Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh

Conference Paper · June 2016

DOI: 10.1145/2909609.2909661

CITATIONS
18

READS
90

5 authors, including:

Syed Ishtiaque Ahmed
University of Toronto
101 PUBLICATIONS **776** CITATIONS
SEE PROFILE

Mohammad Rashidujjaman Rifat
University of Toronto
20 PUBLICATIONS **229** CITATIONS
SEE PROFILE

Faysal Hossain Shezan
University of Virginia
10 PUBLICATIONS **22** CITATIONS
SEE PROFILE

Nicola Dell
University of Washington Seattle
50 PUBLICATIONS **860** CITATIONS
SEE PROFILE

Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh

Syed Ishtiaque Ahmed
Department of Information Science
Cornell University, Ithaca, NY
sa738@cornell.edu

Shion Guha
Department of Information Science
Cornell University, Ithaca, NY
sg648@cornell.edu

Md. Rashidujjaman Rifat
Design Technology Lab
NYU - Abu Dhabi, UAE
mr4592@nyu.edu

Faysal Hossain Shezan
Department of CSE
Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
faysalhossain2007@gmail.com

Nicola Dell
Department of Information Science
Jacobs Institute
Cornell Tech, New York, NY
nixdell@cornell.edu

ABSTRACT

This paper presents an analysis of the privacy issues associated with the practice of repairing broken digital objects in Bangladesh. Historically, research in Human-Computer Interaction (HCI), Information and Communication Technologies for Development (ICTD), and related disciplines has focused on the design and development of new interventions or technologies. As a result, the repair of old or broken technologies has been an often neglected topic of research. The goal of our work is to improve the practices surrounding the repair of digital artifacts in developing countries. Specifically, in this paper we examine the privacy challenges associated with the process of repairing digital artifacts, which usually requires that the owner of a broken artifact hand over the technology to a repairer. Findings from our ethnographic work conducted at 10 repair markets in Dhaka, Bangladesh, 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 in repair and its connections with 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 in ICTD and HCI.

Categories and Subject Descriptors

H.1.2. Human Factors

General Terms

Human Factors

Keywords

Repair; privacy; developing country; ICTD; DEV; Bangladesh.

1. INTRODUCTION

Privacy has been conceptualized in a variety of ways over the past century of scholarship. Warren and Brandeis called it "*the right to be let alone*" [29], while Westin thought about privacy as the ability to determine for ourselves "*when, how, and to what extent information about us is communicated to others*" [30]. More recently, Palen & Dourish suggested that the notion of privacy is a "*dynamic, dialectic process*" [23]. In a similar vein, Nissenbaum developed the idea of privacy as "*contextual integrity*" [20] and postulated that what is construed as private information is contextual, temporal and audience dependent. Although these works discuss conceptual models of privacy in different contexts, one theme that they have in common is that they position privacy as an inalienable human right.

Privacy and computing have been entwined since the inception of computing, with very different foci in different time periods. For instance, appropriate and rigorous security has been seen as the optimal approach to securing private data and computing systems [19]. Initially, this was formulated as a mathematical and engineering problem [27] and indeed, cryptographic and other security based approaches are still popular [7]. However, a few decades ago, there was a subtle shift away from pure engineering solutions to towards a more human centered approach [32]. This nascent field of study has at times been called "usable privacy and security" [6] and considered to be at the intersection of computer science, privacy and security, and HCI. There have been numerous human-centered studies that aim to understand privacy across in computing, including understanding password construction and use [4], text password alternatives [4], inferences about privacy preferences from social network behavior and use [8], design recommendations for supporting privacy [18], as well as privacy in mobile computing and other similar systems [25]. However, the vast majority of these studies have 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 populations in developing countries. One notable exception is work by Kumaraguru and his colleagues that recognized this gap and examined notions of privacy around the use of digital technologies on the Indian subcontinent [16].

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 get broken. Breakdown, maintenance, and repair are inescapable features of the computing technologies that we interact with, and people's privacy may be particularly vulnerable during these moments. Our

ICTD '16, June 3–6, 2016, Ann Arbor, Michigan, USA

http://dx.doi.org/10.1145/2737856.2738013

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 [2, 9, 11]. However, to the best of our knowledge, ours in the first paper to focus on the challenges and issues surrounding privacy in repair in ICTD contexts.

Our paper makes the following contributions. First, we present findings from a three-month ethnographic study conducted at ten major electronic repairing 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 a number of vignettes that highlight privacy concerns and challenges associated with repair. Following this, we conducted an online survey to more broadly assess people's perceptions and prior experiences regarding privacy in repair. We then developed and deployed a mobile application, *Protiraksha*, to explore people's reactions to a software tool that exposes if and when their privacy has been violated during the repair process. Findings from our deployment highlight the challenges associated with privacy law and policy, skepticism regarding technology solutions, as well as the importance of cultural and religious values and trust. Taken together, our findings contribute to the growing discourse around post-use cycles of technology in ICTD and HCI.

