# Examining Security and Privacy Research in Developing Regions

Aditya Vashistha
University of Washington
adityav@cs.washington.edu

Richard Anderson
University of Washington
anderson@cs.washington.edu

Shrirang Mare
University of Washington
shri@cs.washington.edu

## ABSTRACT

Prior research suggests that security and privacy needs of users in developing regions are different than those in developed regions. To better understand the underlying differentiating factors, we conducted a systematic review of Human-Computer Interaction for Development and Security & Privacy publications in 15 proceedings, such as CHI, SOUPS, ICTD, and DEV, from the past ten years. Through an in-depth analysis of 114 publications that discuss security and privacy needs of people in developing regions, we identified five key factors—culture, knowledge gaps, unintended technology use, context, and usability and cost considerations—that shape security and privacy preferences of people in developing regions. We discuss how these factors influence their security and privacy considerations using case studies on phone sharing and surveillance. We then present a set of design recommendations and research directions for addressing security and privacy needs of people in resource-constrained settings.

## CCS CONCEPTS

- **Security and privacy** → **Human and societal aspects of security and privacy**;

## KEYWORDS

Developing Regions, HCI4D, ICTD, Systematic Review, Meta-Analysis, Privacy, Security

**ACM Reference Format:**
Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *COMPASS '18: ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS), June 20–22, 2018, Menlo Park and San Jose, CA, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3209811.3209818

## 1 INTRODUCTION

For over the past two decades there has been a tremendous amount of work on understanding and addressing security and privacy needs of technology users. Much of this work, however, has been focused on users in developed regions, such as North America and Europe, that contain only 19% of the world's population. For the majority of the world's population, which lives in developing regions, their use of technology, and information production, consumption, and sharing practices are significantly different from those living in developed regions. These differences present new and unique security and privacy challenges in Human-Computer Interaction for Development (HCI4D) contexts.

Recent years have seen a tremendous growth in the availability of low-cost smartphones and affordable mobile Internet connectivity in developing regions [98], creating a steady stream of new Internet users with socioeconomic, language, and literacy barriers in urban as well as rural areas. However, many of these users have limited or no prior exposure to technology, which makes them vulnerable to privacy and security attacks. Moreover, many new users in resource-constrained settings use technologies in ways unintended by the technology designers. For example, although mobile phones are designed for personal use, and thus are used as a proxy for the identity of users, phone sharing [107], intermediation [127], and vibrant repair ecologies [30] in developing regions manifests diverse uses of mobile phones that introduce new security and privacy risks that were perhaps unimagined by the designers. Thus, there is a need to examine security and privacy needs of this potentially vulnerable population and investigate how differences in their technology use contribute to unique security and privacy implications. In this paper, we systematically review prior work that focuses on marginalized people in developing regions to inform future security and privacy research in HCI4D contexts.

Prior research in HCI4D contexts has primarily focused on understanding technology use by marginalized people, and designing new interventions to overcome their socioeconomic, infrastructural, literacy, and language barriers. However, availability and usability have been at the forefront of design rather than security and confidentiality. The security and privacy preferences of diverse user groups (*e.g.,* low-income, low-literate, disabled, women, rural, and indigenous communities) in HCI4D contexts have remain largely understudied. While a few scholars exclusively focused on security and privacy preferences of people in resource-constrained settings (*e.g.,* [26, 28, 36, 48]), most of the prior work has only provided scattered insights. It is through systematic analysis of these scattered observations in HCI4D and Security & Privacy literature, we seek to understand the state of security and privacy in developing region.

In this paper, we present the results of a systematic review of HCI4D and Security & Privacy literature conducted to identify factors that shape people's security and privacy preferences in developing regions. Although prior systematic reviews of HCI4D literature [58, 73, 114] have identified overall trends in the field and provided broad future directions, the analysis of prevalent security and privacy threats, perceptions, considerations, preferences, and solutions have been largely missing from these works. Our work contributes to the growing scholarship of HCI4D meta-analyses by perusing security and privacy lens to examine prior research

*COMPASS '18, June 20–22, 2018, Menlo Park and San Jose, CA, USA*
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5816-3/18/06.
https://doi.org/10.1145/3209811.3209818

in HCI4D contexts. We conduct an in-depth examination of 114 papers from 15 proceedings to identify key insights about security and privacy behaviors of marginalized people in developing regions. Through thematic analysis on the findings of these papers, we identify five key factors—culture, knowledge gaps, unintended technology use, context, and usability and cost considerations—that significantly shape security and privacy landscape in developing regions. We present case studies on two phenomena, phone sharing and surveillance, common in both developed and developing regions to highlight how the interplay of these factors impact security and privacy of marginalized people in HCI4D contexts. Finally, we present a set of design considerations and research directions for future security and privacy research in developing regions. Through our systematic review, we aim to provide HCI4D as well as Security & Privacy researchers a holistic understanding of the factors that shape security and privacy behavior of people in developing regions.

| Proceedings | Initial count | Final count | Proceedings | Initial count | Final count |
|---|---|---|---|---|---|
| ACM DEV | 64 | 7 | MobiSys | 5 | 2 |
| CCS | 7 | 1 | NordiCHI | 9 | 2 |
| CHI | 159 | 44 | NSDI | 13 | 0 |
| CSCW | 38 | 8 | NSDR | 15 | 3 |
| DIYNetworking | 1 | 0 | OSDI | 1 | 0 |
| HotPlanet | 1 | 0 | SIGCOMM | 11 | 3 |
| ICTD | 126 | 30 | SOUPS | 5 | 3 |
| IEEE S&P | 1 | 0 | UbiComp | 16 | 4 |
| IMC | 8 | 1 | UbiCrowd | 1 | 0 |
| IndiaHCI | 4 | 1 | USENIX Security | 2 | 0 |
| ITID | 0 | 0 | WearSys | 1 | 0 |
| MobileHCI | 13 | 3 | WWW | 16 | 2 |

**Table 1: Relevant HCI4D and Security & Privacy proceedings with number of publications appeared in the initial search and the publications finally selected for the systematic review.**

## 2 METHODOLOGY

Our methods to identify prior literature for analysis were similar to those used by other scholars for conducting systematic reviews [58, 61, 130]. We surveyed HCI4D literature for the past ten years to identify papers that report on security or privacy behavior of people in resource-constrained settings. We examined papers in 24 HCI4D and Security & Privacy proceedings including CHI, CSCW, ICTD, DEV, SOUPS, IEEE S&P, and USENIX Security, among others. For proceedings that were indexed in the ACM Digital Library, we used ACM's built-in search; for other proceedings, we used the search function of Google Scholar. To identify HCI4D papers, we used the search terms 'ICTD', 'HCI4D', 'developing regions', 'resource-constrained settings', 'low-income', 'global development', and 'international development'. Since we aimed to identify papers that report on any security or privacy related behavior, even if it was just a cursory mention and not the focus of the paper, we searched for HCI4D papers in which the terms 'security', 'privacy', or their variations ('secure', 'securing', 'private', 'sensitive') occurred anywhere within the text including title, abstract, keyword, and the body.

Our search yielded 517 papers from all but one proceedings. We conducted two passes to identify relevant papers from this list. In our first pass, we removed posters and position papers (*i.e.*, less than four pages), and papers that had the term 'security', 'privacy', or their variations only in the references section. In our second pass, we carefully reviewed each paper by reading its title, abstract, and introduction, and skimming other sections. We then removed papers that did not provide any insights about the state of security and privacy for people in resource-constrained settings. For example, although the paper titled 'Early Adopters of the Internet and Social Media in Cuba' [66] contained relevant keywords, we removed it in our second pass since the keyword 'privacy' occurred only in the context of methodology (*e.g.*, to anonymize study data to protect participants' privacy). Our first and second passes eliminated 50 and 353 papers, respectively, narrowing the final set to 114 papers from 15 proceedings. Table 1 shows the name of proceedings, the initial number of papers that our search presented, and the final number of papers obtained after completing two passes.

To critically review the remaining 114 papers, we prepared a rubric to fill for each paper with information about its domain (*e.g.,* agriculture, finance, communication), type of contribution (*e.g.,* to extend our understanding about users, to propose a solution, to evaluate a prototype), extent of focus on security or privacy (*e.g.*, yes, no, somewhat), methodology (*e.g.,* interview, survey, usability study), and a summary of security or privacy related findings. We defined domain as the primary area in which a paper describes or solves a problem. We sourced the list of domains from prior HCI4D meta-analysis work [58, 73].

We carefully reviewed each paper to fill the rubric. For each paper, we coded whether it focused on security or privacy: we coded 'yes', if the paper's goal was to understand or address people's security or privacy concerns (*e.g.,* [28, 48]); 'somewhat', if the paper's focus was not security or privacy but it provided key insights about security or privacy behavior of people (*e.g.,* [67, 136]); and 'no', if the paper provided cursory insights about security and privacy behavior of people (*e.g.,* [116, 141]). Figure 1 shows the distribution of papers in our final set by year and their security and privacy focus based on our coding. Categorizing papers based on their security or privacy focus this way is subjective, and if other researchers were to code these papers, the graph may look different. Through Figure 1, we convey a high-level view of the papers we reviewed through *our* security and privacy lens. The first and last authors coded the entire dataset. We measured the consistency between the first and last authors using Cohen's kappa that yielded a value of 0.77 for the first and second pass, and 0.67 for the coding of papers' focus. These kappa values indicate a good agreement between the coding by first and last authors. The second author reviewed only papers for which the first and last authors had a conflicting coding.

