7-3-2021

Understanding User Behavior, Information Exposure, and Privacy Risks in Managing Old Devices

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

Tanjina Tamanna
University of Dhaka, turnatatatu666@gmail.com

Swapnil Nandy
Jadavpur University, swapnilnandy2@gmail.com

Huzeyfe Kocabas
Utah State University, huzeyfe.kocabas@aggiemail.usu.edu

Recommended Citation

Al-Ameen M.N., Tamanna T., Nandy S., Kocabas H. (2021) Understanding User Behavior, Information Exposure, and Privacy Risks in Managing Old Devices. In: Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2021. Lecture Notes in Computer Science, vol 12788. Springer, Cham. https://doi.org/10.1007/978-3-030-77392-2_18

Understanding User Behavior, Information Exposure, and Privacy Risks in Managing Old Devices

Mahdi Nasrullah Al-Ameen[1], Tanjina Tamanna[2], Swapnil Nandy[3], and Huzeyfe Kocabas[1]

[1] Utah State University, USA
[2] University of Dhaka, Bangladesh
[3] Jadavpur University, India
mahdi.al-ameen@usu.edu, turnatatatu666@gmail.com, swapnilnandy2@gmail.com, huzeyfe.kocabas@aggiemail.usu.edu

Abstract. The goal of this study is to understand the behavior of users from developing countries in managing an old device (e.g., computer, mobile phone), which has been replaced by a new device, or suffers from technical issues providing a notion that it may stop working soon. The prior work explored the ecology and challenges of repairing old devices in developing regions. However, it is still understudied how the strategies of people from developing countries in managing their personal information on old devices could impact their digital privacy. To address this gap in existing literature, we conducted semi-structured interview with 52 participants, including 37 participants living in two developing countries (e.g., Bangladesh, Turkey) and 15 first-generation immigrants from developing regions living in the USA. We found that users leave sensitive information, and online accounts logged in while they give away or sell their old devices. All of our immigrant participants in the USA keep backup of their personal data from an old device, however, some of them store that information in an unprotected medium. Instead of keeping backup, the participants living in Bangladesh and Turkey often keep the old device as a digital storage, or give away to someone where their right to access their information would be preserved. Based on our findings, we unpacked the relation between trust and privacy in managing old devices.

Keywords: Old Device · Privacy Risks · Qualitative Study

1 Introduction

People use a wide-range of digital devices for communication, information storage, entertainment, and utility in everyday life. In this paper, the term: *'device'*

The article is published in HCII 2021. This is the author's copy of the accepted version. The final authenticated version is available online at https://doi.org/10.1007/978-3-030-77392-2_18

refers to a mobile phone or computer/laptop, unless otherwise specified. In general, users purchase a new device once their current device stops working, or they identify any technical issue realizing that their device may stop working in the near future. They also purchase a new device to avail the state-of-art amenities. Here, we do not consider how long a device has been used by a user to denote it as an *old device*, rather for simplicity, any device that a user has replaced by a new device, or a device that suffers from technical issue showing a notion that it may stop working in the near future, is noted as an old device.

The study on sustainability [10] highlighted the importance of rethinking design to encourage the choice of supporting maintenance of old devices over decisions to discard and replace them. The prior study [22] showed that people in developing countries reuse their old devices through availing the repair services, where Jackson et al. [24] studied the importance and challenges of repairing an old device in the context of Bangladesh, a country in South Asia. The study of Ahmed et al. [2] unfolded the privacy risks of users in the Global South when they leave their mobile phones with repairers to fix the technical issues. In another work, Jang et al. [25] explored the privacy implications of user's trust on the repairers in a remote area at rural Philippines.

While prior studies examined the ecology and challenges of repairing old devices in developing countries, there is a dearth in existing literature to understand the privacy implications of users' behavior with managing their information in old devices. We addressed this gap in our work through investigating the following research questions: i) How do users manage their information once they identify that an old device may stop working in the near future? ii) How do users manage an old device and the information stored in it once they get a new device? iii) What are the privacy and security implications of users' strategies of managing their old devices and the information stored in those devices?

According to the recent studies [7,20,41], privacy is contextual that demands a situated understanding of users' perceptions and behavior in order to explore the design and policy practices. In this paper, we focused on the participants who currently live in a developing country (e.g., Bangladesh, Turkey) or are the immigrants from developing regions living in a developed country (e.g., USA). In particular, we interviewed 52 participants; 29 of them (denoted by *BP*) live in Bangladesh, eight of them (denoted by *TP*) live in Turkey, and 15 participants (denoted by *IP*) are first-generation immigrants in the USA who are originally from the developing countries located in different continents, including Bangladesh (located in South Asia), Turkey (a country straddling Eastern Europe and Western Asia), Bolivia (located in central South America), Nigeria (located in West Africa), and Pakistan (located in South Asia).