2. RELATED WORK

A number of research papers have pointed out the need to consider repair as a research topic in the study of computing technologies. For example, Lucy Suchman's "*Plans and Situated Actions*" demonstrated that machines that had been designed to perform certain tasks failed when they experienced uncertain or unexpected conditions [28]. Although Suchman's empirical work focused on an artificial intelligence machine built to communicate with human beings, the general idea of vulnerability of computing systems under unexpected situations remains a concern. This perspective helps us to understand the paucity of research and development efforts that specifically focus on the moments in which a computing machine does not work. As a result, knowledge of maintenance and repair is often unstructured, poorly documented, and ignored by formal engineering scholarship. Julian Orr's work, "*Talking About the Machine*", further advanced our understanding around repair. Orr studied how repair workers at Xerox learnt repairing techniques from their seniors through informal conversations [22], and helped to position repair as an important concern in the study of computing technologies.

A growing strand of work in Human-Computer Interaction (HCI) and Computer Supported Collaborative Works (CSCW) focus on the importance of repair and maintenance and a number of lessons have been learned around repairing electronic devices. For example, Jackson and his colleagues conducted ethnography with electronic repairers in Namibia and found that local repairing practices are connected with the global network on knowledge and materials [14, 15]. Houston studied the innovative technical practices associated with repairing mobile phones in Kampala, Uganda [9]. Jackson et al. conducted ethnography in Dhaka, Bangladesh and studied mobile phone repairer communities, revealing the art and craft involved in repair work that are often ignored and/or unrecognized in mainstream study and research in electronic engineering [12]. Ahmed et al. also studied repairer communities in Dhaka, documenting different kinds of explicit, tacit, and social knowledge that are practiced among those communities [2]. These ethnographic studies show how the nature of repair is embedded in the socio-economic fabric of a country and has the potential to play an important role both in strengthening the knowledge of technology and in advancing international development through technical means. Jackson's essay, "*Rethinking Repair*", depicts a broad picture of repair and its connection with our conceptualization of infrastructure in general [11]. His essay puts forth the experiences around breakdown and repair, and how infrastructures are conceptualized and organized against the constant threat of breakdowns.

In addition to technology and repair, scholars have connected repair with global development in different ways. For example, some have depicted repair as a response to post-colonial computing [10], pointing out that technology transfer from the developed western world to developing countries have economic, cultural, and political aspects that may be detrimental to the development of a country. In addition, post-colonial computing points out that western practices regarding technology are often centered on design and use. The consumerist spirit that is present in many developed countries promotes the consumption of new technologies over the repair of old technologies to further the capitalist agenda of production. This practice has resulted in the topic of repair often being neglected or overlooked. However, repair is important for many developing countries for both economic and cultural reasons. For example, a large number of mobile phone users in developing countries depend on repaired and/or second-hand mobile devices. In these developing economies, repairers play an important role in the consumption and sustainability of technologies, contributing to a reduction in the purchase of foreign products and western consumerist culture.

Repair is also deeply connected with a number of human factors beyond purely economic or functional reasons. For example, Jackson and Kang investigated the reasons why people fix broken objects, finding that their reasons included 'preservation of memory', 'love toward the object', 'artistic interest', and 'fun' [13]. These 'non-functional' human factors are often ignored in ICTD discourse. Chirumamilla and Pal argued that conventional ICTD research often treats people in developing countries as objects that are strictly concerned with functional needs, including food, employment, education, medicine, etc. Their work describes a need for more research that values 'non-functional' human factors [5]. We argue that repair offers a platform for people to be engaged with the material objects around them, and to be more mindful of themselves, family, society, and culture through those materials by going beyond purely functional values.

The art and craft of repair that technology repairers in developing countries often possess are mostly ignored in mainstream western-oriented technical discourse. However, Jackson et al. showed that those skills are in fact highly valuable and can constitute a novel platform for interacting with technologies as well as an important technical platform for development [12]. The paper points out that although many countries in the 'developed West' are focused on producing more and more new objects, many of which find their way across the globe, developing countries are able to set an example for the rest of the world by repairing, repurposing, and recycling those technologies. Building on the necessity of being mindful about the entire lifecycle of technology, as depicted by Lepwasky [17], this platform of technology repair and recycling can be as important as that of production. At the same time, repairing can make substantial contributions to the reduction of e-waste, which is a big concern across the globe, and particularly in developing countries [31].

2.1 Privacy and Repair

Research that examines the relationship between privacy and repair is notably absent in current literature. In a broad sense, privacy in repair communities can be thought of as a transactional and submission process [20] 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 servicing centers to operate according to predefined policies that don't directly address the privacy issue but that perhaps reduce the motives for repairers to delve into the private information of users. However, if a breach of privacy happens, 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 [33]. 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 [34]. 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 is regarded as private and is protected by HIPAA [3], which provides standards, conditions and legislative redressal mechanisms for violations of patient data interchange. Similarly, in civil and criminal law, attorney-client discussions are considered privileged information and cannot be disclosed to the public except under very narrow circumstances [24]. In the realm of higher education, FERPA [21] manages and protects the education records of students, which are respected as private information by United States federal law. However, there are no such protections afforded to repairer-user negotiations. Prior usable privacy research has shown that not only are people concerned about mobile data privacy [25] 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 the mental and social health of users [25]. In light of similar, potentially harmful disclosures also occurring in repairer-user communities, we argue that this issue is relevant, understudied and ripe for further investigation.