After our review, we collected the summaries for each paper, used thematic analysis as outlined by Braun and Clarke [42], and rigorously categorized our codes to identify patterns and broad themes that shape security and privacy preferences of people in resource-constrained settings. Our first-level codes were specific and linked to the findings of the papers, such as *"data security is important to users," "people reluctantly shared phone out of social norms,"* and *"participants did not update software because of the cost."* Through several rounds of iterations, we condensed our codes into high-level themes, such as *"cultural factors"* and *"usability."*

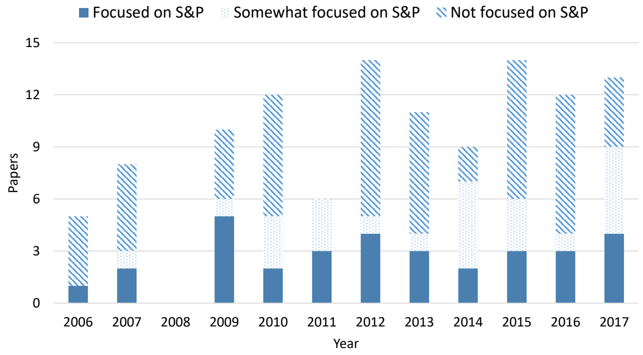

**Figure 1: Number of papers by year and their security and privacy focus.**

| Domain | Paper Count |
|---|---|
| Access | 30 |
| Communication | 14 |
| Digital Financial Services | 10 |
| Health | 9 |
| ICTD Research | 8 |
| Social Media | 8 |
| Technology and Tools | 8 |
| Gender | 4 |
| Entertainment | 3 |
| Physical Security | 3 |

**Table 2: Number of papers in our final set for ten most frequent domains.**

Our analysis of the methodology used in the papers indicated that a wide variety of methods, including interviews, surveys, deployments, ethnography, usability studies, case studies, design exercises, focus groups, observations, and quantitative analysis were used by the scholars. About 45% of the papers used mixed-methods analysis. The papers contributed to 26 domains, including access, agriculture, communication, education, employment, governance, health, sustainability, and transportations, among others. Table 2 shows the name and paper count for ten most frequent domains.

In addition to reviewing papers published in academic research venues, we also examined industry reports on the state of security and privacy for people in developing regions. We reviewed Microsoft Intelligence, GSMA, CGAP, Pew, The World Bank, and Garner repositories and found 14 relevant reports providing key insights on a breadth of topics including software piracy in developing regions and the resultant growth in security risks (*e.g.*, [16]), privacy laws in developing regions (*e.g.*, [7, 11]), security and privacy attitudes of children (*e.g.*, [5]), privacy preferences on mobile phones and across the mobile ecosystem (*e.g.*, [6, 20]), privacy guidelines for designers and developers (*e.g.*, [8]), and identity and access management solutions (*e.g.*, [15, 17]).

# 3 FACTORS

Through our thematic analysis of 114 papers, we identified five key factors that shape people's attitudes towards security and privacy: culture, knowledge gaps, unintended technology use, context, and usability and cost considerations. Before we discuss these factors, it is worth mentioning that the very notion of security and privacy differs across cultures and regions. In our analysis, we followed Nissenbaum's 'contextual integrity' notion of privacy, which refers to the norms that regulate flow of information, and lends well to the different views of privacy in different cultures and contexts [106]. When identifying these factors, we were careful to draw conclusions from the privacy preferences and needs as expressed by the participants in prior studies, and not impose our own views of privacy.

## 3.1 Culture

Cultural values play a key role in shaping individuals' social perceptions [29, 107], attitude towards security and privacy [35, 57], and even the use of technology [22, 78]. In our analysis, rather than looking at *culture* as an all-encompassing singular entity, we examined several facets of cultural values. In particular, we investigated how collectivist and individualist cultural values, social construction of gender, and interplay of trust and religious values inform security and privacy preferences of marginalized people.

*3.1.1 Collectivist vs. Individualist Society.* According to Hofstede's model on cultural differences across nations, Western and developed countries are *individualist* societies with emphasis on the right to privacy, whereas Eastern and developing countries are *collectivist* societies with more emphasis on trust and belongingness than on individual privacy [80]. Although people's preferences and expectation of privacy vary based on whether their cultural values align more with collectivist or individualist values, there does seem to exist a universal desire of privacy, even among the poor [91]. For example, in the slums of Mumbai, where limited physical space is shared with several people in the community, there is an expectation of privacy behind closed doors and curtains [71]. Similarly, although collective concepts such as 'people' and 'population' are deeply rooted in Chinese culture, Liu et al. found that migrant workers use social media platforms to negotiate their cultural identity against the collectivist traditions [93].

Cultural differences in privacy attitudes are even more evident among low-literate and low-income users in rural regions, which are arguably closer to Hofstede's *collectivist* society notion compared to the metropolitan cities in developing regions. For example, in some rural Indian villages, it is a common practice to publicly display vaccinations given by community health workers or salaries of laborers working on a public works project. Such practices would be considered an invasion of privacy in other parts of the world or even in cities in India, but in those villages people willingly sacrifice their privacy for transparency, income security, and accountability. Similarly, sharing bank credentials with family members is a common practice in Saudi Arabian culture, despite severe financial risks due to limited liability assumed by banks when credentials are shared with others [32, 68]. Information gathering practices of marginalized people in resource-constrained settings are primarily based on interactions with friends and family members [86], which at times expose them to unintended privacy risks. For example, siblings trade favors when they encounter traces of digital activities while helping each other navigate digital spaces [27]. Moreover, misconceptions about a local culture by developers or designers may result in inappropriate threat modeling. For example, an ODK[1] solution architect highlighted how privacy takes a backseat in their design and development process: *"Within the village everybody knows who's poor, everybody knows if you have some sort of special needs, so I don't think [privacy] is really on the forefront of their minds"* [51]. We argue against such preconceived notions. Rather than accepting the lack of demand for secure and private solutions by marginalized people or forcing designers' notion of security and privacy on them, there is a need to carefully inspect sociocultural values to design appropriate security and privacy measures that adapt to their existing needs, practices, and behaviors.

*3.1.2 Gendered Identities.* Sociocultural factors impact construction, perception, and performance of different gendered identities [45], and influence the adoption of technology and acceptable norms of participating in the information ecology. A recent GSMA report estimates that over 1.7 billion women in low- and middle-income countries do not even own mobile phones [76]. For women who have access to a phone, their access is often mediated or monitored by family members, friends, and other community actors who discount women's need of security, privacy, and personal identity [63, 128]. For example, although Grameen Telecom's Village Phone program [21] attempts to improve phone access of low-income women, often these women have to sacrifice their privacy by using the phone in presence of a Village Phone operator [40]. Moreover, asymmetrical spousal rights to privacy allow husbands to monitor the communication of their spouses in such shared phone scenarios [40]. This phenomena is pervasive in other marginalized communities across the world [102].

Low-income, low-literate women have expressed the need to use their phones independently to protect their privacy [63], but expressing or fulfilling such privacy needs at times result in untoward consequences or missed opportunities due to the sociocultural fabric of their community. For example, Sambasivan et al. found that women in urban India are hesitant to provide their phone number to receive a one-time-password required to access public Wi-Fi out of the fear of its misuse and the risk of harassment [125]. Similarly, several women working as sex workers, without the knowledge of their family members, were hesitant to provide their fingerprints for accessing health information due to perceived privacy risks to their identity [110]. For people that identify with non-binary gender identities in developing regions, aversive sociocultural factors further complicate their access to solutions that are designed to improve people's security and privacy. For example, transgenders have reported difficulties in registering for India's national identification program due to discriminatory attitudes of government officials as well as the requirement of supporting documents that do not recognize 'third gender' [3].

Although it is evident that researchers and designers need to conceptualize, design, and build appropriate security and privacy solutions that overcome barriers imposed on gendered identities, sociocultural values also disproportionately affect the access of researchers to women and transgenders in low-income settings, making it difficult to examine and analyze their security and privacy needs. HCI4D researchers have used several coping mechanisms to gain access to these hard-to-reach groups. For example, while user studies and interviews in developed regions are often conducted in closed private spaces, HCI4D researchers have found it rewarding to conduct interviews in open public spaces to motivate other marginalized women in low-income settings to participate in the design and research process [118]. Similarly, HCI4D scholars also recommend employing a mediator to overcome barriers around the social norms of cross-gender communication [105]. However, these practices should be used with caution since they could lead to inadvertent sharing of confidential information or controversial views that could be overheard by other community members or misused by the local mediator, resulting in severe security and privacy risks for study participants.

*3.1.3 Trust and Religion.* While mobile phones are seen as a proxy of identity in developed countries, the phones often do not have a one-to-one mapping with a user in resource-constrained settings due to prevalent socio-technological practices such as phone sharing and intermediated use. Since phones are not designed for a group use, existing mechanisms to protect identity and secure information often fail. The social fabric in such societies is based on notions of trust and collectivism, and tight security and privacy features could even disrupt the existing relationships [128]. Although information on phones could be protected by creating passwords or managing user profiles, even the act of using a password or switching a profile may seem offensive to values emphasizing trust and collectivism. For example, Alghamdi et al. reported how keeping the banking information and credentials private was seen as a sign of distrust by family members [32].

Religious values also shape privacy behaviors that in turn could influence the technology adoption and use. For example, while Sangeet Swara, a voice forum dedicated to songs, jokes, and poems, received instant adoption by low-income people in rural India [142], Songline—a similar system in Pakistan—failed to attract enough interest because users were worried about the confidentiality of songs that anyone could access [120], probably due to controversial religious views towards certain types of music [132].

Cultural and religious values also shape inherent trust marginalized people place in their communities and technological interventions. A study of urban slum dwellers in Mumbai and Bangalore reported high-levels of trust in the community and examined how mobile phones were used as instruments to mediate trust-building and negotiate privacy in a pervasive oral culture [128]. Due to the high amount of trust that people place in their communities, they readily accept intermediated use, which helps them learn technologies such as mobile phones and digital cameras [127]. This trust is sometimes misplaced and exposes people to security and privacy risks. An examination of repair ecologies in Bangladesh revealed serious privacy breaches by repairers who accessed personal data of their customers and shared it with others, without customers' knowledge. Interestingly, some at-risk customers placed more trust in religion and social and cultural values, rather than the technological solution built by designers to mitigate such privacy risks: *"when*

[1] ODK is a popular phone-based data collection tool used by international development practitioners [79].