Our results unfold the strategies of participants in managing their information in an old device. All of our immigrant participants in the USA keep backup of their personal data from an old device, however, they often fail to understand the requirements and strategies for secure backup, and thus, end up with storing information and credentials in an unprotected medium. On the other hand, the participants living in Bangladesh and Turkey often keep the old device as a digi-

tal storage, or give away to someone where their right to access their information would be preserved. We identified the rationals behind users' choice of mediums to keep backup of information from their old devices, and discussed how these strategies could expose them to privacy risks due to their misconceptions, lack of technical efficacy, and dependency on caregivers.

We reported the unexpected incidents of information loss and exposure in the process of managing old devices. We found that users leave sensitive information (e.g., bank account number), and important online accounts logged in while they give away or sell their old device; in these contexts, our analysis unpacked how user's behavior is related to their situated trust on peers, risk perceptions, and the awareness of existing controls offered by a device. Taken together, our findings have important implications to advance the HCI and Privacy community's understanding of user behavior and corresponding privacy risks in managing old devices.

2 Related Work

In this section, we briefly describe the findings from notable prior studies on user's security and privacy behavior, followed by a discussion on existing literature in the context of situated privacy and security.

The study of Wash [43] identified eight 'folk models' of threat in the context of hackers and computer viruses – used by people in deciding which security software to use on their home computer. The findings from this study [43] shed light on how the users exploit these models to justify their insecure behavior in computing environment. In another study [23], Ion et. al. compared the online security practices of expert and non-expert users, where they found differences in their security behavior. For instances, expert users generally install updates, use password manager, and leverage two-factor authentication, where the non-expert users prefer to use antivirus application, change their passwords, and visit only the known websites [23].

The study of Ruoti et. al. [35] found that users' security behavior depend upon their understanding of a threat, evaluation of risks, and the estimation of impact, where they select coping strategies based on their evaluation of the trade-offs between potential harms and the costs to take protective measures. As reported by Habib et al. [19], users' motivations behind using private browsing mode could extend beyond the privacy reasons, e.g., to address their practical and security needs. People have certain misconceptions about private browsing mode, where they are found to overestimate the protection guarantee offered by private browsing mode, especially from online tracking and targeted advertising [19].

The study of Nthala et al. [32] identified a wide-range of security practices that exist when people ask for help from their social circles to address the security issues on their digital devices, where the survival or outcome bias, and availability and quality of security support impact people's security decisions in a home environment. Zou et. al. [44] focused on Equifax data breach, where the findings

revealed users' perceived risks of data leakage. The authors [44] identified the factors that could influence users towards not taking a protective measure, which include but not limited to the optimism bias, procrastination until harms occur, and the costs of taking a security-preserving action. In a separate study [18], Frik et al. found uncertainty among older adults about the information flow, and data persistence, which lead them to rely on ineffective security protection techniques. The authors [18] also revealed the privacy and security misconceptions of older adults, for example, they tend to think that a user who has nothing to hide, does not need to protect her digital privacy.

2.1 Situated Privacy and Security

Privacy is contextual that demands a situated understanding of users' perceptions and behavior in order to explore the design and policy practices [30,33,15]. The findings from recent usable privacy studies [7,3,13] support this argument that local values often contrast with the liberal notions of privacy embedded in current computing systems. However, the digital privacy research beyond Western contexts and a liberal framing is still at its very early stage [14,42]. Below, we briefly discuss the notable usable privacy studies conducted outside the Western contexts.

Although online threats are global, perceptions of threat are very localized [7,20,26,13]. The study of Al-Ameen et al. [7] explored how the privacy perceptions of people relate to their effort to deal with the issues of urbanization and the opportunities that come with digitization in the Global South. The authors [7] examined how users balance their needs, conveniences, and privacy in the context of data collection and sharing by apps, and unveiled how privacy leakage incidents affect app usage behavior. The study of Haque et al. [20] presented how clientelization, reputation, and situated morality influence the privacy behavior of people in the digital service centers at Bangladesh. In another study [13], Chen et al. investigated the security and privacy practices of the people in urban Ghana while browsing Internet. The study [13] shows that participants judge the trustworthiness of a website based on the appearance, lack of popups, and loading speed, where they reported confidence of being able to defend against cyberattacks despite passwords often being their only line of defense.