2.2 Privacy and Development

Although some prior work related the idea of privacy with the liberal definition of development [30], we have not found any direct relationship between general development theory and privacy discourse in information technologies. In this paper, we draw two separate connections between privacy in broken technologies and development. First, we develop connections between ICTD and privacy. To this end, we seek refuge in the classic development theory given by Nobel Laureate economist Amartya Sen, who defined development as "freedom" that has to be achieved through both instrumental and constitutive means [26]. We extend this idea of development to explain the need for privacy. As seen in other studies and also in the latter part of our study, lack of privacy may discourage people from using a technology. As a result, the person loses his or her instrumental freedom to access information technologies and therefore any developmental services provided through those technologies. At the same time, the issue of privacy also has a constitutive aspect. A person, being a part of a particular society and culture, develops his or her own definition of privacy that has to be nurtured and protected by the society and the state in order to preserve the constitutive means of freedom. Hence, from both of these perspectives, privacy is an important factor for development through technology.

Finally, Ahmed et al. [2] suggested that repair should be considered as a potential novel venue for development. As we will discuss in this paper, the repair workshops in Bangladesh, like in many other countries, suffer from a serious level of privacy vulnerability. As a result, many customers hold back from going to those workshops to get their broken technology repaired. This practice, in turn, negatively impacts both the technology ecology of the country and the socioeconomic development of the repairers as a technical community. Thus, we argue that understanding and addressing privacy in repair constitutes an important research agenda for ICTD. Our work both contributes to this agenda and proposes it an avenue for future research.

3. METHODS

Our study was conducted in Dhaka, the capital city of Bangladesh. Our investigations around repair, privacy, and practices associated with these took place through a number of studies conducted between May 2013 and May 2015. In the first phase, we conducted a 3-month ethnographic study in Dhaka to understand the practice of repairing mobile phones from the point of view of repairer communities. From June to September 2013, we visited ten major electronic repairing sites in Dhaka. In addition, during this period one researcher on our team spent time learning to repair mobile phones at a training center operated by a senior repairer. Following this, the researcher worked for three weeks in another repair shop as an apprentice. This allowed him to be deeply engaged with the community and learn the norms and values associated with mobile device repairing. While working as an apprentice he also conducted semi-formal interviews of individual repairers working in stand-alone workshops or as 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 ten sites. In this round, he studied 70 negotiations between customers and repairers at different repair shops. In addition to documenting their conversations, he separately interviewed both parties after the negotiations and asked questions regarding the privacy of the data stored on the broken device and other related questions.

Following this ethnographic work, we conducted an online survey that asked people questions regarding their experiences while fixing their broken personal electronic devices. In addition to collecting demographic data about the participants, we asked about general use of electronic technologies, experiences with repairing technologies, and any concerns about privacy in repair. We made the questionnaire available online using Google forms and shared an invitation and link to the questionnaire publicly on Facebook. The invitation explicitly solicited participation from Bangladeshi citizens. A total of 48 participants responded to our online survey, with all of the participants reporting that they were indeed from Bangladesh.

To further investigate people's perceptions and opinions regarding privacy in repair, we designed and developed a mobile phone application, called '*Protiraksha*', that allowed users to keep track of the history of applications that were accessed on their phone using timestamps. This essentially enabled people to monitor if and when somebody had accessed an application on their phone. To understand users' perceptions around privacy through this application, we circulated an advertisement on the Facebook groups of three universities in Dhaka and recruited 23 university students who responded to the advertisement. 50% of our participants were female. We began by conducting an initial interview that asked 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 participants a second time and asked about their experiences using the application. We inquired about the challenges that 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 out of five members of our team were born and brought up in Bangladesh and are also citizens of Dhaka. The ethnography was conducted by one of these three members and all field notes were written in Bangla. Three Bangla speaking members of our team conducted the interviews. All the interviews were voluntary, conducted in Bangla, and lasted no more than 15 minutes. Then the interviews were translated into English and transcribed.

4. PRIVACY AND REPAIR IN DHAKA

To gain a better understanding of privacy among the repair communities in Dhaka we first present a picture of this ecology from our ethnography. The electronic repair ecology in Bangladesh consists of a complex combination of different actors and activities. Brand repairers are formal repairing units that are mostly found in modern shopping malls or stand-alone outlets on the side of busy streets in wealthy neighborhoods. Renowned companies, like Nokia, Samsung, and Siemens, have their own 'repair and service' stalls spread across the city. Smaller brands also have their 'service centers' in most big shopping malls and other commercially important places. The repairers working in these 'service centers' are usually educated and have formal certificates from government-registered universities. They only provide service to customers who use mobile phones of their relevant brand. In our study we found that the type of repairing that they do for broken mobile phones is mostly 'replacement' rather than a real 'repair'. Fixing mobile phones at these service centers is often free if the device is still covered by the warranty period. However, in other cases, repairs done in these centers can quickly become very expensive because the repairers demand both the price of the new components that replace the faulty ones and a high price for their labor. As a result, most of the customers who utilize these brand name service centers are wealthy.

In addition to formal brand repairing and servicing centers, a large number of repairers work individually or under a master repairer in different parts of the city. In most cases, these repairers are not well educated and they do not have any formal certificates that document their repairing skills. They learn repairing from master repairers through apprenticeship. Gulistan Underground Market is one place where many such repairers work (see Figure 1). The market is located underground at a busy cross-section in Gulistan area of Dhaka. About 500 mobile phone repairers work there. Almost all of the shops there either offer mobile phone repairing services or sell parts that are used for repairing mobile phones. There are also shops for selling second hand mobile phones and some repairers work in these shops. However, most of the repairers set up a desk in front of these shops and offer mobile phone services as their individual business. The market is almost always crowded, extremely hot, and full of dirt and mud. Most of the customers that frequent the market are from low-income communities and go there to fix their mobile phones cheaply.

