

# POSTER: Privacy Concerns in Repairing

Syed Ishtiaque Ahmed

Department of Information Science  
Cornell University  
Ithaca, NY 14850  
sa738@cornell.edu

Shion Guha

Department of Information Science  
Cornell University  
Ithaca, NY 14850  
sg648@cornell.edu

Md. Rashidujjaman Rifat

Computer Science & Engineering  
BUET  
Dhaka -1000, Bangladesh  
ne.rifat@gmail.com

## 1. INTRODUCTION

Storing private data in personal electronic devices such as: mobile phone, laptop, or digital camera, is a common practice in many places of the world. These electronic devices often start causing troubles, lose efficiency, or break down due to physical injury, wear and tear, and some other reasons. A highly prevalent practice with broken electronic devices is to fix the problem with the help of a repairer. In many cases, the repairer gets the full access of the digital contents stored in those devices. We identify this as a potential spot where privacy of personal data is vulnerable.

The scholarship in computing technologies and electronic devices is mostly centered on design and development. The studies of Human-Computer Interaction have significantly contributed to the literature by bringing in lessons on how people as an individual or as a community interact with these computing systems. However, their interests hardly crossed the boundary defined by use and design. Hence, historically study and research regarding electronic devices have always asked question around the functional state of a device. But human encounter with technology lasts long after the breakdown of an electronic artifact through a series of actions including repairing, repurposing, and recycling. Many core interests of computing, HCI, and usable security and privacy communities lie in the ways digital contents are taken care of after the breakdown of their hosting architecture. However, this area has not got much attention in literature.

Recently, Jackson turned our attention toward this broken side of the world in his article “Rethinking Repair” [5], and allowed us to think about technology keeping breakdown as the pivotal point. A recent body of literature focused on the electronic repairing practices in different countries including the studies on the global and local network infrastructure of the repairing in rural Namibia [6], and art, craft, innovation and collaboration in repairing works in Kampala, Uganda [4]. However, not much has been studied on how the privacy and security of the digital contents are dealt with in repairer communities.

In a broad sense, privacy in repair communities can be thought of as a transactional and submission process where a specific commodity or information type is relinquished to a specialized agent for a particular kind of labor or advice. 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. In medicine, there exists confidentiality between doctors and their patients. In the United States, medical advice and information is regarded as private information 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 under common law, cannot be disclosed to the public except under very

narrow circumstances [9]. Again, in the realm of higher education, the FERPA [2] manages and protects the education records of students, which are respected as private information by United States federal law. However, there do not seem to be any such protections afforded to repairer-user negotiations. Previous usable privacy research has shown that not only are people concerned about mobile data privacy [1] but that, they feel embarrassed, deceived and regretful after disclosures or violations of mobile phone generated data [8]. This has shown to have impacts on mental and social health of users [7]. In light of similar, potentially harmful disclosures also occurring in the repairer-user communities, we hold that this issue is unexplored and relevant and therefore, also potentially ripe for investigation.

This paper sets up a discussion around the privacy and security of digital data after the breakdown of digital artifacts based on an initial ethnographic fieldwork in Dhaka, Bangladesh and a follow-up online survey.

## 2. OUR STUDY

Our study is broadly divided into two phases. In the first phase, we conducted a 4 months long ethnography in Dhaka, Bangladesh studying the IT repair practices. This included 58 semi-formal interviews of repair workers, repair shop owners, customers in repair shops, e-waste collectors, and novice apprentices. This also included 70 case studies of repairing tasks at 10 repair sites, taking a one-month long training of repairing, and participatory observation of repairing tasks in a repair shop. The interviews were taken in Bangla and then transcribed and translated by native Bangla speakers. This study also produced several hundred pages of field notes, more than 1000 photos, and 10 videos.

This preliminary level of study informed us about this potential privacy threats through the observational data of three common practices. First, the customers leave their device at the repair shops for more than one week. During this period of time, the repairers have the full access to all the contents stored in those devices. Second, a common practice among the repairers is to hand the device they are working on to other repairers either for teaching, or for seeking help. Third, the customers do not ask many questions about the privacy of their personal data either when they hand the device to the repairers, or when they get that back. Although, no case of private data intrusion was observed during our field study, these observations sparked the question around potential threats of personal data privacy during repairing. A further investigation discovered a number of CD/DVD shops close to two of the major repair sites we studied, which would sell private videos captured with the cameras of mobile phones. Couple of shopkeepers there informed us that they had received many of those videos from the local mobile phone repairers.