The religious views and cultural norms of people have impacts on their sense of confidentiality and privacy. The study of Alghamdi et al. [8] investigated the privacy and security practices for households bank customers in Saudi Arabia, showing that trust, driving restrictions, and the esteem placed in family motivate female participants to share their banking information with male family members, including their father, and husband. The study of Abokhodair et al. [1] examined how the youth in the middle east conceptualize values such as privacy, intimacy, and freedom of expression in the context of social media. The authors [1] found that the interpretation of privacy among participants goes beyond the concerns for security, safety, and having a control to separate oneself

from a larger group, where they observed adherence to Islamic teachings, maintenance of reputation, and the careful navigation of activity in social media to preserve respect and modesty.

Digital harassment is a growing concern in many developing countries, wherein the majority of cases, female users are the victims of such incidents [31,6]. The study of Nova et al. [31] reveals the online harassment that women in Bangladesh encounter while using anonymous social media (ASM). Participants reported receiving sexually offensive messages and dating inquiries from the people in ASM. While public discussion on sex or any topic containing sexual content are considered taboo and frowned upon in Bangladesh [34,29], the curtain of anonymity in ASM provides a safer way to break these invisible norms of society without being judged or scrutinized. In another study, Sambasivan et al. [38] identified that the risks and fear of harassment refrained the women in urban India to provide their phone number for accessing public Wi-Fi services.

Digital devices, such as mobile phones that are designed for developing regions often fail to satisfy their local needs. In a study conducted with low-literate Berber women in Morocco [16], the authors examined the gap between high rates of mobile phone ownership and low use of productive features - noted as 'mobile utility gap'. The study identified that lack of functional literacy and non-standard mobile phone interface including a complex language environment with both Arabic and Berber dialects presented significant barriers to using mobile phones, which contributed to the mobile utility gap in that community. The studies conducted by Ahmed et al. [4] and Sambasivan et al. [37] demonstrate that the mobile phones often do not have one-to-one mapping with a user in the resource-constrained settings of developing countries, while the social fabric in these societies is based on the notions of trust and collectivism. Thus, the strict privacy requirements in using digital technology could disrupt the relationships with friends and family members [4,37]. In a separate study with women in Global South [36], the authors explored the privacy negotiation of female users from their family members while using a mobile phone.

Our Study. The overall findings from these studies indicate that the misconceptions about local culture by developers or designers may result in inappropriate threat modeling, where there is a dearth in existing literature to understand the behavior of users from developing countries in managing old devices. We addressed this gap in our work through investigating how users manage their old device and the information stored in it once they identify that their device may stop working in the near future or once they get a new device, where we identified the privacy implications of users' strategies in managing their old devices.

3 Methodology

We conducted semi-structured interview (audio-recorded) with 52 participants. We recruited participants through sharing the study information via email and online social media, posting flyers on public places, snowball sampling, and leveraging authors' personal connections. We interviewed the participants over tele-

Gender	**Participants**
Male	BP1-BP3, BP6-BP9, BP11, BP15, BP17-BP29, IP1-IP4, IP7, IP8, IP9-IP11, IP13, IP14, IP15, TP1, TP3, TP4, TP6, TP8
Female	BP4, BP5, BP10, BP12-BP14, BP16, IP5, IP6, IP12, TP2, TP5, TP7
Age-range	
18-24	BP4, BP7, BP8, IP5, IP6, IP15
25-29	BP2, BP3, BP5, BP6, BP9, BP19, BP20, BP25, IP2, IP7-IP14, TP1-TP3
30-34	BP1, BP17, BP18, BP21, BP24, BP28, IP1, IP3
35-39	BP23, TP6
40-44	BP16, BP22, BP26, BP27, BP29, IP4
45-49	BP14, TP4, TP7
50-54	BP15, TP5, TP8
55+	BP10, BP11, BP12, BP13
Literacy Level*	
Fifth Grade	BP19, BP27, BP29, TP6, TP7
Between Eighth and Tenth Grade	BP17, BP20, BP22, BP24, BP25, BP26, BP28, TP4
Twelfth Grade	BP12, BP18, BP21, BP23, IP15, TP2, TP5, TP8
Undergraduate and above	BP1-BP11, BP13-BP16, IP1-IP14, TP1, TP3
Profession	
Student	BP4, BP5, BP7, BP9, IP1-IP3, IP6-IP13, IP15
Employee at Industry	BP1-BP3, BP6, BP8, BP11, BP17-BP19, BP21-BP29, IP5, TP3, TP4, TP6
Employee at Educational or Non-profit Org.	BP10, BP15, IP4, IP14 TP1
Car Driver	BP20
Housewife	BP12-BP14, TP2, TP5, TP7
Physician	BP16
Retired	TP8

Table 1. The Highlight of Participants' Demographic Traits [*Either completed or currently studying at the noted education level]. **Note:** *IP*: Immigrant participants living in the USA; *BP*: Participants living in Bangladesh; *TP*: Participants living in Turkey

phone, via Skype, or in person. The study was approved by the Institutional Review Board at our university.