*he [repairer] will have those ethics, that fear [of Allah], then he will not access it [the private content of consumers]"* [26].

Culture, with its different notions of identity and trust, introduces new security and privacy challenges, but also opportunities. Researchers may find it more suitable to address security and privacy problems by interweaving technological interventions in the socio-cultural fabric of local communities rather than using them in silo. For example, user awareness and education may be targeted at communities than individuals, leveraging social influence prevalent in collectivist cultures [123].

## 3.2 Knowledge Gaps

Although the security and privacy risks due to lack of user awareness are not unique to users in developing regions, they are compounded by low literacy skills, socioeconomic barriers, and infrastructural constraints prevalent in resource-constrained settings. For example, several low-income users of a mobile money service found comfort in receiving SMS-based receipts without realizing that SMS could be spoofed [111]. The rapid adoption of mobile phones in developing regions could be deceptively seen as an indicator that marginalized people are becoming technologically literate. In reality, many people learn only a limited set of functions on the phone [63] (*e.g.*, they can only make and receive phone calls [97]).

Users in developing regions lack the technology knowledge that many take for granted today such as tap and swipe gestures, navigating menus and screens, recognizing soft buttons and icons on a display, and locating symbols when entering input [97]. In a study to explore Internet security perceptions in urban and peri-urban Ghana, Chen et al. found that computer skills—scarce for people in low-income and rural environments—were correlated with the ability to perform security and privacy measures such as deleting text messages, cookies, browsing history, and emails [48]. Moreover, due to lack of knowledge, people form incomplete or incorrect mental models related to security and privacy threats, which may lead to risky behavior [48, 148]. For example, participants in studies conducted in Ghana as well as the United States ascribed higher risks to physical threat model (*e.g.*, people looking over their shoulder) than mental threat model (*e.g.*, browsing untrustworthy websites) because of limited understanding of the underlying technology [48, 85]. Lack of knowledge due to low digital and print literacy also affects the understanding of security and privacy risks [26]. For most online systems and services, information about their security and privacy practices (*e.g.,* terms and conditions, privacy policy) is often only in English and at a grade-level that low-literate users cannot easily understand [41]. Even when these populations are aware of security and privacy risks, they lack the knowledge to take any effective action to mitigate these threats. For example, Dodson et al. reported how low-income women with limited technological skills had to reluctantly accept the invasion of their privacy when they requested help from shopkeepers and local retailers to install mobile credits [63]. Dodson et al. found utility gaps—*"the spaces between high rates of mobile phone ownership and low use of productive features on mobile phone"*—as the key privacy barrier for low-income Berber-Muslim women in southwest Morocco [63].

Due to lack of awareness of how online systems work, users may develop misconceptions and form incorrect mental models [125], which lead them to adopt risky practices [131]. Furthermore, a bad experience (either a personal one or a heresy) causes ignorant users to develop apprehension for a system they do not fully understand, and without readily available knowledge or simple mechanisms to handle potential bad situations, users may take the extreme precautionary measure of not using a system, despite the system’s benefits to the user. For instance, a novice low-literate mobile user may avoid using mobile banking services due to the fear of getting defrauded [44, 103]. This phenomenon is not unique to technology, and can be found in other walks of life. For example, researchers have observed low-literate, low-income users exhibit misconceptions and fear with respect to signatures and thumb impressions [56, 110, 138] due to association of such actions with identity and legal accountability.

We argue that using a deficit-based perspective (*e.g.,* focusing only on educating users to fill the *knowledge gaps*) to examine security and privacy measures for marginalized people could be insufficient. Instead, researchers, designers, and developers should employ assets-based approach [94] to leverage strengths and current practices of people in resource-constrained settings for creating usable, secure, and private socio-technological interventions. An exemplar solution that uses assets-based approach is FlashPatch [53]—a software security system that uses USB drives to transmit security updates to Internet café in Ghana by building on existing user behaviors instead of assuming users’ knowledge and preparedness to install and regularly update anti-virus softwares.

## 3.3 Unintended Technology Use

In developing regions people often use technology to suit their needs in ways unintended by the technology designers.

### 3.3.1 Sharing and Intermediation.

The most common example of unintended use is sharing of resources such as mobile phones and computers. Mobile phones are designed as single-user personal devices, but they are often shared with family members and friends, especially in low-income environments [64, 119]. People who are aware of the privacy risks of phone sharing use ad-hoc measures such as renaming files (*i.e.,* security by obscurity), using folder- or application-level locks [64], and using multiple storage cards [136] to hide content from others, but none of these methods offer a suitable solution since people tend to share their passwords with others because of social obligations [51, 68, 147].

Intermediated sharing is a manifestation of collectivist sociocultural values and phone sharing phenomena. Several users in marginalized communities experience technological artifact through help and intermediation from another user, either due to the fear of technology, limited literacy skills, lack of access to devices, or habits of dependency [127]. In such scenarios, privacy is often socially-negotiated between intended user and facilitator [107, 127]. The intermediated access introduces new privacy risks and raises an important question of how to design a secure and private software that distinguishes between intermediary-user and beneficiary-user?

### 3.3.2 Phone Repair.

The life cycle of digital devices is much longer in developing regions compared to developed regions: with the pervasive repair ecologies and the used phone markets digital devices undergo several cycles of ownership and repair. Although these markets reduce and recycle e-waste through reuse, repair, and resale, they often contribute to security and privacy violations. For example, researchers have reported prevalence of pornographic material near repair markets, in which repairers were found lurking and sharing private data of customers who left their devices (*e.g.,* PCs and mobile phones) with the third-party repairers [26, 30, 119]. Researchers found that repair-shop customers often assumed that the repairer cannot (or trusted that the repairer will not) access their data, and customers who were aware of the risks during the repair process did not know how to avoid it [26]. Full-disk encryption on mobile phones may help in such circumstances, but if the repairer asks for phone password in order to repair the phone, customers may not be technically literate enough to argue or may have little choice but to comply if they want to get their phone repaired.

*3.3.3 Mobile Media and Piracy.* Users in developing regions, including low-income users, heavily engage in media consumption and dissemination on their mobile phones [88, 109, 143]. Mobile shops in rural areas serve as a focal point for mobile media distribution. In these shops, low-income, low-literate people hand over their phones to mobile shop owners to get content of their choice, without fully realizing the security and privacy implications. For example, mobile shop owners download customers' photos and videos, without the customer's permission or knowledge, to expand their media repository. Mobile shop owners also share their repository with each other [143] (generally via external hard drives to minimize the bandwidth cost of downloading new media content from the Internet). Thus, a customer's private data, copied in one shop, could traverse long geographical distances resulting in severe privacy violations.

Low-income people are also frequent users of pirated media and software. For example, O'Neill et al. [109] and Kumar et al. [90] reported how low-income phone users were oblivious about the illegality of piracy. Even when they understood that piracy is illegal, they continued to download and share pirated content, thereby violating the digital rights of the content owners. Since local folk musicians have no effective means to combat piracy, they trade-off the security of their content (*i.e.,* Digital Rights Management) with popularity, even when it comes at the expense of lost earning [89]. Similarly, software piracy is rampant in developing regions. Pirated software may not be a security risk in and of themselves, but it may be challenging to verify the integrity of the software or to get software updates, which may put users at risk [36]. For example, developing countries with widespread software piracy like Bangladesh, Pakistan, and Indonesia [9] also have high malware encounter rate [16].

For these unique use cases in diverse HCI4D contexts, we argue for a thorough examination of technology ecosystem that goes beyond investigating factors that impact technology adoption and use by marginalized people. Equally important is to examine the motivations and practices of other stakeholders (*e.g.*, mobile shop owners, repairers) before designing interventions that increase awareness of users about prevalent security and privacy risks.

## 3.4 Context

The context in which low-income, low-literate people use a technology artifact also affect their security and privacy perceptions and preferences. For example, different stakeholders may ascribe divergent values to information security for the same artifact based on the context of its use. In a study examining user perceptions of different receipt delivery mechanisms for a mobile-based branchless banking system, users perceived paper receipts as more reliable, accessible, and tangible, and preferred them despite known security vulnerabilities [113]. Similarly, low-income clients of a microfinance institution also ascribed higher security and trust to paper receipts [47]. Conversely, in a study conducted to examine security risks for data collection technologies, several deployment architects perceived digital devices as more secure than paper [51]. Interestingly, in yet another study, clinicians were concerned about security risks of storing patient data on mobile phones and advocated using paper records [34]. These examples demonstrate that the security and privacy perceptions for a technology artifacts are transient. A solution perceived as secure and private in one context could be perceived as risky in another context.

Where a technology artifact is used also influence security and privacy risks associated with it. Often one reality coexist with another contrasting reality. For example, although phone sharing by family members [128], intermediation through community members [107, 127], and public access [135] are common in developing regions, users of low-cost smartphones in India preferred to use their phones in personal physical spaces due to the anxiety of privacy invasion by onlookers and strangers [72]. The expectation of security and privacy measures also varied based on the information content and people with whom technology was used. For example, beneficiary-users socially-negotiated their privacy with intermediary-users when they anticipated arrival of confidential information [107] by using simple measures such as callbacks instead of leaving private information with intermediary-users. Similarly, people reported different privacy preferences when sharing phones with their parents, children, siblings, and friends [27].

Since a technology such as mobile phones could be used by a diverse set of users (*e.g.,* beneficiary-user, intermediary-user, low-income people, low-literate people, women) in distinct settings (*e.g.,* private use, shared access, intermediated access), a *one-size-fits-all* approach to mitigate security and privacy risks is inadequate. We argue to carefully examine these contexts to design adaptable, flexible, secure, and private technological interventions.

## 3.5 Usability and Cost Considerations

Security and privacy needs have been often expressed by diverse user groups, including health workers [39], new mothers [62], and children of migrant workers [151]. However, the desire for usable and personalized technologies often eclipses security and privacy needs of marginalized people in developing regions. For example, to get free access to high-speed public Wi-Fi, people in urban India connected their phones to an unsecure network despite being aware of security risks [125]. In a study conducted with people in Ghana, India, and the United States, people were willing to risk their privacy to obtain detailed reports on the use of the Internet in their home [50]. Low-income people in India used an informal, insecure network to send money home because of the usability barriers in services of existing mobile money providers [87]. Similarly, urban slum dwellers in India indicated a preference for personalization instead of privacy to improve their user experience [128].