This led us to the second phase of our investigation where a questionnaire on repair and privacy was made and circulated in

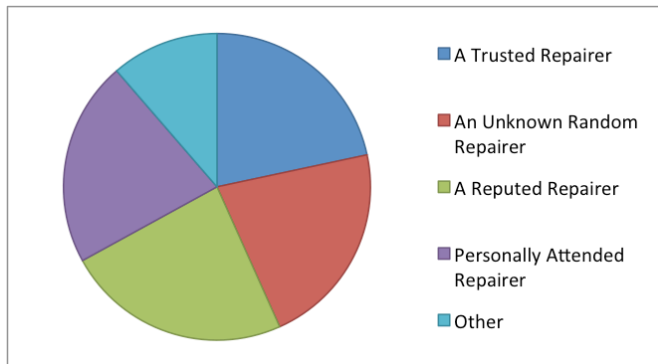
the Facebook groups of the universities of Bangladesh. Since a major part of both the early adopters of technology, and technology consumers of Bangladesh, is coming from this population, we used this as a probe to understand the public reaction to this issue. Both current university students and alumni participated in this study.



**Figure 1: Repairers fixing mobile phones in Gulistan, Dhaka**

Among 48 participants (33 male, 15 female), 37 were students, 7 had official jobs, and 3 owned business. 87% of them fell into the age range 20-30 and 11% were below 20 years.

The result of the survey told us interesting stories around repair and privacy. Laptops, Desktops, and Mobile Phones were the three main electronic devices that they brought to the repairers for fixing. 42% of their personal data were in image files, 19% of those were in text files, and 16% of those were video files. While choosing the repairer, some (21%) preferred a trusted friend, some (21%) chose a reputed repairer, some (23%) did not mind to go to a totally unknown repairer, some (21%) attended the repairer all through the repairing, and the rests adopted some other means (Figure 2).



**Figure 2: Repairer selection strategies**

Almost half of our participants (46%) suspected that their private data had been accessed during the repairing process, and 5 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 while we were visiting a place in a group. He kept on looking at those pictures. Although the pictures were very typical "tour pics" kind, 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."*

Besides sharing their frustration regarding this issue, the participants also made a number of suggestions regarding how to protect privacy in repairing. Those suggestions included the locking of personal data with authentication, online storage and monitoring, surveillance over the repairers, etc.

### 3. FUTURE DIRECTIONS

The results of our study indicate the prevalence of the tension between repair and privacy. This calls for further investigation to get the deeper insight of this issue. Design interventions can be introduced to help users protect their privacy at immediate level. However, policy implications may become necessary to introduce the ethical practice of repairing through education and social awareness. This is a work-in-progress and here, we have only summarized our initial impressions. We hope to report on the results of further research in the near future.

### 4. REFERENCES

- [1] Chin, E., Felt, A.P, Sekar, V., and Wagner, D. 2012. Measuring user confidence in smartphone security and privacy. In Proceeding of Symposium On Usable Privacy and Security SOUPS'12. ACM, New York, NY, USA, Article 1, 16 pages. DOI= <http://doi.acm.org/10.1145/2335356.2335358>
- [2] Family Educational Rights and Privacy Act.1974. Stat. 20 USC.1232g.
- [3] Health Insurance Portability and Accountability Act 1996. Pub.L.104-191.Stat.1936.
- [4] Houston, L. 2014. Inventive Infrastructure: An Exploration of Mobile Phone. PhD Thesis, Lancaster University.
- [5] Jackson, S. J. 2013. Rethinking Repair. In T. Gillespie, P. Boczkowski and K. Foot, eds., Media Meets Technology: Essays on Communication, Materiality and Society. MIT Press.
- [6] Jackson, S.J., Pompe, A., and Krieschok, G. 2012. Repair worlds: maintenance, repair, and ICT for development in rural Namibia. In Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW'12), ACM (2012), 107–116. ACM, New York, NY, USA, 107-116. DOI= <http://doi.acm.org/10.1145/2145204.2145224>
- [7] Nissenbaum, H. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto, CA. Stanford University Press.
- [8] Patil, S, Norcie, G, Kapadia, A, Lee, A.J. 2012. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In Proceeding of ACM Symposium on Usable Privacy and Security (SOUPS '12). ACM, New York, NY, USA, Article 5 , 15 pages. DOI= <http://doi.acm.org/10.1145/2335356.2335363>
- [9] Watson, Andrew S. Lawyer as Counselor. The Journal of Family law. Volume: 5, Issue: 7, 1965.