During interview, we asked participants about how they manage their information when they identify that an old device may stop working in the near future, and how they manage an old device and the information stored in it once they get a new one. Then they were asked about their experiences of dealing with old devices that they had purchased or received as gifts, and the past incidents of information loss and privacy breach in the process of managing old

devices. At the end, participants answered a set of demographic questionnaire. On average, each session took between 20 and 30 minutes.

The interview was audio recorded. We transcribed the audio recordings at the end of data collection. We conducted the interview in English with the immigrant participants living in the USA. For the participants living in Bangladesh and Turkey, the authors of this paper who are originally from these countries conducted the interview in their local language (e.g., Bengali, Turkish), and translated the transcriptions into English.

We performed thematic analysis on our transcriptions [11,12]. Two researchers independently read through the transcripts of half of the interviews, developed codes, compared them, and then iterated again with more interviews until we had developed a consistent codebook. Once the codebook was finalized, two researchers divided up the remaining interviews and coded them. After all interviews had been coded, both researchers spot-checked the other's coded transcripts and did not find any inconsistencies. Finally, we organized and taxonomized our codes into higher-level categories.

Participants. Among our 52 participants, 13 of them are women, and 39 are men. Table 1 presents their demographic information. Most of our participants were in the age range of 18 to 55, where four participants were above 55 years old. 60% of our participants were either undergraduate students or had already earned the degree, where the literacy level of other participants were between fifth and twelfth grade. 31% of our participants were students, where others were from diverse professions, including physician, car driver, housewife, and the employee at industry, educational institution, or non-profit organization.

4 Results

In this section, we report the findings from our study. We used following terms to represent the frequency of comments in participants' responses: *a few* (0-10%), *several* (10-25%), *some* (25-40%), *about half* (40-60%), *most* (60-80%), and *almost all* (80-100%).

4.1 Managing Accessibility to Information

All of our immigrant participants living in the USA have reported that when they identify any technical issue in an old device giving a notion that it may stop working in the near future, they keep backup of at least some of their information. On the other hand, most of the participants living in Bangladesh and Turkey do not keep backup from their old devices.

Participants Who Keep Backup. Among participants who keep backup of their information, most of them use the external hard drive, USB flash drive, or online cloud storage. The participants who prefer local storage (e.g., hard

drive/USB flash drive) to cloud service to keep backup from an old device, emphasized on two reasons behind their preference. First, local storage gives them a sense of security that no one would be able to gain their personal documents without having a physical access to their storage devices. The less-understood security threats (e.g., how an online hacking works [17]) make some participants less comfortable with storing their sensitive information in a cloud storage. Second, several participants reported concern about the internet speed and delays involved in uploading documents to the cloud storage.

A few participants email their important documents to themselves, or use social networking accounts to store photos and information from their old devices. IP19 stores the username and password of her online accounts in a file on her computer. When she identifies any technical issue in her device realizing that it may stop working in the near future, she writes down her authentication secrets on a paper, so that she could later restore that once a new device is purchased.

Participants Who Do Not Keep Backup. Participants who do not keep back up of their information, try to ensure their access to that after purchasing a new device in one of three different ways: i) They keep the old device as a digital storage of their personal documents and information; ii) They give away an old device to someone for use, where their right to access documents (as a previous owner) will be preserved; iii) They directly transfer their documents to the new device.

Our participant, BP11 used to directly transfer his information to a new device from the old one. According to him, *"I am not a technical person and don't know much about transferring documents...While transferring I lost many of my data before. When I was transferring data to my new device somehow these information were missed out and eventually got deleted."* Thus, he now keeps his old device with him (a new one is purchased, too) along with his documents and information stored in it. Several participants, who live in Bangladesh, take help from their family members to directly transfer the documents and photos from the old device to a new one. For instance, BP13 requests her daughter to complete the transfer process for her. Participants also reported taking help from their friends and colleagues (whom they mentioned as 'tech-savvy') to transfer their documents to the new device.

4.2 Privacy Protection Strategies

Our participants reported to handle the old device (once they get a new one) in one of three different ways: they keep the device, give it to a family member or friend as a gift, or sell it. In this section, we present our findings on users' strategies to protect their privacy as they adopt one of these three approaches to manage their old devices.