A third important community in the repair ecology of Dhaka is the community of e-waste collectors, known locally as '*Bhangari*'. The Bhangari roam around the city collecting broken electronic devices (or their parts) from repair shops, offices, and individual houses. After collection, they categorize different devices or parts based on their value in the recycling market. For example, motherboards are usually sorted based on the presumed gold that they contain. Other important components of broken electronics are metals and undamaged integrated circuits. The Bhangari community that we studied was located at a narrow street connected with Elephant Road, one of the busiest areas of Dhaka, and populated with a number of computer markets and repairing shops. The Bhangaris that we studied would go to the repair shops to collect broken mobile phones and computer parts that the repairers had rejected because they were beyond repairing. The Bhangaris bought those broken devices for a nominal fee. They would then sell the components on to local and foreign e-waste businessmen. For example, some of the Bhangaris told us stories of Chinese businessmen who would often come and buy broken devices. According to the Bhangaris, these businessmen would melt the electronic devices to separate out the precious metals. The rest of the materials would then be used for producing new motherboards. Most of those recycling facilities were in China although there were also several in Bangladesh.

Figure 1. A busy lane in the Gulistan Underground Market on which there are many mobile phone repair stalls.

4.1 Repairing Transactions

Based on findings from our ethnographic studies, we describe below a number of vignettes that illustrate several of the privacy threats that surround the repairing process. Although each of these cases is situated within a specific context, none of them is a discrete incident. Rather they represent a general pattern and commonplace activities associated with mobile phone repairing practices in Dhaka. To protect the privacy of our participants, real names have been replaced by pseudonyms.

4.1.1 Case 1

This excerpt from our field notes constitutes our first case:

Mr. A is a 40-year-old businessman living in the Shantinagar Area. He has been married for seven years and has a three-year-

old daughter. He bought a smartphone last year that is now giving him trouble. The mobile phone often fails to transmit his voice to the person he his speaking to. The problem was difficult for him to figure out at the beginning. At first, he thought it was a network problem, or a problem with the phone of the person he was speaking to. However, when the same problem occurred a number of times with different people, he decided to test his own phone with the help of his wife at home. When he could not hear anything from his wife's phone, he understood that there was something wrong with his phone. So, he has brought the phone to Mr. R's shop for fixing. He did not know Mr. R before. He was just looking for a repair shop in the mall and found this one.

Mr. R first examined Mr. A's mobile phone and then demanded 500 Taka (approx. USD 6.2) to fix it. After an episode of bargaining, they settled on 300 Taka (approx. USD 3.9). Mr. R kept Mr. A's phone, and asked him to come back after 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 mobile phone since he did not like to carry a separate camera with him all the time. So, his phone contained photographs of his 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.

4.1.2 Case 2

This excerpt from our field notes constitutes our second case:

Ms. Y is a 22-year-old undergraduate student at a local private university. She lives with her parents on Elephant Road. She recently bought a new mobile phone because her previous phone was very old. However, her new mobile phone started giving her trouble right from the beginning. She has been using this phone for five months now and she has had to take the phone to a repairer almost every month. The main problem she has is with the charging unit of the phone. At first, she thought the problem occurred because of a faulty battery. However, the problem persisted even after she changed the battery. The previous repairer charged her about 1000 Taka (approx. USD 12), but the problem reappeared after just a few days. She heard from different sources that Mr. A was a well-reputed repairer and so she has brought her phone to him today.

After examining her phone, Mr. A demanded 700 Taka (approx. USD 9) to fix it. Mr. A told the girl that there was no chance of bargaining and she agreed to the price with little argument. Mr. A told her to come back after four days.

We talked to Ms. Y as she left Mr. A'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 with other people seeing these photos. The photos were stored on the mobile phone that she left with Mr. A.

These two cases represent a general pattern that we observed with many of the repair customers that we interviewed: they stored private photos and videos on their mobile phones that they would not feel comfortable sharing with others. However, all of them left their mobile phones with the repairer who then had full access to the phone and their private data stored on it.

4.2 Inside a Repair Shop

We now describe the scenario of a typical repair shop, drawing on ethnographic field notes from a researcher who spent three weeks working as an apprentice in a workshop. The following two incidents highlight the vulnerability of private data stored on broken mobile phones in repair workshops.

4.2.1 Case 3

This excerpt from our field notes constitutes our third case:

Two senior students are practicing at Mr. A's training center. They have already graduated from the training program and they are now practicing the skills to gain some practical experience. They are also looking for jobs and Mr. A is helping them with their job search. In return, they are helping Mr. A in his workshop by doing basic repair tasks. One of the students is 18-year-old Mr. K. Mr. K left his school at his home district and came to Dhaka looking for work. The other student is 25-year-old Mr. R. Mr. R graduated from university after studying Bangla literature and now works in a local press. However, he does not earn much money in his profession and so he is trying to become a repairer. Today, Mr. A left them with seven mobile phones, 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 that he is supposed to fix. He turns the phone on and says to Mr. R, "Look this is a phone of the latest model. Mr. A said that the phone's speaker is not working. Look at the screen and the speed! This is a great phone." Mr. K keeps looking at different features of the phone. Mr. R is less interested, saying, "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. R 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. A in the evening. Don't worry." Mr. R says, "Kids!" ...