Since a majority of new Internet users in developing regions live under harsh economic constraints, cost considerations also dictates their security and privacy practices, for example, ignoring security updates to optimize data usage [49, 95]. Other researchers have also reported the preference of people in developing regions to save bandwidth costs even if it effectively degrades their user experience [108]. However, the economic constraints do not always drive security and privacy preferences in poor communities. Urban sex workers in India, even though poor, bought multiple SIM cards and frequently switched them to protect their anonymity [129].

Although these findings suggest that usability and cost considerations are central to the design of technology for marginalized people, security and privacy measures must not take a backseat like it did for ODK architects who preferred data availability and integrity over data confidentiality [51]. We argue that technology platforms must present meaningful trade-offs between security-privacy measures, and usability and cost considerations. In addition, security and privacy measures should be designed in a usable and cost-effective manner to support existing practices and workflows of marginalized people in resource-constrained settings. An exemplar work that gives precedence to cost considerations without sacrificing security is by Panjwani and Cutrell who designed a secure yet low-cost authentication scheme for mobile banking users without compromising usability [112].

# 4 CASE STUDIES

To further elaborate how these factors shape people's security and privacy perceptions and behavior, we present case studies on phone sharing and surveillance.

## 4.1 Phone Sharing

We selected phone sharing as our first case study since it is a phenomena common in developed [83, 96] as well as developing regions [27] with underlying differences in the nature of sharing (*e.g.,* why people share and how often) and the extent of sharing (*e.g.,* with whom and the type of sharing). Because of these differences, phone sharing phenomena provides a good lens to examine how interplay of the factors we identified in the previous section shapes security and privacy behaviors and expectations of the people in developing regions.

*4.1.1 Motivations for Phone Sharing.* In developed regions, convenience is the primary motivation for sharing phones, and the predominant type of sharing could be classified as borrowing (*e.g.,* using a phone that is nearby to check weather or news) [96]. In developing regions, convenience is a factor but not the primary motivation. In low- and middle-income families, lack of ownership (*i.e.,* only one phone in the family) and the need for a shared resource (*i.e.,* only one smartphone in a family that has multiple phones) dictates sharing [107]. Thus, the predominant type of sharing in developing regions is for mutual use. Sociocultural norms (*culture*) also influence sharing, more in developing regions compared to developed regions, and often lead to forced sharing (*e.g.,* sharing a phone with a friend due to social pressure) [27, 147]. Lack of knowledge (*knowledge gap*) and self-confidence to operate phones also lead people to request outside help (*i.e.,* intermediation [127]) that could lead to unexpected privacy risks.

*4.1.2 Mechanisms for Phone Sharing.* In developed regions, phone sharing is less common on a daily basis, and often the phone owner is nearby when the phone is being shared [83]. In developing regions, when a phone is mutually used, it is shared on a regular basis. Factors such as gender discrimination (*culture*), *knowledge gaps*, and intermediated use (*unintended technology use*) leads to a more asymmetric sharing: one person gets access to the other person's content, but not the other way around. For example, husband checks his wife's phone, but wife is not allowed to check her husband's phone [63]; women do not get their own phones, but men do; a tech-literate youngster in a family controls access and content on the family phone; and a youngster who helps his neighbor use a messaging application gets access to his neighbor's content [27].

*Context* is another key factor that influence sharing. The rules for sharing are flexible and they are often socially-negotiated at the time of sharing; for example, kids are sometimes allowed to play games on father's phone and sometimes not, and siblings trade favors for access to a phone controlled by another sibling [27]. Sharing also depends on the phone's perceived utility (*i.e.,* how it is seen or used). In developed regions, phone is seen as a device primarily for education, emergencies, or entertainment, whereas low- and middle-income users in developing regions perceive phone also as an instrument for economic growth and communication [65, 82, 107]. This in turn strongly influences how tightly people control their phone based on the context of its use.

*4.1.3 Concerns Around Phone Sharing.* Studies in developing regions suggest that participants share phones with family and friends due to social norms (*culture*), but they do so reluctantly, and take ad-hoc measures when they can such as using folder or application locks, and using a second memory card for storing private content [27, 64, 136]. Other coping mechanisms unique to developing regions include keeping phones hidden [152], buying used phones [152], or using multiple phones [109] for different purposes. In a recent study, participants expressed a need to keep their data secret without others knowing the existence of the private data, because use of a separate account or application locks is seen as lack of trust, and the individual may be forced to share the password [27].

Given the current sharing behavior in developing regions, the design challenge is how to facilitate shared use of a phone while preserving individuals privacy. Design must take into account that sharing implies a changing set of users and contexts of use [127]. The current solution—multi-user accounts—does not fully address the issue. It fails to consider the cultural context, where norms of sharing override concerns of privacy, security, and personal identity [128]. Given the differences in the reasons for sharing and the nature of sharing between developed and developing regions, a solution designed for sharing behavior in developed regions is unlikely to facilitate privacy-preserving sharing in developing regions. However, a solution designed for sharing behavior in developing regions—a more constrained requirement—may address privacy concerns around sharing in developed regions.

## 4.2 Identity and Surveillance

We selected surveillance as our second case study because it is a growing concern in developing regions. We examine how the five factors influence people's security and privacy attitudes and actions with regards to state surveillance.

An increasing number of governments in developing regions have undertaken nation-wide surveillance programs recently. Although state surveillance is a concern throughout the world, we think, it is more concerning for people in developing countries because several developing countries have unstable democracies or have limited (or no) individual privacy and data protection regulations that put their citizens at a greater risk of security and privacy violations. There have been several incidents of governments exercising its surveillance abilities to curb anti-government sentiments or promoting specific agenda, for example, by arresting individuals for posting anti-government comments on social media [115], or banning access to certain Internet services and applications [10, 28, 70, 92, 122]. For these reasons, several non-profit organizations like Privacy International and intergovernmental organizations like The World Bank have advocated strengthening privacy laws against surveillance [7, 11].

Many developing countries are undertaking efforts to enroll citizens in national identification programs, which are promoted as designed to facilitate welfare programs to serve the marginalized population. However, there are concerns that such systems could be misused to further enhance the government's surveillance capabilities, and discriminate and exploit marginalized people and dissidents, a fear that stems from ingrained mistrust in the governments [28, 134] due to socio-political factors. Moreover, there are concerns about government's ineffectiveness in safeguarding the identity information from misuse by non-state actors. For example, recent reports indicate a security breach in the biometric database created and managed by the government of India [124].

National identification programs challenge the existing use of identity and ownership in developing regions. Compared to developed regions, the concept and use of identity is different in developing regions. It is complicated by social and cultural norms (*culture*), which influence how people socially negotiate identities. For example, a woman assumes a man's identity when enrolling for a SIM card out of the fear of harassment [28]; in a public distribution system where government subsidized goods are sold, merchants log the sale under an assumed identity if a customer does not have the appropriate documents (*unintended technology use*) [100]. Sociocultural factors (*culture*) also make it difficult for women and transgenders to obtain digital identity from national identification programs. For example, in a recent study on Bangladesh's national biometric program, researchers found that some Bangladeshi women hesitated to provide biometric identifiers since male staff members at the registration booths had to touch their hand to take the fingerprints [28]. Similarly, some Indian transgenders found it difficult to get digital identification because of the discriminatory attitudes of government officials [1].

*Knowledge gaps* and *cost considerations* significantly limit the ways in which marginalized people can protect themselves from surveillance. People may use an insecure platform (instead of looking for secure alternatives) because they feel they have 'nothing to hide', an attitude that stems from a myopic view of privacy as a form of secrecy used only to hide *bad* things [137], and their lack of awareness of how different stakeholders of a platform may use consumer data. Some common practices surrounding technology use in developing regions could also lead to increased security risks for marginalized people. For example, in a shared-phone settings, it is difficult to understand who used a shared phone when and for what purpose. Lack of awareness could pose severe security risks if a social connection misuses the phone of an individual to carry protest or unlawful activities against the state.

The defense against the rising threat of large scale surveillance cannot be technology alone. If individuals use technology to subvert government agenda without the appropriate policies that protect individuals' rights, it could lead to conflicts between individuals and government [38]. Non-governmental and activist organizations could help establish the necessary regulations to protect individuals' privacy and rights.

# 5 DISCUSSION

Through a systematic review of HCI4D and Security & Privacy literature, we highlighted five factors that shape security and privacy considerations of low-income people in resource-constrained settings. We described how factors such as *unintended technology use* and *context* present new security and privacy risks in developing regions, factors such as *usability and cost considerations* render existing security and privacy solutions ineffective in developing regions, and other factors such as *knowledge gaps* and *sociocultural values* amplify existing security and privacy risks in developing regions. Based on the gaps revealed by our systematic review of existing literature, we now outline three research directions to understand and mitigate security and privacy risks for marginalized people in resource-constrained settings.

## 5.1 Understanding Attitudes and Preferences

To develop solutions that match users' security and privacy expectations, it is important to understand their beliefs and expectations towards security and privacy as well as investigate other internal and external forces such as sociocultural fabric and context that shape their preferences. Prior scholars have noted that mental models of potential threats for users in developing regions are significantly different than those for users in developed regions [48]. Thus, it is important to examine how people in a particular context perceive security and privacy threats, where are the knowledge gaps, and how their surroundings affect their use of technology and shape their mental models.