Keeping Old Devices. As discussed in §4.1, keeping the old device is considered as a potential way to preserve personal information and documents. IP3

commented, *"I have all of my old devices with me. I didn't throw them out because I'm worried about what will happen with my information, my apps that are in that cell phone."* Several participants living in Bangladesh and Turkey keep the old device as a backup one, so that they could use it in case their current device gets broken or lost, where BP5 said, *"If the device can still be used then I keep that as a backup device as long it survives, and if the device is dead then I dump it."* Most of the participants in these two groups who keep the old device as a backup one, or use it to keep their information stored, do not sign out of their online accounts, nor delete any of their information from the device. They keep their old devices in a container, drawer, or under the cabinet at their home with no apparent physical security (e.g., using a physical lock).

A few participants, who live in Bangladesh, mentioned keeping the old device so that their family members could use it for entertainment, where they do not take any steps to protect their privacy while sharing the device. For instance, BP12 said, *"Old devices remain in the house, used by my youngest grandson for playing games. All information remain intact in there. All applications and accounts are logged in."* On the other hand, IP5 worried about the security and privacy risks of giving away or selling an old device. She reported concern that the adversary might find a backdoor to access her information even if she deletes that from her device; she added, *"Right now I just keep all the old devices with me just for security, because I don't know what [else] to do with [an old device]."*

Giving Away Old Devices. Around one-third of our participants reported that they give their old device as a present to their family member or friend. Among them, several participants keep their personal information stored, and the online accounts logged in while giving a device to the recipient. IP14 gives his old laptop to his family member whom he trusts. He is not willing to sell the device as he worried that the information in his device could be exposed to a stranger in that case. Several participants referred to trust as the reason why they did not delete any information from their old smartphone while giving it to their friend or family member. Here, we identified situated trust among participants while giving away their old devices. For instance, IP2 was comfortable with keeping his online accounts logged in while giving his old smartphone as a present to his girlfriend, who, however, would prefer to factory-reset the device if he would give it to any of his other friends.

Several participants living in Bangladesh and Turkey prefer to give the old device to their friend or family member instead of selling it to a stranger, so that they could preserve their right to access their personal information residing in that device, and could retrieve any photos or documents as per their need in the future. The participants in this group did not delete any information from the old device while giving it away for their friend or family member to use. In this context, a few participants intend to keep a balance between having the information stored in their old device while giving it away and protecting that from being exposed to the recipient. Here, TP8 chose to hid his personal information inside his old computer while giving it away, and expressed his belief that the

recipient's technical efficacy would not suffice to retrieve that information from a secret folder in the device.

Several participants reported taking steps to protect their information while giving away their computer or mobile phone for someone else to use. We found instances where participants factory-reset the old device before giving it away, where several other participants mentioned, they had deleted some of their information and documents from the old device depending upon their relationship with the recipient. The perceptions of relations, and so on, the protection strategies varied among participants. For instance, IP12 trusts her siblings with the photos and documents in her smartphone. So, she only signed out of her online accounts and kept other information stored in the phone as she gave it to her sibling.

Selling Old Devices. About one-fifth of our participants reported selling the old device to a previously unknown person (no participant reported selling an old device to someone they already knew, e.g., a friend or family member), where above half of them reported that they had factory-reset their device before handing it over to the buyer. Among other participants who sold their old devices, some of them signed out of their online accounts, but did not delete any of their information, documents, or photos from their devices, where other participants deleted those information only, that they considered would put their privacy into risks if exposed to a stranger. We found that several participants were not aware of the factory-reset option available in their phones.

4.3 Information Loss and Exposure

Participants' Information. Several participants reported unpleasant experiences of information loss and privacy breach from their old devices. A few of our participants who used an old computer to store files and information instead of keeping a backup in an external storage, lost access to their documents when their device stopped working. IP12 lost access to personal documents stored in her old phone that she used to use before she purchased a new phone, as she could no longer recall the password to unlock her old phone.

IP2 did not keep backup of his personal documents stored in his smartphone, when he sent it to the manufacturer for fixing a technical issue. He expected that the device would be returned after a repair, however, instead he received a new device as a replacement. As a result, IP2 lost access to all of his information in that old phone. A few participants living in Bangladesh reported the privacy risks when they avail cost-savvy third-party services to repair their old devices. BP5 reported an incident, where she found that her personal information from her mobile phone was accessed by the repairer without taking her permission.

Others' Information. Above one-third of our participants reported receiving a used device through purchase or as a present from someone they know, where

about half of them found personal information of the previous owner residing in that old computer or mobile phone.