4.2.2 Case 4

This excerpt from our field notes constitutes our fourth case:

Mr. R has become my friend. He shares a lot of things with me 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 that 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. He said he wanted to open a Facebook account because he had heard that there were many pretty women on Facebook. He seemed to be very excited about that and asked me if I had a Facebook account. I told him that I had one and that 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 ..."

4.2.3 Case 5

This excerpt from our field notes constitutes our fifth case:

Mr. B was a student of Mr. A. He trained at Mr. A's mobile repairing training center for three months and then he went back to his village and started his mobile phone repair business there. Although he learned most of the techniques needed for fixing basic problems that occur with mobile phones, he often gets more complex problems that he cannot fix by himself. In those cases, he brings the mobile phones to Dhaka and meets Mr. A, who helps him to fix them. In such cases, Mr. A gets half of the total service fees and Mr. B keeps the rest for himself.

Today Mr. B brought 12 mobile phones from Chandpur (a district three hours away from Dhaka). Mr. A 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 different things on the phone. He then 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."

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

4.3 Mobile Pornography Market

Right over the Gulistan Underground Market, a number of street hawkers sell CDs and DVDs that contain movies in different languages, including Bangla, Hindi, and English (see Figure 2). When we went to ask on 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 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 further requested that the hawker introduce us to the repairer who was selling these videos to the hawkers, the hawker said he did not know any particular repairer and then he quickly left the place. We then approached three other such hawkers and all of them said that the source of the pornographic videos was the underground repair market. However, none of the hawkers was willing to introduce us to any particular repairer who was selling these videos.

When we interviewed repairers in the underground market and asked them about the market for mobile pornographic photos and videos, all of them agreed that they had heard these kinds of stories, but none of them 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 at Gulistan Underground Market. 6 out of 10 major repair sites that we visited had a similar kind of CD/DVD market nearby, and each of those markets would sell pornographic content in MMS format. At all of these sites, the hawkers informed us that the source of the pornographic content was the mobile phone repair shops at nearby repair markets, but none of them was willing to introduce us to a particular repairer who sold such content. In addition, all of the repairers that we interviewed admitted to being familiar with such incidents but denied being involved in these practices.

Figure 2. A computer CD/DVD shop in Dhaka. These shops often offer customers CDs and DVDs loaded with pornographic photos and videos captured with mobile phone camera (faces are blurred to preserve anonymity).

4.4 Takeaways

We learned a number of lessons from our observations and interviews at the repair markets in Dhaka. First, private customer data stored on broken mobile phones is often leaked during the repair process. In addition, 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 their personal use. In addition, they often look at the media content stored on customers' mobile phones. When we asked them how they felt about looking at such content, we found that none of them considered that they were 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, the ecology of repair in Dhaka involves complex networks of sharing, help, and exchange. As a result, it often becomes difficult for a repairer to track who is working on a particular phone at a particular time in the workshop. In a typical repair shop, both expert repairers and apprentices work together and the mobile phones move around from one hand to another, both for the purpose of fixing the phones and of teaching 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 different people and the original repairer may not have control over who has access to private data stored on the phone.

5. ONLINE SURVEY

The objective of our online survey was to better understand privacy threats in repairing from the user perspective. 48 people responded to our survey (33 male, 15 female). Of the 48 participants, 37 were students, 7 had official jobs, and 3 owned a business. 87% were between 20 and 30 years old, while 11% were younger than 20 years old.

The results of the survey reveal a number of interesting findings around repair and privacy. Laptops, desktops, and mobile phones were the three main electronic devices that participants had taken to repairers to be fixed. 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. When choosing a repairer, 21% said that they preferred to use a trusted friend, 21% said that they chose a reputed repairer, 23% said that they did not mind to go to a totally unknown repairer, and 21% said that they stayed with the repairer for the entire repairing process. The rest of the participants adopted some other means (see Figure 3).

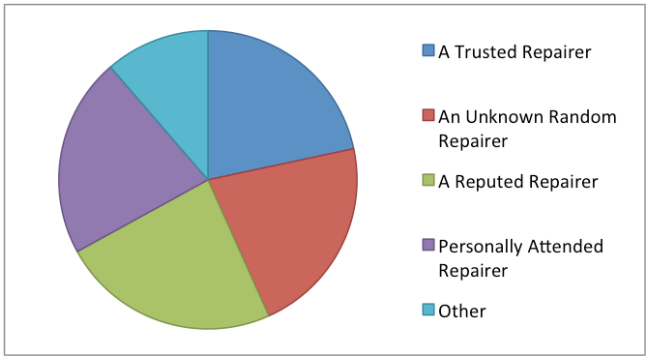

Figure 3: Repairer selection strategies

Almost half of our participants (46%) suspected that their private data had been accessed during the repair process, and five participants were absolutely sure about it. One participant wrote that the repairer had erased all the personal data from his father's mobile 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 frustration regarding data privacy violations, our participants made a number of suggestions about how to protect privacy in repair, such as locking personal data with authentication, using online storage and monitoring, surveillance over repairers, and more. These findings suggest a need for design interventions that better protect privacy in repair.

6. PROTIRAKSHA

In the next phase of our study, we designed and developed a mobile phone application, "*Protiraksha*", to explore how users would think about a software intervention to approach the problem of privacy in repair. In Bangla, the word, "*Protiraksha*" means "protection" or "security". The mobile phone application was built on the Android operating system and was designed to keep track of the time at which each application on the phone was last accessed and display this information to the user.