*5.1.1 Studying Behavior at Scale.* A growing number of HCI4D scholars are examining security and privacy needs of marginalized people in developing regions [26, 28, 48, 51, 64], however, more research is needed to examine security and privacy preferences of diverse user groups (*e.g.,* disabled people, low-literate people, rural residents, women) using technologies in different contexts (*e.g.,* health, education, finance) and geographical locations (*e.g.,* South Asia, Africa) to avoid inappropriate generalizations. Equally important is to use human-centered research methods and assets-based approaches [94] to examine sociocultural factors, context, and unique technology use cases, and identify knowledge gaps, and usability and cost considerations to design secure, usable, private, and cost-effective technological interventions. Exemplar work is by Panjwani and Cutrell to design a secure mobile banking authentication scheme without compromising usability [112], and by Corrigan-Gibbs and

Chen to design a security system to mitigate computer viruses by leveraging existing user behaviors [53]. Another exemplar work is by Sambasivan et al. where human-centered methods were employed to investigate how women in India, Pakistan, and Bangladesh use performative strategies, such as using phone and app locks, deleting content, avoiding technology, and using hidden modes, among others, to negotiate their privacy from family members and social connections [126]. Although we emphasize the need to use human-centered design to examine security and privacy preferences in diverse HCI4D contexts, we recognize that doing so in every context for every user group in distinct geographic locations is unscalable. An alternative is to conduct large-scale cross-gender and cross-country studies (*e.g.*, [18] and [78] ) to design high-level security and privacy models, similar to Hofstede’ cross-cultural models [80], for different HCI4D contexts.

*5.1.2 Case for Replication.* Users’ security and privacy behavior and preferences have been a topic of interest in the usable security & privacy research community for over two decades [25, 149, 155]. The subjects of interest in previous studies, however, have been primarily users in developed countries. Given the cultural and regional differences in people’s behavior and preferences, it is unclear how much of the existing work in usable security & privacy literature is applicable to users in developing regions. Careful replication of some of the past user studies conducted in developed regions into developing regions could help researchers identify concrete differences in security and privacy attitudes of users in developing and developed regions, and compare lessons learned and future research directions. Replicating scientific studies is a norm in hard sciences, common in psychology [52, 154], and recently has gained momentum in Data Sciences [12] as well as Human-Computer Interaction [150]. Although there is no rigid dichotomy between developed and developing regions, we argue that unique technology use, sociocultural differences, and different knowledge gaps warrant a careful inspection of the differences between users’ attitudes and preferences in developing and developed regions to avoid inappropriate generalizations.

*5.1.3 Considerations for Conducting Studies in HCI4D Contexts.* Traditional ways of understanding users’ attitudes and behaviors involves conducting users studies with quantitative surveys (*e.g.,* [78]), observations done in person (*e.g.,* [133]), data collected by instrumenting users’ devices (*e.g.,* [146]), and qualitative interviews (*e.g.,* [148]). However, conducting surveys and qualitative interviews with low-income, low-literate people is challenging, particularly in rural regions, due to literacy constraints, cultural differences, socioeconomic barriers, and response bias [59, 144]. Moreover, instrumenting low-cost devices, such as basic and feature phones, that are intermittently connected to the Internet is also difficult. Popular platforms for large-scale surveys such as Amazon Mechanical Turk [13] are not easily accessible to over 97% of the households in India that do not have a computer [2] and other user groups such as low-income, low-literate communities [84] and visually impaired people [145]. Services such as mSurvey [19] could help reach mobile phone users, however, designing rich surveys on mobile phones is challenging, and is an area worth exploring. Security and privacy researchers may derive inspiration from HCI4D researchers who have overcome these challenges by creating strong partnerships with local grassroots organizations, and designing socioculturally appropriate studies and interventions for marginalized people in resource-constrained settings.

## 5.2 Designing with Users in Developing Regions

Once we understand users’ security and privacy needs, the challenge is *how* to design systems that address those needs.

*5.2.1 Designing for Local Context.* Designers needs to be cognizant about cultural and local context of developing regions as well as the additional constraints that HCI4D contexts offer such as poor network connectivity and low-cost devices. The different technology and device usage models (*e.g.,* shared and intermediated use) introduce new challenges for providing personalized online services. For example, in a shared phone setting, consider the problem of providing a personalized online service to a user who does not have an email account or a dedicated phone number. For most online services, email is an acceptable and often the only way to communicate to users (*e.g.,* to reset a password). Some services associate users’ identity with a phone number, but that approach discounts users who share a mobile phone. For such scenarios, the design challenge is how to support multiple users accessing the same online service from the same device, while safeguarding their information from each other. Multi-user accounts on a mobile phone is one approach, but current implementations require switching accounts, which is not seamless and could be perceived as culturally inappropriate since changing accounts before sharing a device implies a sign of mistrust in some cultures [27]. Perhaps behavioral authentication methods [37, 69, 101] based on sensors in a smartphone could be leveraged to address this problem by seamlessly identifying a user and switching profiles accordingly to provide personalized services to the current user while protecting data of the other users of that smartphone. This would also transfer the onus on switch on the technology instead of a user, protecting users from social costs that comes with switching profiles. The implementation of these methods, however, would need to be efficient on smartphones to minimize consumption of phone battery since several people in developing regions struggle to power their phones [43]. Similarly, for intermediated use, it is important to identify solutions to protect data of beneficiary-users from intermediary-users.

*5.2.2 Leveraging Social Values.* Some challenges are better addressed with socio-technological intervention than a pure technological intervention; for example, using participatory design based approaches to design *with* users, rather than simply *for* users. Given that participatory design approaches are rooted in political and socioeconomic empowerment, these approaches would also help achieve design solutions that conform to cultural norms and local context while empowering users. Designing with users also enables researchers to leverage deeply-rooted social and religious values to engage and educate users about the underlying technology more effectively [123]. Making users aware of how the underlying technology works and the associated security and privacy issues helps build their trust and confidence in the technology. It is worth further exploring how peer-to-peer learning and social influence [54, 55, 99], which are more effective in a collectivist society compared to an individualist society, could be used to reduce security and privacy knowledge gaps.

Participatory design approaches have their own challenges in societies with asymmetrical power structures. For example, engaging women in rural India is often impossible without approval from agents supporting patriarchal structures (e.g., husbands and in-laws). In order to design secure and private solutions for women and non-binary gender identities in rural, resource-constrained settings with prevalent and powerful patriarchal structures, we echo Sultana et al.'s suggestion of designing within the patriarchy instead of against it and leveraging existing relationships women have with organizations (e.g., non-governmental organizations) and individuals (e.g., health workers, amity group, female elders) [139].

*5.2.3 Designing for Reliability.* Bridging knowledge gaps and designing usable interfaces could lower the bar for a user to try a new technology, but unless the technology works reliably, a user is less likely to continue using it. New technology users are sensitive to failures. It is easy for novice users with low self-confidence to blame themselves for technology failures and get discouraged from using the technology. This psychology is seen even in technologically literate users, who see failures as a sign of their incompetence to use the technology [140]. For low-income users, security or privacy failures in services such as banking or healthcare could lead to financial or health shocks that are significant determinants to poverty alleviation [31, 60]. Thus, it is critical to build reliable systems with security and privacy in mind, rather than considering those as add-on features.

## 5.3 Supporting Designers and Developers

Although common vulnerabilities and errors that occur in software design and development are well enumerated [14], our systematic review indicated that several designers and developers have misconceptions about the security and privacy needs of marginalized people (*e.g.*, ODK deployment architects [51]), lack knowledge and resources to incorporate security and privacy features [121, 153], or have poor economic incentives to prioritize security and privacy over the more visible (to users) functional features in their software [33]. The economic incentive is even lower for developers in developing regions, because of the low-paying capacity of low- and middle-income users, or their unwillingness to pay for software when free or pirated software are available [74].

*5.3.1 Policy.* Technology and regulatory frameworks surrounding security and privacy in several developing countries either do not exist or are often borrowed from those in developed regions without adaptations and appropriations [4]. For example, only 40 developing economies have privacy laws around cloud computing [117]. Lack of formal identification mechanisms in many developing countries makes it difficult for marginalized communities to access essential services such as banking, and participate in analogue and digital worlds [17]. There is a need to build suitable identity and access management solutions to empower marginalized groups including disabled people, refugees, transgenders, children, women, rural residents, low-literate and low-income communities [15, 17]. The policymakers have a key role to design and implement laws that ensure creation of secure identity and access management solutions, and safeguard them from internal and external threats. Policies and laws surrounding security and privacy research could also play a large role to motivate designers and developers to keep security and privacy at the forefront of their design process and use best practices to store, process, and transfer users' data. There is also a need to build capacity and increase awareness to ensure that these laws and best practices are enacted.

*5.3.2 Incentivizing developers.* How can we help developers build secure software? One school of thought suggests changing developers' incentives and to make developers accountable for the security errors in their softwares [77], while another suggests that developers need more usable security tools and APIs [75]. The latter thought is based on the argument that developers wish to do the right thing (*i.e.,* develop secure software), but they often make poor security and privacy decisions because the current available security tools and recommendations are too difficult to understand, use, and implement. Findings from a recent user study with developers about their security practices echoes with this premise [46]. There are several open questions in this research direction. For example, how do developers handle secure software engineering process, where and what kind of errors they make in the software development cycle, what are their mental models about the threats for their software, and how can we make security and privacy best practices more accessible to them? We recommend using a human-centered approach to examine the incentives of designers and developers, and identify areas for educating them about security and privacy preferences of their target population. This human-centered approach to improve security has recently gained attention of security researchers [24, 81], and the recent work in this area (*e.g.,* [23, 104]) is a promising step towards answering these questions.

# 6 CONCLUSION

In this paper, we presented a systematic review of the HCI4D and Security & Privacy literature to examine the state of security and privacy for marginalized people in resource-constrained settings. Our in-depth analysis of 114 publications from 15 proceedings indicated that sociocultural values, lack of knowledge and awareness, use of technology in ways unintended by the technology designers, contexts in which a technology is used, and usability and cost considerations shape perceptions surrounding security, privacy, and confidentiality in developing regions. We presented case studies on phone sharing and surveillance—phenomena common in both developing and developed regions—to highlight interplay of these differentiating factors. For researchers interested in designing security and privacy measures for low-income, low-literate people in developing regions, we outlined how they can understand attitudes and preferences of people in developing regions, co-design appropriate and contextualized solutions with them, and help designers and developers keep security and privacy at the center of their design and development process.