Several participants living in Bangladesh have reported that they are trusted with the information in a device when they receive it as a gift from their family member. BP12 received a smartphone from her husband, where she said, *"Every information of my husband is still in there [smartphone]. He just gave me the device, and all his apps, photos, videos, contact numbers, and messages were in there."* In the case of BP20, participant's family member who gave away her mobile phone, explicitly requested the recipient (BP20) not to delete her personal information residing in that device, so that those information could be accessed by that family member in the future. In some instances, the previous owner puts trust on the recipient to delete their personal information from the device and sign out of their online accounts. BP25 who received a used smartphone from his elder brother, said, *"He [elder brother] showed me the way of resetting the device and following his way, I reset the device and started using it. Before resetting everything was intact in his device which I used for one or two days."*

Our findings indicate that personal information of users may remain in the used mobile phones and computers when those devices are sold. IP2 purchased a smartphone where he found the financial information (e.g., bank account number) of the previous owner. A few participants noticed that the previous owner did not sign out of social networking and communication apps. BP3 said, *"I am using a second-hand laptop, and the laptop contained all the information of the previous owner."* In such instances, participants reported deleting the stored information and signing out of online accounts of the previous owner of the device.

5 Discussion

Security Perceptions and Behavior. The participants living in the USA use different mediums to keep backup of their information from an old device, where a local storage device (e.g., external hard drive, USB flash drive), although not protected by passwords, provides them with a higher sense of security than a password-protected cloud storage service. The physical possession of a local storage device, coupled with participants' uncertainty about the attacker's strategies to steal information from an online server, contributed to their higher comfort level with keeping backup in an external hard drive or USB flash drive. We found instances where participants perceive that if the adversaries get physical access to their old devices, they would manage to find a backdoor to access all of their information including the deleted ones. So, they see no security benefits in deleting personal documents from an old device although it is no longer in use, and prefer to keep the device instead of selling or giving it away, to protect their personal information.

Trust and Privacy. Participants' approach towards information management while giving away an old device depends upon their situated trust on the recip-

ient. In some instances, participants simply believe that the recipient would not access their information, while in other cases, they explicitly ask to delete their information and trust the recipient with doing so. We found that several participants living in Bangladesh and Turkey want to preserve their right to access information in the old device while giving it away to a friend of family member. Their personal information remains stored in that device, and in most cases, they trust the recipient with protecting their information. While prior studies [21,28] revealed the risks of privacy violation and digital abuse when there occurs a change in trust and relationship, we suggest that the future research should further investigate the privacy implications for the previous owner of an old device as their relationship with the recipient of that device changes over time.

Technical (In)Efficacy and Privacy Risks. Due to the lack of technical efficacy, several participants living in Bangladesh take help from others to transfer documents from the old device to a new one. To avail such help, participants need to share their devices with caregivers, which may pose privacy risks to them as shown in prior studies on mobile phone sharing in Bangladesh [36,5]. Our results reveal that users leave sensitive personal information in their old devices while selling, or giving those away. One reason behind such behavior is the unawareness of available features (e.g., factory-reset option in mobile phone) to protect user privacy.

Limitations. In this study, we followed the widely-used method for qualitative research [9,12,11], where we focused in depth on a small number of participants and continued the interviews until no new themes emerged (saturation). We acknowledge the limitations of such study that a different set of samples might yield varying results. Our sample size is not uniformly distributed across geographic regions, or demographic traits. For instance, the age of most of our participants were below 55, where three-fourth of our participants identified as male. Thus, we do not draw any quantitative, generalizable conclusion from this study. In addition, self-reported data might have limitations, like recall and observer bias.

Our study is based in urban areas. We note that users' privacy perceptions might be different in rural areas. Since users' security and privacy perceptions are positively influenced by their knowledge and technical efficacy [23,39,27], and the literacy rate is generally higher in urban areas as compared to that in rural areas [40], we speculate that the privacy perceptions and behavior of users reported in this paper represent an upper bound in the context of managing old devices.

6 Conclusion

Our study unpacked users' strategies of managing information in their old devices, and revealed the underlying privacy risks. Based on our findings, we shed light on users' security and privacy perceptions of storage mediums to keep

backup of information from an old device, identified the relation between trust and privacy, and discussed how the lack of technical efficacy and awareness of available tools and features could expose users' private information in the context of managing old devices. In our future work, we would extend the findings from this study through a large-scale online survey with the participants from diverse demographic traits, backgrounds, and technical efficacy.