Fig 4. Screenshots of the *Protiraksha* application. Left: the application is prompting the user to turn on tracking. Right: the application is showing the log of timestamps for when different applications were accessed.

The rationale for developing this application is two-fold. First, many of the customers and repairers that we encountered did not know that a technical solution would be a possible approach to combating privacy threats. As a result, we wanted to create a very simple application that they could easily understand and that would generate further insights and additional thoughts or opinions. Second, we wanted to involve our participants in thinking about different ways to combat privacy threats. An encryption-based solution would be challenging for them to understand and we suspected that presenting any computation-heavy ideas might drive them away from thinking about the problem. Thus, we focused on designing a very simple application that would be clear to participants and motivate them to provide us with additional ideas and concerns.

After the user activated the *Protiraksha* application it worked silently on the phone without interrupting other operations. Every time an application on the phone was accessed *Protiraksha* simply recorded a timestamp of the access. When the user opened the application, they could see the 'last access time' of all applications since *Protiraksha* had been turned on.

The benefit of using the *Protiraksha* application is that the user would be able to know if any other person accessed any of the phone's applications. In the repair process, the application would record if and when the repairer accessed personal information using an application on the device. Then, when the user obtains their mobile phone from the repairer, they would be able to see any privacy breaches by analyzing the application timestamps.

The objective of developing this application was not to use surveillance to preserve the privacy of personal data stored on broken devices. It was obvious that if the software part of the phone was non-functioning, then this application itself might also not work properly. In addition, it would be possible for the repairer to turn off the application or find other ways to access private data that bypassed this kind of surveillance. However, we designed the application 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 in repair. After deploying the application, we conducted a number of interviews as described in the following section.

6.1 Evaluation and Feedback

Our participants provided us with a rich amount of feedback regarding their opinions about privacy in repair, their suggestions for preserving privacy, and their ideas about both technology and policy-based solutions. From their feedback, we have distilled a number of important themes that both represent participants' thoughts around these topics and that are relevant to our ongoing discussion around privacy and repair. The themes are presented in no particular order. We are also not suggesting that these themes represent the privacy perceptions of Dhaka or Bangladesh as a whole. Instead, the themes are intended to conceptualize some of the challenges associated with privacy in repair.

6.1.1 Ignorance, uncertainty, and confusion

Lack of understanding around privacy and repair was common among all of our participants. We found different levels of familiarity with privacy threats. For example, several of our participants were not even aware of the privacy of data on their mobile phone, and they only realized this when we asked them questions about the topic. Several other participants knew about data privacy but did not realize that their privacy could become vulnerable during the repair process. Four participants were well aware of privacy threats during the repair process but were unaware of any ways to avoid these threats.

We encountered a range of different hypotheses, strategies, and general confusion surrounding data privacy. For example, three participants said that they 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 get the relevant help from people close to them. Several other participants relied on the reputation of the repairer, assuming that a good reputation meant that the repairer could be trusted. Several others stayed with the repairer for the entire time that it took to repair the phone to prevent a possible breach of privacy. Another two participants took the memory card out of the phone before handing their device over to the repairer. However, they agreed that the repairers could still see any pictures saved on the phone's built-in memory, or access their email and Facebook accounts. All of our participants expressed concern around these issues but none of them knew any way to combat this problem.

6.1.2 Skepticism of a technical solution

We asked participants if they would want to have some technical solution that would help to preserve the privacy of their personal data during the repair process. 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 around the usability of the software, describing how the application would help them to preserve their privacy during the repair process 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 also asked them about other potential mechanisms related to data encryption. It is worth noting that most of our participants were not familiar with these technical terms and so we also had to explain to them how encryption worked, and we encountered a range of arguments and concerns against encryption mechanisms. Most participants said that they shared passwords, screen-locking keys, and other credentials with the repairers so that the repairers would be able to operate the phone as necessary. All participants said that their email and social media applications remained logged in at all times. So, they did not see how encryption could help them. In addition, most of our participants did not use external memory cards so the strategy of taking out the memory card was not helpful for them either.

6.1.3 Challenges around law and policy

Next, we asked participants if they would support imposing laws and/or policies for preserving the privacy of personal data during the repair process. 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 of our participants vetoed this idea. We found that there were two primary reasons for their disagreement. First, all of our participants said that they would not be comfortable 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 of our participants were skeptical that it would be possible to implement such laws or policies in Dhaka. Several participants highlighted the weakness of law enforcement agencies in Bangladesh, while others pointed out their familiarity with police corruption and said it was common for the police to silently support the perpetrators.

6.1.4 Trust, religion, and cultural values

When we asked our 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 given around 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 and therefore 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 also emphasized a need to teach the repairers about social, cultural, and religious values. However, one senior and educated repairer blamed the inflow of uneducated or 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."*

7. DISCUSSION

This section synthesizes our findings into a number of key takeaways. Due to the limited number of participants, we cannot draw any generalized conclusion from our studies. In addition, our interview population was limited to university students that do not represent the entire Bangladeshi population. Despite these limitations, we present the results of our study as the first step in a larger research agenda that aims to better understand privacy in repair and we hope that our work will open up future scholarly discussions and initiate new research directions.