# REFERENCES

[1] 2012. Getting Aadhaar Card Big Challenge for Transgenders. http://www.deccanherald.com/content/250353/getting-aadhaar-card-big-challenge.html

[2] 2012. Press Note on Release of Data on Houses, Household Amenities and Assets, Census 2011. http://censusindia.gov.in/2011census/hlo/Data_sheet/India/HLO_Press_Release.pdf

[3] 2013. India’s ‘Third Gender’: A Marginalised Social Class. http://ajmn.tv/26tav

[4] 2013. Information Economy Report 2013. http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=710

[5] 2016. Children’s Use of Mobile Phones - An International Comparison 2015. https://www.gsma.com/publicpolicy/childrens-use-mobile-phones-international-comparison-2015

[6] 2016. Country Overview: Pakistan - A Digital Future. https://www.gsma.com/mobilefordevelopment/programme/connected-society/country-overview-pakistan-a-digital-future

[7] 2016. The Global Surveillance Industry, Privacy International Beta. https://www.privacyinternational.org/node/807

[8] 2016. Mobile Privacy Principles. https://www.gsma.com/publicpolicy/mobile-privacy-principles

[9] 2016. Over 80 Percent Software Installed in Pakistan, Bangladesh and Indonesia Unlicensed. https://tribune.com.pk/story/1110292/asia-hotbed-piracy-despite-economic-growth/

[10] 2016. Vietnam Blocks Facebook and Cracks Down on Human Rights Activists During Obama Visit. https://www.accessnow.org/vietnam-blocks-facebook-human-rights-obama/

[11] 2016. World Development Report 2016: Digital Dividends. http://www.worldbank.org/en/publication/wdr2016

[12] 2017. ACM SIGMOD 2017 Most Reproducible Paper Award Winners: SIGMOD Website. https://sigmod.org/2017-reproducibility-award/

[13] 2017. Amazon Mechanical Turk. https://www.mturk.com/mturk/

[14] 2017. Common Vulnerabilities and Exposures. https://cve.mitre.org/

[15] 2017. Enabling Access to Mobile Services for the Forcibly Displaced. https://www.gsma.com/mobilefordevelopment/programme/digital-identity/enabling-access-mobile-services-forcibly-displaced

[16] 2017. Global Security Intelligence Report, Microsoft. https://www.microsoft.com/en-us/security/Intelligence-report

[17] 2017. GSMA Mobile Economy 2017. https://www.gsma.com/mobileeconomy/

[18] 2017. Helix Institute of Digital Finance. http://helix-institute.com/

[19] 2017. mSurvey. https://msurvey.co.ke/

[20] 2017. Safety, Privacy and Security Across the Mobile Ecosystem. https://www.gsma.com/publicpolicy/safety-privacy-security-across-mobile-ecosystem

[21] 2017. Village Phone - Grameen Telecom. http://www.grameentelecom.net.bd/village-phone.html

[22] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & Social Media in the Context of the Arab Gulf. In *Proceedings of the Conference on Designing Interactive Systems (DIS)*. https://doi.org/10.1145/2901790.2901873

[23] Yasemin Acar, Michael Backes, Sascha Fahl, and Simson Garfinkel. 2017. Comparing the Usability of Cryptographic APIs. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. https://www.ieee-security.org/TC/SP2017/papers/161.pdf

[24] Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2016. You Are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. In *IEEE Cybersecurity Development (SecDev)*. IEEE, 3–8. https://doi.org/10.1109/SecDev.2016.013

[25] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. https://doi.org/10.1145/322796.322806

[26] Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM. https://doi.org/10.1145/2909609.2909661

[27] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the ACM: Human Computer Interaction (PACM)*. https://doi.org/10.1145/3134652

[28] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 906–918. https://doi.org/10.1145/3025453.3025961

[29] Syed Ishtiaque Ahmed, Steven J. Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md. Rashidujjaman Rifat, A.S.M Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A Platform for Fighting Sexual Harassment in Urban Bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2695–2704. https://doi.org/10.1145/2556288.2557376

[30] Syed Ishtiaque Ahmed, Steven J. Jackson, and Md Rashidujjaman Rifat. 2015. Learning to Fix: Knowledge, Collaboration and Mobile Phone Repair in Dhaka, Bangladesh. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM Press, 1–10. https://doi.org/10.1145/2737856.2738018

[31] Khurshid Alam and Ajay Mahal. 2014. Economic Impacts of Health Shocks on Households in Low and Middle Income Countries: A Review of the Literature. *Globalization and Health* 10 (April 2014), 21. https://doi.org/10.1186/1744-8603-10-21

[32] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 297–308. https://www.usenix.org/conference/soups2015/proceedings/presentation/alghamdi

[33] Ross Anderson. 2001. Why Information Security is Hard - An Economic Perspective. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. IEEE Comput. Soc, 358–365. https://doi.org/10.1109/ACSAC.2001.991552

[34] Yaw Anokwa, Nyoman Ribeka, Tapan Parikh, Gaetano Borriello, and Martin C. Were. 2012. Design of a Phone-based Clinical Decision Support System for Resource-limited Settings. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 13–24. https://doi.org/10.1145/2160673.2160676

[35] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society* 20, 5 (Nov. 2004), 313–324. https://doi.org/10.1080/01972240490507956

[36] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric Brewer. 2011. Computing Security in the Developing World: A Case for Multidisciplinary Research. In *Proceedings of the ACM Workshop on Networked Systems for Developing Regions (NSDR)*. ACM, 39–44. https://doi.org/10.1145/1999927.1999939

[37] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. 2002. User Authentication Through Keystroke Dynamics. *ACM Transactions on Information and System Security (ACM TISSEC)* 5, 4 (Nov. 2002), 367–397. https://doi.org/10.1145/581271.581272

[38] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. 2017. When the Internet Goes Down in Bangladesh. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*. ACM, 1591–1604. https://doi.org/10.1145/2998181.2998237

[39] Jon Bird, Peter Byass, Kathleen Kahn, Paul Mee, and Edward Fottrell. 2013. A Matter of Life and Death: Practical and Ethical Constraints in the Development of a Mobile Verbal Autopsy Tool. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1489–1498. https://doi.org/10.1145/2470654.2466198

[40] Sara Boettiger, Kentaro Toyama, and Rezwana Abed. 2012. Natural Obsolescence of Village Phone. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 221–229. https://doi.org/10.1145/2160673.2160702

[41] Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. 2017. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. https://www.semanticscholar.org/paper/582606bb70ac6060066890ec7967f31ce155503b

[42] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. http://dx.doi.org/10.1191/1478088706qp063oa

[43] Eric Brewer, Michael Demmer, Bowei Du, Melissa Ho, Matthew Kam, Sergiu Nedevschi, Joyojeet Pal, Rabin Patra, Sonesh Surana, and Kevin Fall. 2005. The Case for Technology in Developing Regions. *Computer* 38, 6 (May 2005), 25–38. https://doi.org/10.1109/MC.2005.204

[44] Mercy Buku and Rafe Mazer. 2017. *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*. Technical Report. CGAP. http://www.cgap.org/publications/fraud-mobile-financial-services

[45] Judith Butler. 2006. *Gender Trouble: Feminism and the Subversion of Identity* (first ed.). Routledge.

[46] Sam Castle, Fahad Pervaiz, Galen Weld, and Franziska Roesner. 2016. Let’s Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *Proceedings of the ACM Symposium on Computing for Development (ACM DEV)*. http://dl.acm.org/citation.cfm?id=3001919

[47] Jay Chen, Azza Abouzied, David Hutchful, Joy Ming, and Ishita Ghosh. 2016. Printr: Exploring the Potential of Paper-based Tools in Low-resource Settings. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 23:1–23:11. https://doi.org/10.1145/2909609.2909649

[48] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 129–142. https://www.usenix.org/conference/soups2014/proceedings/presentation/chen

[49] Marshini Chetty, Richard Banks, A.J. Brush, Jonathan Donner, and Rebecca Grinter. 2012. You’re Capped: Understanding the Effects of Bandwidth Caps on Broadband Use in the Home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 3021–3030. https://doi.org/10.1145/2207676.2208714

[50] Marshini Chetty, Hyojoon Kim, Srikanth Sundaresan, Sam Burnett, Nick Feamster, and W. Keith Edwards. 2015. uCap: An Internet Data Management Tool For The Home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 3093–3102. https://doi.org/10.1145/2702123.2702218

[51] Camille Cobb, Samuel Sudar, Nicholas Reiter, Richard Anderson, Franziska Roesner, and Tadayoshi Kohno. 2016. Computer Security for Data Collection Technologies. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 2:1–2:11. https://doi.org/10.1145/2909609.2909660

[52] Open Science Collaboration. 2015. Estimating the Reproducibility of Psychological Science. *Science* 349, 6251 (Aug. 2015), aac4716. https://doi.org/10.1126/science.aac4716

[53] Henry Corrigan-Gibbs and Jay Chen. 2014. FlashPatch: Spreading Software Updates over Flash Drives in Under-connected Regions. In *Proceedings of the ACM Symposium on Computing for Development (ACM DEV)*. ACM, 1–10. https://doi.org/10.1145/2674377.2674384

[54] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. ACM, 739–749. https://doi.org/10.1145/2660267.2660271

[55] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*. ACM, 1416–1426. https://doi.org/10.1145/2675133.2675225

[56] Liza Dawson and Nancy E. Kass. 2005. Views of US Researchers about Informed Consent in International Collaborative Research. *Social Science & Medicine* 61, 6 (Sept. 2005), 1211–1222. https://doi.org/10.1016/j.socscimed.2005.02.004

[57] Antonella De Angeli and Leantros Kyriakoullis. 2006. Globalisation vs. Localisation in E-Commerce: Cultural-aware Interaction Design. In *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI)*. ACM, 250–253. https://doi.org/10.1145/1133265.1133314