References

1. Abokhodair, N., Vieweg, S.: Privacy & social media in the context of the arab gulf. In: Proceedings of the 2016 ACM Conference on Designing Interactive Systems. p. 672–683. DIS '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2901790.2901873
2. Ahmed, S.I., Guha, S., Rifat, M.R., Shezan, F.H., Dell, N.: Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In: Proceedings of the Eighth International Conference on Information and Communication Technologies and Development. pp. 1–10 (2016)
3. Ahmed, S.I., Guha, S., Rifat, M.R., Shezan, F.H., Dell, N.: Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In: Proceedings of the Eighth International Conference on Information and Communication Technologies and Development. pp. 11:1–11:10. ICTD '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2909609.2909661
4. Ahmed, S.I., Haque, M.R., Chen, J., Dell, N.: Digital privacy challenges with shared mobile phone use in bangladesh. Proc. ACM Hum.-Comput. Interact. **1**(CSCW), 17:1–17:20 (Dec 2017). https://doi.org/10.1145/3134652
5. Ahmed, S.I., Haque, M.R., Chen, J., Dell, N.: Digital privacy challenges with shared mobile phone use in bangladesh. Proceedings of the ACM on Human-Computer Interaction **1**(CSCW), 17 (2017)
6. Ahmed, S.I., Jackson, S.J., Ahmed, N., Ferdous, H.S., Rifat, M.R., Rizvi, A., Ahmed, S., Mansur, R.S.: Protibadi: A platform for fighting sexual harassment in urban bangladesh. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. p. 2695–2704. CHI '14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2556288.2557376
7. Al-Ameen, M.N., Tamanna, T., Nandy, S., Ahsan, M.A.M., Chandra, P., Ahmed, S.I.: We don't give a second thought before providing our information: Understanding users' perceptions of information collection by apps in urban bangladesh. In: Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'20). p. 32–43. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3378393.3402244
8. Alghamdi, D., Flechais, I., Jirotka, M.: Security practices for households bank customers in the kingdom of saudi arabia. In: Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security. p. 297–308. SOUPS '15, USENIX Association, USA (2015)
9. Baxter, K., Courage, C., Caine, K.: Understanding Your Users: A Practical Guide to User Research Methods. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2 edn. (2015)
10. Blevis, E.: Sustainable interaction design: invention & disposal, renewal & reuse. In: Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 503–512 (2007)

11. Boyatzis, R.E.: Transforming qualitative information: Thematic analysis and code development. sage, Thousand Oaks, CA, USA (1998)
12. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
13. Chen, J., Paik, M., McCabe, K.: Exploring internet security perceptions and practices in urban ghana. In: Proceedings of the Tenth USENIX Conference on Usable Privacy and Security. p. 129–142. SOUPS '14, USENIX Association, USA (2014)
14. Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., Kohno, T.: Computer security for data collection technologies. Development engineering **3**, 1–11 (2018)
15. Crabtree, A., Tolmie, P., Knight, W.: Repacking 'privacy' for a networked world. Comput. Supported Coop. Work **26**(4-6), 453–488 (Dec 2017). https://doi.org/10.1007/s10606-017-9276-y
16. Dodson, L.L., Sterling, S.R., Bennett, J.K.: Minding the gaps: Cultural, technical and gender-based barriers to mobile use in oral-language berber communities in morocco. In: Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers - Volume 1. p. 79–88. ICTD '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2516604.2516626
17. Florêncio, D., Herley, C., Van Oorschot, P.C.: An administrator's guide to internet password research. In: 28th Large Installation System Administration Conference (LISA14). pp. 44–61 (2014)
18. Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., Egelman, S.: Privacy and security threat models and mitigation strategies of older adults. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (2019)
19. Habib, H., Colnago, J., Gopalakrishnan, V., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L.F.: Away from prying eyes: analyzing usage and understanding of private browsing. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 159–175 (2018)
20. Haque, S.M.T., Haque, M.R., Nandy, S., Chandra, P., Al-Ameen, M.N., Guha, S., Ahmed, S.I.: Privacy vulnerabilities in public digital service centers in dhaka, bangladesh. In: Proceedings of the 2020 International Conference on Information and Communication Technologies and Development. ICTD2020, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3392561.3394642
21. Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., Ristenpart, T.: Clinical computer security for victims of intimate partner violence. In: 28th USENIX Security Symposium. pp. 105–122 (2019)
22. Houston, L., Jackson, S.J., Rosner, D.K., Ahmed, S.I., Young, M., Kang, L.: Values in repair. In: Proceedings of the 2016 CHI conference on human factors in computing systems. pp. 1403–1414 (2016)
23. Ion, I., Reeder, R., Consolvo, S.: "...no one can hack my mind": Comparing expert and non-expert security practices. In: Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security. p. 327–346. SOUPS '15, USENIX Association, USA (2015)
24. Jackson, S.J., Ahmed, S.I., Rifat, M.R.: Learning, innovation, and sustainability among mobile phone repairers in dhaka, bangladesh. In: Proceedings of the 2014 conference on Designing interactive systems. pp. 905–914 (2014)
25. Jang, E.H.B., Garrison, P., Vistal, R.V., Cunanan, M.T.D., Perez, M.T., Martinez, P., Johnson, M.W., Evangelista, J.A., Ahmed, S.I., Dionisio, J., et al.: Trust and