The findings presented in previous sections from our ethnography and interviews point out a number of important concerns around privacy in repair. First, following the notion of privacy as contextual integrity given by Nissenbaum [20], we have obtained a local interpretation of privacy threats through our interviews. The responses of our participants clearly demonstrate that privacy is threatened at repair workshops. Our investigation also reveals that people often lack the proper technical knowledge to combat such privacy threats and this often results in frustration, anxiety, and even non-use of technologies and/or the repair ecosystem. For some customers, concerns about privacy constitute a threat large enough to prevent them from being willing to get their electronic devices repaired in the market. As a result, we identify the problem of privacy in repair as a critical challenge for a country like Bangladesh, where repair ecosystems have been found to have the potential for being an alternate venue of development.

Second, we reveal that technical interventions are not necessarily appropriate solutions to privacy related problems in the context of mobile phone repairing in Bangladesh. Our study has shown that people are skeptical about encryption-based solutions and that they believe tech-based solutions will not work in Bangladeshi contexts, both because of the practice of sharing passwords with the repairers and for the desire to avoid tech-heavy solutions. Our design probe software, *Protiraksha,* further revealed that some participants did not want to appear to be untrusting of the repairers (and others) by installing and/or using the software. Those participants that did react favorably to the software liked *Protiraksha* because of its silent mode of operation and its potential to work in a variety of settings in addition to repair.

Third, our study reveals a number of challenges associated with designing laws and policies to be imposed upon the repair process, with participants expressing hesitation around reporting 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 were reluctant or unwilling to report sexual harassment [1]. The barriers and limitations that affect both technical and policy-based interventions create new challenges for the privacy of mobile repair in Dhaka. Most existing privacy-related design interventions depend heavily on these two ideas - designing new technologies or creating new policies – but our study suggests a need for new, innovative approaches that are able to overcome these limitations.

Fourth, our study indicates that possible solutions to the problem of preserving privacy in repair could come from leveraging the religious and cultural values of Bangladeshi society. Almost all of our participants expressed that the repairers needed to be taught with proper moral education in addition to their technical lessons. Participants frequently mentioned how the fear of God could prevent a repairer from accessing information stored on customers' broken devices. On the other hand, many repairers said that they considered ethical practices to be a part of good repairing. For them, doing anything that might breach customers' privacy would be bad for the repairing community. Both of these conceptualizations indicate that there are both religious and cultural values that affect the privacy in repair ecosystem and that, even without technical and/or policy measures, could help to prevent privacy breaches.

However, the problem of privacy breaches continues to be well known among repairer communities, which indicates that there are still a number of unethical repairers that are not affected by the social or cultural values of the community. Our participants suggested teaching moral values to the repairers as a solution to this problem. Although we support this idea as a long-term strategy to mitigate the problem of maintaining privacy in repair, we also believe that there are opportunities for designing technologies that try to motivate repairers to engage in ethical practices. For example, connecting repairers with wider communities through social media might create a social obligation to engage in ethical repair practices. Similarly, designing systems that reward repairers for being honest and respectful towards customers' personal data may help to preserve customer privacy.

Beyond these immediate implications, our study also opens up opportunities to think about privacy in a wider context and its connection with development. The privacy vulnerability that is associated with information and communication technologies has not yet been extensively researched, particularly when technologies are deployed in developmental contexts. In addition, the transfer of technologies from the global North to the global South also carries the threats associated with of privacy in the developing world. For example, in post-colonial literature the transfer of technology has been seen as a major conveyor of cultural imperialism through technical means [10]. Since privacy is culturally situated in a place, it becomes vulnerable when foreign practices of interaction intrude into the community through technologies. In the western world, privacy vulnerabilities are often combated through technical and/or policy level solutions, both of which may prove to be much weaker in developing countries like Bangladesh. Our study contributes to post-colonial computing literature by highlighting new challenges associated with the transfer of western technologies to developing countries that may have different social or cultural values.

Finally, another important takeaway from our study is to highlight the value of broken technologies. Unlike many developed countries, many populations in developing countries cannot afford to simply discard their broken digital devices. The consumerist attitude of the western world and the related practices around technologies are often inappropriate for the contexts experienced in many developing countries. As a result, repairing broken digital technologies actually constitutes a large portion of the activities associated with digital ecosystems in many developing countries. Our findings reveal that there are important challenges associated with digital repair practices that have not yet been adequately addressed or studied in ICTD research. Moreover, we highlight opportunities for future research that aims to both understand the challenges associated with privacy in repair as well as create innovative new solutions that further strengthen ecosystems around repairing, repurposing, and recycling in ICTD contexts.

8. CONCLUSION

This paper examines the 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 a number of privacy threats through a series of vignettes that highlight the nature and complexity of the problems surrounding privacy in repair. Next we described the challenges associated with designing technologies and creating new laws/policies to combat privacy threats in repair communities in Bangladesh. Our study reveals a number of broad social and cultural tensions that surround privacy in repair and opens up opportunities for designing technologies and/or creating new policies to address those challenges. Beyond its direct contribution to the topic of privacy, this paper joins a growing literature around post-use cycles of technology in ICTD and HCI by revealing a variety of social and cultural values that shape human activities while interacting with technologies in their post-use phases.