[58] Nicola Dell and Neha Kumar. 2016. The Ins and Outs of HCI for Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2220–2232. https://doi.org/10.1145/2858036.2858081

[59] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. Yours is Better!: Participant Response Bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. https://doi.org/10.1145/2207676.2208589

[60] Stefan Dercon and John Hoddinott. 2003. *Health, Shocks and Poverty Persistence*. Technical Report 008. World Institute for Development Economic Research (UNU-WIDER). https://ideas.repec.org/p/unu/wpaper/dp2003-08.html

[61] Audrey Desjardins, Ron Wakkary, and William Odom. 2015. Investigating Genres and Perspectives in HCI Research on the Home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 3073–3082. https://doi.org/10.1145/2702123.2702540

[62] Catherine D'Ignazio, Alexis Hope, Becky Michelson, Robyn Churchill, and Ethan Zuckerman. 2016. A Feminist HCI Approach to Designing Postpartum Technologies: "When I First Saw a Breast Pump I Was Wondering if It Was a Joke". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2612–2622. https://doi.org/10.1145/2858036.2858460

[63] Leslie L. Dodson, S. Revi Sterling, and John K. Bennett. 2013. Minding the Gaps: Cultural, Technical and Gender-based Barriers to Mobile Use in Oral-language Berber Communities in Morocco. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 79–88. https://doi.org/10.1145/2516604.2516626

[64] Pankaj Doke and Anirudha Joshi. 2015. Mobile Phone Usage by Low Literate Users. In *Proceedings of the India HCI Conference on Human Computer Interaction (IndiaHCI)*. ACM, 10–18. https://doi.org/10.1145/2835966.2835968

[65] Jonathan Donner. 2008. Research Approaches to Mobile Use in the Developing World: A Review of the Literature. *The Information Society* 24 (2008), 140–159. https://doi.org/10.1080/01972240802019970

[66] Michaelanne Dye, Annie Antón, and Amy S. Bruckman. 2016. Early Adopters of the Internet and Social Media in Cuba. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*. ACM, 1295–1309. https://doi.org/10.1145/2818048.2819947

[67] Michaelanne Dye, David Nemer, Laura R. Pina, Nithya Sambasivan, Amy S. Bruckman, and Neha Kumar. 2017. Locating the Internet in the Parks of Havana. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 3867–3878. https://doi.org/10.1145/3025453.3025728

[68] Ivan Flechais, Marina Jirotka, and Deena Alghamdi. 2013. In the Balance in Saudi Arabia: Security, Privacy and Trust. In *Proceedings of the Conference on Human Factors in Computing Systems: Extended Abstracts (CHI EA)*. ACM, 823–828. https://doi.org/10.1145/2468356.2468503

[69] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the Applicability of Touchscreen Input As a Behavioral Biometric for Continuous Authentication. *IEEE Transactions on Information Forensics and Security* 8, 1 (Jan. 2013), 136–148. https://doi.org/10.1109/TIFS.2012.2225048

[70] Sheera Frenkel. 2018. Iranian Authorities Block Access to Social Media Tools. *The New York Times* (Jan. 2018). https://www.nytimes.com/2018/01/02/technology/iran-protests-social-media.html

[71] Annie George and Surinder Singh Jaswal. 1995. Understanding Sexuality: An Ethnographic Study of Poor Women in Bombay, India. Washington DC International Center for Research on Women [ICRW]. https://www.popline.org/node/304873

[72] Sanjay Ghosh, Sarita Seshagiri, and Aditya Ponnada. 2016. Exploring Regional User Experience for Designing Ultra Low Cost Smart Phones. In *Proceedings of the Conference on Human Factors in Computing Systems: Extended Abstracts (CHI EA)*. ACM, 768–776. https://doi.org/10.1145/2851581.2851597

[73] Ricardo Gomez, Luis Fernando Baron-Porras, and Brittany Fiore-Silfvast. 2012. The Changing Field of ICTD: Content Analysis of Research Published in Selected Journals and Conferences, 2000-2010. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. https://doi.org/10.1145/2160673.2160682

[74] Ram D. Gopal and G. Lawrence Sanders. 2000. Global Software Piracy: You Can't Get Blood out of a Turnip. *Commun. ACM* 43, 9 (Sept. 2000), 82–89. https://doi.org/10.1145/348941.349002

[75] Matthew Green and Matthew Smith. 2016. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy* 14, 5 (2016), 40–46. https://doi.org/10.1109/MSP.2016.111

[76] GSMA. 2015. Bridging the Gender Gap: Mobile Access and Usage in Low- and Middle-income Countries. http://www.gsma.com/mobilefordevelopment/programmes/connectedwomen/bridging-gender-gap

[77] J. Alex Halderman. 2010. To Strengthen Security, Change Developers' Incentives. *IEEE Security & Privacy* 8, 2 (2010), 79–82. https://doi.org/10.1109/MSP.2010.85

[78] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. https://doi.org/10.1145/2858036.2858273

[79] Carl Hartung, Adam Lerer, Yaw Anokwa, Clint Tseng, Waylon Brunette, and Gaetano Borriello. 2010. Open Data Kit: Tools to Build Information Services for Developing Regions. In *Proceedings of the ACM/IEEE International Conference on Information and Communication Technologies and Development*. ACM. https://doi.org/10.1145/2369220.2369236

[80] Geert Hofstede. 2011. Dimensionalizing Cultures: The Hofstede Model in Context. *Online readings in psychology and culture* 2, 1 (2011). https://doi.org/10.9707/2307-0919.1014

[81] Thorsten Holz, Norbert Pohlmann, Eric Bodden, Matthew Smith, and Jorg Hoffmann. 2016. Human-Centered Systems Security: IT Security by People for People. http://donar.messe.de/exhibitor/cebit/2017/G541499/human-centered-systems-security-eng-483137.pdf

[82] Robert Jensen. 2007. The Digital Provide: Information (Technology), Market Performance, and Welfare in the South Indian Fisheries Sector. *The Quarterly Journal of Economics* 122, 3 (Aug. 2007), 879–924. https://doi.org/10.1162/qjec.122.3.879

[83] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1647–1650. https://doi.org/10.1145/1518701.1518953

[84] Shashank Khanna, Aishwarya Ratan, James Davis, and William Thies. 2010. Evaluating and Improving the Usability of Mechanical Turk for Low-income Workers in India. In *Proceedings of the ACM Symposium on Computing for Development (ACM DEV)*. https://doi.org/10.1145/1926180.1926195

[85] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. "When I am on Wi-Fi, I am fearless": Privacy concerns & practices in everyday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1993–2002. https://doi.org/10.1145/1518701.1519004

[86] Beth E. Kolko, Emma J. Rose, and Erica Johnson. 2007. Communication As Information-seeking: The Case for Mobile Social Software for Developing Regions. In *Proceedings of the International Conference on World Wide Web (WWW)*. ACM, 863–872. https://doi.org/10.1145/1242572.1242689

[87] Deepti Kumar, David Martin, and Jacki O'Neill. 2011. The Times They Are A-changin': Mobile Payments in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1413–1422. https://doi.org/10.1145/1978942.1979150

[88] Neha Kumar, Gopal Chouhan, and Tapan Parikh. 2011. Folk Music Goes Digital in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. https://doi.org/10.1145/1978942.1979151

[89] Neha Kumar and Tapan S. Parikh. 2013. Mobiles, Music, and Materiality. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2863–2872. https://doi.org/10.1145/2470654.2481396

[90] Neha Kumar and Nimmi Rangaswamy. 2013. The Mobile Media Actor-network in Urban India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1989–1998. https://doi.org/10.1145/2470654.2466263

[91] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. Privacy in India: Attitudes and Awareness. In *Privacy Enhancing Technologies*. https://doi.org/10.1007/11767831_16

[92] Lily Kuo. 2017. Uganda has Launched a Total Social Media Blackout for the Second Time in Three Months. https://goo.gl/Ds4mj3

[93] Yong Liu, Jorge Goncalves, Denzil Ferreira, Bei Xiao, Simo Hosio, and Vassilis Kostakos. 2014. CHI 1994-2013: Mapping Two Decades of Intellectual Progress Through Co-word Analysis. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 3553–3562. https://doi.org/10.1145/2556288.2556969

[94] Alison Mathie and Gord Cunningham. 2005. Who is Driving Development? Reflections on the Transformative Potential of Asset-based Community Development. *Canadian Journal of Development Studies* 26, 1 (2005), 175–186. https://doi.org/10.1080/02255189.2005.9669031

[95] Arunesh Mathur, Brent Schlotfeldt, and Marshini Chetty. 2015. A Mixed-methods Study of Mobile Users' Data Usage Practices in South Africa. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*. ACM, 1209–1220. https://doi.org/10.1145/2750858.2804292

[96] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll Just Grab Any Device That's Closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 5921–5932. https://doi.org/10.1145/2858036.2858051

[97] Indrani Medhi, Somani Patnaik, Emma Brunskill, S. N. Nagasena Gautama, William Thies, and Kentaro Toyama. 2011. Designing Mobile Interfaces for Novice and Low-Literacy Users. *ACM Transactions on Computer-Human Interaction* 18, 1 (April 2011), 1–28. https://doi.org/10.1145/1959022.1959024

[98] Mary Meeker. 2015. 2015 Internet Trends. http://www.kpcb.com/blog/2015-internet-trends

[99] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors: Peer Versus Authoritative Sources. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*. ACM, 581–593. https://doi.org/10.1145/2998181.2998323

[100] Microsave. 2017. Assessment of AeFDS (Aadhaar Enabled Fertilizer Distribution System) Pilot. http://www.microsave.net/resource/assessment_of_aefds_aadhaar_enabled_fertilizer_distribution_system_pilot

[101] Manar Mohamed and Nitesh Saxena. 2016. Gametrics: Towards Attack-resilient Behavioral Authentication with Simple Cognitive Games. In *Proceedings of the Annual Computer Security Applications Conference*. ACM, 277–288. https://doi.org/10.1145/2991079.2991096

