, both of which may prove to be much weaker in developing countries like Bangladesh. Our study contributes to postcolonial computing literature by highlighting new challenges associated with the transfer of Western technologies to developing countries with different social or cultural values.

Conclusion

This article examines privacy challenges associated with technology repair markets in Dhaka, Bangladesh. We conducted ethnographic work to identify and explore privacy vulnerabilities that occur during the repair process. We identified and described several privacy threats through five vignettes that highlight the nature and complexity of these problems. Next, we described challenges associated with designing technologies and drafting laws and policies to combat privacy threats in the Bangladeshi repair communities. Our study reveals many broad social and cultural tensions that surround privacy during repair, and we uncover opportunities to develop technologies or draft policies to address those challenges. Beyond its direct contribution to the topic of privacy, this article joins a growing literature on post-use cycles of technology in ICTD by revealing a variety of social and cultural values that shape human activities while interacting with technologies in their post-use phases. ■

Syed Ishtiaque Ahmed, Assistant Professor, Department of Computer Science, University of Toronto. sa738@cornell.edu

Shion Guha, Assistant Professor, Department of Mathematics, Statistics and Computer Science, Marquette University. shion.guha@marquette.edu

Mohammad Rashidujjaman Rifat, PhD Student, Department of Information Science, University of Colorado Boulder. rashidujjaman.rifat@colorado.edu

Faysal Hossian Shezan, PhD Student, Department of Computer Science, University of Virginia. faysalhossain2007@gmail.com

Nicola Dell, Assistant Professor, The Jacob's Institute, Cornell Tech. nixdell@cornell.edu

References

Ahmed, S. I., Hoque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017). Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. *CHI'2017 Proceedings of the 35th ACM Conference on Human Factors in Computing Systems,* 906–918. doi:10.1145/2556288.2557376

Ahmed, S. I., Jackson, S. J., Ahmed, N., Ferdous, H. S., Rifat, M. R., Rizvi, A. S. M., & Mansur, R. S. (2014). Protibadi: A platform for fighting sexual harassment in urban Bangladesh. *CHI'2014 Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems,* 2695–2704. doi:10.1145/2556288.2557376

Ahmed, S. I., Jackson, S. J., & Rifat, M. R. (2015). Learning to fix: Knowledge, collaboration and mobile phone repair in Dhaka, Bangladesh. *ICTD'2015 Proceedings of the Seventh ACM Conference on Information and Communication Technologies and Development,* 4. doi:10.1145/2737856.2738018

Annas, G. J. (2003). HIPAA regulations: A new era of medical-record privacy? *New England Journal of Medicine, 138*(15), 1486–1490. doi:10.1056/NEJMlim035027

Chiasson, S., van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. *European Symposium on Research in Computer Security* (pp. 359–374). doi:10.1007/978-3-540-74835-9_24

Cranor, L. F., & Garfinkel, S. (2004). Guest editors' introduction: Secure or usable? *IEEE Security & Privacy, 2*(5), 16–18. doi:10.1109/MSP. 2004.69

CTV News Winnipeg. (2015, September 4). *Child pornography found during laptop repair leads to arrest, charges.* Retrieved from http://Winnipeg.ctvnews.ca/Child-Pornography-Found-during-Laptop-Repair-Leads-to-Arrest-Charges-1.2548589

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. doi:10.1109/TIT.1976.1055638

DiSalvo, C., Sengers, P., & Brynjarsdóttir, H. (2010). Mapping the landscape of sustainable HCI. *CHI'2010 Proceedings of the 28th ACM Conference on Human Factors in Computing Systems,* 1975–1984. doi:10.1145/1753326.1753625

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71–80). ACM. Alexandria, VA. doi:10.1145/1102199.1102214

Houston, L. (2014). *Inventive infrastructure: An exploration of mobile phone.* (PhD Thesis). Bailrigg, UK: Lancaster University.

Irani, L., Vertesi, J., Dourish, P., Philip, K., & Grinter, R. E. (2010). Postcolonial computing: A lens on design and development. *CHI'2010 Proceedings of the 28th ACM Conference on Human Factors in Computing Systems,* 1311–1320. doi:10.1145/1753326.1753522

Jackson, S. J. (2013). Rethinking repair. In T. Gillespie, P. Boczkowski, & K. Foot (Eds.), *Media meets technology: Essays on communication, materiality and society.* Cambridge, MA: MIT Press. doi:10.7551/mitpress/9780262525374.001.0001

Jackson, S. J., Ahmed, S. I., & Rifat, M. R. (2014). Learning, innovation, and sustainability among mobile phone repairers in Dhaka, Bangladesh. *DIS'14 Proceedings of the 10th Conference on Designing Interactive Systems,* 905–914. doi:10.1145/2598510.2598576

Jackson, S. J., Pompe, A., & Krieshok, G. (2011). Things fall apart: Maintenance, repair, and technology for education initiatives in rural Namibia. *Proceedings of the Sixth iConference,* 83–90. doi:10.1145/1940761.1940773

Kumaraguru, P., & Cranor, L. F. (2006). Privacy in India: Attitudes and awareness. In G. Danezis & D. Martin (Eds.), *Privacy enhancing technologies.* PET 2005. Lecture Notes in Computer Science (Vol. 3056). Berlin and Heidelberg, Germany: Springer. doi:10.1007/11767831_16

Lipford, H. R., Hull, G., Latulipe, C., Besmer, A., & Watson, J. (2009). Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference* (Vol. 4, pp. 985–989). IEEE. Vancouver, BC. doi:10.1109/CSE.2009.241

Mao, W. (2003). *Modern cryptography: Theory and practice.* Upper Saddle River, NJ: Prentice Hall Professional Technical References.

Microsoft. (n.d.). *To decrypt a file or folder.* Retrieved from https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt_to_decrypt_file.mspx?mfr=true

Nissenbaum, H. (2004). Privacy as contextual integrity. *Walsh Law Review, 79,* 119.

O'Donnell, M. L. (2002). FERPA: Only a piece of the privacy puzzle. *Journal of College and University Law, 29,* 679.

Orr, J. E. (1996). *Talking about machines: An ethnography of a modern job.* Ithaca, NY: Cornell University Press,

Raab, C. D. (1997). Privacy, democracy, information. In B. D. Loader (Ed.), *The governance of cyberspace* (pp. 155–174). London, UK: Routledge.

Raleigh, W. J. (1988). Attorney-client privileges. *Barrister, 15,* 49.

Sadeh, N., Hong, J., Cranor, L. F., Fette, I., Kelley, P., Prabakar, M., & Rao, J. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing, 13*(6), 401–412. doi:10.1007/s00779-008-0214-3

Sen, A. (1999). *Development as freedom.* Oxford, UK: Oxford University Press.

Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review, 5*(1), 3–55. doi:10.1145/584091.584093

Suchman, L. (2007). *Human-machine reconfigurations: Plans and situated actions.* Cambridge, UK: Cambridge University Press.

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

Zurco, M. E., & Simson, R. T. (1996). User-centered security. In *Proceedings of the 1996 workshop on new security paradigms* (pp. 27–33). ACM. doi:10.1145/304851.304859