9. REFERENCES

[1] Ahmed, S.I., Jackson, S.J., Ahmed, N., Ferdous, H.S., Rifat, M.R., Rizvi, A.S.M., Ahmed, S. and Mansur, R.S. 2014. Protibadi: A Platform for Fighting Sexual Harassment in Urban Bangladesh. *In Proc. CHI'14* (2014), 2695–2704.

[2] Ahmed, S.I., Jackson, S.J. and Rifat, M.R. 2015. Learning to fix: knowledge, collaboration and mobile phone repair in Dhaka, Bangladesh. *In Proc. ICTD'15* (2015), 4:1–4:10.

[3] Annas, G.J. 2003. HIPAA regulations-a new era of medical-record privacy? *New England Journal of Medicine*. 138, 15 (2003), 1486–1490.

[4] Chiasson, S., van Oorschot, P.C. and Biddle, R. 2007. Graphical password authentication using cued click points. *In Proc. Computer Security-ESORICS* (2007), 359–374.

[5] Chirumamilla, P. and Pal, J. Play and power: A ludic design proposal for ICTD. *In Proc. ICTD'13* 25–33.

[6] Cranor, L.F. and Garfinkel, S. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE Security & Privacy*. 2, 5 (2004), 16–18.

[7] Diffie, W. and Hellman, M.E. 1976. New directions in cryptography. *IEEE Transaction on Information Theory*. 22, 6 (1976), 644–654.

[8] Gross, R. and Acquisti, A. 2005. Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (2005), 71–80.

[9] Houston, L. 2014. *Inventive Infrastructure: An Exploration of Mobile Phone.* Lancaster University.

[10] Irani, L., Vertesi, J., Dourish, P., Philip, K. and Grinter, R.E. Postcolonial computing: a lens on design and development. *In Proc. CHI'10* 1311–1320.

[11] Jackson, S.J. 2013. Rethinking Repair. *Media Meets Technology: Essays on Communication, Materiality and Society*. T. Gillespie, P. Boczkowski, and K. Foot, eds. MIT Press.

[12] Jackson, S.J., Ahmed, S.I. and Rifat, M.R. 2014. Learning, innovation, and sustainability among mobile phone repairers in Dhaka, Bangladesh. *In Proc. DIS'14* (2014), 905–914.

[13] Jackson, S.J. and Kang, L. 2014. Breakdown, Obsolescence, and Reuse: HCI and the Art of Repair. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Forthcoming, 2014).

[14] Jackson, S.J., Pompe, A. and Krieshok, G. 2012. Repair worlds: maintenance, repair, and ICT for development in rural Namibia. *In Proc. CSCW'12* (2012), 107–116.

[15] Jackson, S.J., Pompe, A. and Krieshok, G. 2011. Things fall apart: maintenance, repair, and technology for education initiatives in rural Namibia. *Proceedings of the 2011 iConference* (2011), 83–90.

[16] Kumaraguru, P. and Cranor, L.F. 2006. Privacy in India: Attitudes and awareness. *Privacy Enhancing Technologies*. (2006), 243–258.

[17] Lepawsky, J. and Mather, C. 2011. From beginnings and endings to boundaries and edges: rethinking circulation and exchange through electronic waste. *Area*. 43, 3 (2011), 242–249.

[18] Lipford, H.R., Hull, G., Latulipe, C., Besmer, A. and Watson, J. Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. *In Computational Science and Engineering, 2009. CSE'09. International Conference* 985–989.

[19] Mao, W. 2003. *Modern cryptography: theory and practice*. Prentice Hall Professional Technical References.

[20] Nissenbaum, H. 2004. Privacy as contextual integrity. 79, 1 (2004).

[21] O'Donnell, M.L. 2002. FERPA: Only a piece of the privacy puzzle. *JC & UL*. 29, (2002), 679.

[22] Orr, J.E. 1996. *Talking about machines: An ethnography of a modern job*. Cornell University Press.

[23] Palen, L. and Dourish, P. 2003. Unpacking privacy for a networked world. *In Proc. CHI'03* (2003), 129–136.

[24] Raleigh, W.J. 1988. Attorney-Client Privileges. *Barrister*. 15, (1988), 49.

[25] Sadeh, N., Hong, J., Cranor, L.F., Fette, I., Kelley, P., Prabakar, M. and Rao, J. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*. 13, 6 (2009), 401–412.

[26] Sen, A. 1999. *Development as freedom.* Oxford University Press.

[27] Shannon, C.E. 2001. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*. 5, 1 (2001), 3–55.

[28] Suchman, L. 2007. *Human-machine reconfigurations: Plans and situated actions*. Cambridge University Press.

[29] Warren, S.D. and Brandeis, L.D. 1890. The right to privacy. *Harvard Law Review*. (1890), 193–220.

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

[31] Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., Schnellmann, M. and Böni, H. 2005. Global perspectives on e-waste. *Environmental impact assesment review*. 25, 5 (2005), 436–458.

[32] Zurco, M.E. and Simson, R.T. 1996. User-centered security. *In Proceedings of the 1996 workshop on New security paradigms* (1996), 27–33.

[33] 2015. Child pornography found during laptop repair leads to arrest, charges. *CTV News Winnipeg http://winnipeg.ctvnews.ca/child-pornography-found-during-laptop-repair-leads-to-arrest-charges-1.2548589*.

[34] Encrypt or decrypt a folder or file. *Microsoft http://windows.microsoft.com/en-us/windows/encrypt-decrypt-folder-file#1TC=windows-7*.