technology repair infrastructures in the remote rural philippines: Navigating urban-rural seams. Proceedings of the ACM on Human-Computer Interaction **3**(CSCW), 1–25 (2019)
26. Kumaraguru, P., Cranor, L.: Privacy in india: Attitudes and awareness. Privacy Enhancing Technologies **3856**, 243–258 (2006)
27. Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R., Ur, B.: Measuring password guessability for an entire university. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. p. 173–186. CCS '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2508859.2516726
28. McCormick, L.: The internet and social media sites: A shift in privacy norms resulting in the exploitation and abuse of adolescents and teens in dating relationships. Alb. Gov't L. Rev. **7**, 591 (2014)
29. Nahar, P., Van Reeuwijk, M., Reis, R.: Contextualising sexual harassment of adolescent girls in bangladesh. Reproductive health matters **21**(41), 78–86 (2013)
30. Nissenbaum, H.: Privacy as contextual integrity. Wash L. Rev **79**, 119 (2004)
31. Nova, F.F., Rifat, M.R., Saha, P., Ahmed, S.I., Guha, S.: Online sexual harassment over anonymous social media in bangladesh. In: Proceedings of the Tenth International Conference on Information and Communication Technologies and Development. pp. 1:1–1:12. ICTD '19, ACM, New York, NY, USA (2019). https://doi.org/10.1145/3287098.3287107
32. Nthala, N., Flechais, I.: Informal support networks: an investigation into home data security practices. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 63–82 (2018)
33. Patrick, A., Kenny, S.: From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In: Privacy Enhancing Technologies. pp. 107–124. Springer, Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
34. Rashid, S.F., Standing, H., Mohiuddin, M., Ahmed, F.M.: Creating a public space and dialogue on sexuality and rights: a case study from bangladesh. Health Research Policy and Systems **9**(1), S12 (2011)
35. Ruoti, S., Monson, T., Wu, J., Zappala, D., Seamons, K.: Weighing context and trade-offs: How suburban adults selected their online security posture. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 211–228 (2017)
36. Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., Consolvo, S., Churchill, E.: "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 127–142. USENIX Association, Baltimore, MD (Aug 2018), `https://www.usenix.org/conference/soups2018/presentation/sambasivan`
37. Sambasivan, N., Rangaswamy, N., Cutrell, E., Nardi, B.: Ubicomp4d: Infrastructure and interaction for international development–the case of urban indian slums. In: Proceedings of the 11th International Conference on Ubiquitous Computing. p. 155–164. UbiComp '09, Association for Computing Machinery, New York, NY, USA (2009). https://doi.org/10.1145/1620545.1620570
38. Sambasivan, N., Weber, J., Cutrell, E.: Designing a phone broadcasting system for urban sex workers in india. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. p. 267–276. CHI '11, Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/1978942.1978980

39. Seng, S., Kocabas, H., Al-Ameen, M.N., Wright, M.: Poster: Understanding user's decision to interact with potential phishing posts on facebook using a vignette study. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 2617–2619. CCS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3363270
40. of Statistics, B.B.: Literacy assessment survey 2008 (Nov 2008), http://www.un-bd.org/Docs/Publication/Bangladesh_Literacy_Assessment_Survey_2008.pdf
41. Sultana, S., Saha, P., Hasan, S., Alam, S.M.R., Akter, R., Islam, M.M., Arnob, R.I., Al-Ameen, M.N., Ahmed, S.I.: Understanding the sensibility of social media use and privacy with bangladeshi facebook group users. In: Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'20). p. 317–318. Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3378393.3402235
42. Vashistha, A., Anderson, R., Mare, S.: Examining security and privacy research in developing regions. In: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS'18). COMPASS'18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3209811.3209818
43. Wash, R.: Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. pp. 1–16 (2010)
44. Zou, Y., Mhaidli, A.H., McCall, A., Schaub, F.: " i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 197–216 (2018)