[102] Marie-Hélène Mottin-Sylla. 2016. The Gender Digital Divide in Francophone Africa: A Harsh Reality. https://www.apc.org/en/pubs/manuals/gender/africa/gender-digital-divide-francophone-africa-harsh-rea

[103] Joseck Luminzu Mudiri. 2013. *Fraud in Mobile Financial Services*. Technical Report. MicroSave. http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf

[104] Sarah Nadi, Stefan Krüger, Mira Mezini, and Eric Bodden. 2016. Jumping through Hoops: Why do Java Developers Struggle with Cryptography APIs?. In *Proceedings of the International Conference on Software Engineering (ICSE)*. ACM, 935–946. https://doi.org/10.1145/2884781.2884790

[105] Soud Nassir and Tuck Wah Leong. 2017. Traversing Boundaries: Understanding the Experiences of Ageing Saudis. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 6386–6397. https://doi.org/10.1145/3025453.3025618

[106] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

[107] Erick Oduor, Carman Neustaedter, Tejinder K. Judge, Kate Hennessy, Carolyn Pang, and Serena Hillman. 2014. How Technology Supports Family Communication in Rural, Suburban, and Urban Kenya. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2705–2714. https://doi.org/10.1145/2556288.2557277

[108] Anne Oeldorf-Hirsch, Jonathan Donner, and Edward Cutrell. 2012. How Bad is Good Enough?: Exploring Mobile Video Quality Trade-offs for Bandwidth-constrained Consumers. In *Proceedings of the Nordic Conference on Human-computer Interaction (NordiCHI)*. ACM, 49–58. https://doi.org/10.1145/2399016.2399025

[109] Jacki O'Neill, Kentaro Toyama, Jay Chen, Berthel Tate, and Aysha Siddique. 2016. The Increasing Sophistication of Mobile Media Sharing in Lower-Middle-Class Bangalore. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. https://doi.org/10.1145/2909609.2909656

[110] Michael Paik, Navkar Samdaria, Aakar Gupta, Julie Weber, Nupur Bhatnagar, Shelly Batra, Manish Bhardwaj, and William Thies. 2010. A Biometric Attendance Terminal and Its Application to Health Programs in India. In *Proceedings of the ACM Workshop on Networked Systems for Developing Regions (NSDR)*. ACM, 4:1–4:6. https://doi.org/10.1145/1836001.1836005

[111] Saurabh Panjwani. 2013. Practical Receipt Authentication for Branchless Banking. In *Proceedings of the ACM Symposium on Computing for Development (ACM DEV)*. ACM, 3:1–3:10. https://doi.org/10.1145/2442882.2442886

[112] Saurabh Panjwani and Edward Cutrell. 2010. Usably Secure, Low-cost Authentication for Mobile Banking. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. ACM, 4:1–4:12. https://doi.org/10.1145/1837110.1837116

[113] Saurabh Panjwani, Mohona Ghosh, Ponnurangam Kumaraguru, and Soumya Vardhan Singh. 2013. The Paper Slip Should Be There!: Perceptions of Transaction Receipts in Branchless Banking. In *Proceedings of the International Conference on Human Computer Interaction With Mobile Devices and Services (MobileHCI)*. ACM, 328–331. https://doi.org/10.1145/2493190.2493236

[114] Rabin K. Patra, Joyojeet Pal, and Sergiu Nedevschi. 2009. ICTD State of the Union: Where Have We Reached and Where are We Headed. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. https://doi.org/10.1109/ICTD.2009.5426693

[115] Nicole Perlroth. 2016. Governments Turn to Commercial Spyware to Intimidate Dissidents. *The New York Times* (May 2016). https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html

[116] Trevor Perrier, Nicola Dell, Brian DeRenzi, Richard Anderson, John Kinuthia, Jennifer Unger, and Grace John-Stewart. 2015. Engaging Pregnant Women in Kenya with a Hybrid Computer-Human SMS Communication System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1429–1438. https://doi.org/10.1145/2702123.2702124

[117] Claire Provost. 2013. Poorer Countries Need Privacy Laws as They Adopt New Technologies. *The Guardian* (Dec. 2013). http://www.theguardian.com/global-development/2013/dec/04/poorer-countries-privacy-laws-new-technology

[118] Divya Ramachandran, Matthew Kam, Jane Chiu, John Canny, and James F. Frankel. 2007. Social Dynamics of Early Stage Co-design in Developing Regions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1087–1096. https://doi.org/10.1145/1240624.1240790

[119] Nimmi Rangaswamy and Nithya Sambasivan. 2011. Cutting Chai, Jugaad, and Here Pheri: Towards UbiComp for a Global Community. *Personal and Ubiquitous Computing* 15, 6 (April 2011), 553–564. https://doi.org/10.1007/s00779-010-0349-x

[120] Agha Ali Raza, Mansoor Pervaiz, Christina Milo, Samia Razaq, Guy Alster, Jahanzeb Sherwani, Umar Saif, and Roni Rosenfeld. 2012. Viral Entertainment As a Vehicle for Disseminating Speech-based Services to Low-literate Users. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 350–359. https://doi.org/10.1145/2160673.2160715

[121] Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. 2015. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (USENIX Security)*. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/reaves

[122] Matthew Reynolds. 2018. Iran's Social Media Blackout Forces Apps to Submit or Face a Total Ban. http://www.wired.co.uk/article/iran-protests-2017-2018-twitter-telegram-instagram-censorship

[123] Md. Rashidujjaman Rifat, Jay Chen, and Kentaro Toyama. 2017. Money, God, and SMS: Explorations in Supporting Social Action Through a Bangladeshi Mosque. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 5941–5953. https://doi.org/10.1145/3025453.3025960

[124] Michael Safi. 2018. Personal Data of a Billion Indians Sold Online for £6, Report Claims. *The Guardian* (Jan. 2018). http://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar

[125] Nithya Sambasivan and Paul M. Aoki. 2017. Imagined Connectivities: Synthesized Conceptions of Public Wi-Fi in Urban India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 5917–5928. https://doi.org/10.1145/3025453.3025545

[126] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura S. Gaytán-Lugo, Matthews, Tara, Consolvo, Sunny, and Churchill, Elizabeth. 2018. "Privacy is not for me, it's for those rich women": Notions and Practices of Privacy on Shared Phones among South Asian Women. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[127] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. 2010. Intermediated Technology Use in Developing Communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2583–2592. https://doi.org/10.1145/1753326.1753718

[128] Nithya Sambasivan, Nimmi Rangaswamy, Ed Cutrell, and Bonnie Nardi. 2009. Ubicomp4D: Infrastructure and Interaction for International Development–the Case of Urban Indian Slums. In *Proceedings of the International Conference on Ubiquitous Computing (UbiComp)*. ACM, 155–164. https://doi.org/10.1145/

1620545.1620570

[129] Nithya Sambasivan, Julie Weber, and Edward Cutrell. 2011. Designing a Phone Broadcasting System for Urban Sex Workers in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 267–276. https://doi.org/10.1145/1978942.1978980

[130] Ari Schlesinger, W. Keith Edwards, and Rebecca E. Grinter. 2017. Intersectional HCI: Engaging Identity Through Gender, Race, and Class. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 5412–5427. https://doi.org/10.1145/3025453.3025766

[131] Mark B. Schmidt, Allen C. Johnston, Kirk P. Arnett, Jim Q. Chen, and Suichen Li. 1. A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness. *Journal of Global Information Management* 16, 2 (Jan. 1), 91–103. https://doi.org/10.4018/jgim.2008040106

[132] Amnon Shiloah. 1997. Music and Religion in Islam. *Acta Musicologica* 69, 2 (1997), 143–155. https://doi.org/10.2307/932653

[133] Sara Sinclair and Sean W. Smith. 2010. What's Wrong with Access Control in the Real World? *IEEE Security & Privacy* 8, 4 (July 2010), 74–77. https://doi.org/10.1109/MSP.2010.139

[134] Ranjit Singh and Steven J. Jackson. 2017. From Margins to Seams: Imbrication, Inclusion, and Torque in the Aadhaar Identification Project. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 4776–4824. https://doi.org/10.1145/3025453.3025910

[135] Thomas N. Smyth, John Etherton, and Michael L. Best. 2010. MOSES: Exploring New Ground in Media and Post-conflict Reconciliation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1059–1068. https://doi.org/10.1145/1753326.1753484

[136] Thomas N. Smyth, Satish Kumar, Indrani Medhi, and Kentaro Toyama. 2010. Where There's a Will There's a Way: Mobile Media Sharing in Urban India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 753–762. https://doi.org/10.1145/1753326.1753436

[137] Daniel J. Solove. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press.

[138] S. Revi Sterling and Nimmi Rangaswamy. 2010. Constructing Informed Consent in ICT4D Research. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 46:1–46:9. https://doi.org/10.1145/2369220.2369264

[139] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. 2018. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 536:1–536:13. https://doi.org/10.1145/3173574.3174110

[140] Leila Takayama, Caroline Pantofaru, David Robson, Bianca Soto, and Michael Barry. 2012. Making Technology Homey: Finding Sources of Satisfaction and Meaning in Home Automation. In *Proceedings of the International Conference on Ubiquitous Computing (UbiComp)*. ACM, 511–520. https://doi.org/10.1145/2370216.2370292

[141] Charlotte Tang, Yunan Chen, Bryan C. Semaan, and Jahmeilah A. Roberson. 2015. Restructuring Human Infrastructure: The Impact of EHR Deployment in a Volunteer-Dependent Clinic. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*. ACM, 649–661. https://doi.org/10.1145/2675133.2675277

[142] Aditya Vashistha, Edward Cutrell, Gaetano Borriello, and William Thies. 2015. Sangeet Swara: A Community-Moderated Voice Forum in Rural India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 417–426. https://doi.org/10.1145/2702123.2702191

[143] Aditya Vashistha, Neha Kumar, Anil Mishra, and Richard Anderson. 2016. Mobile Video Dissemination for Community Health. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*. ACM, 20:1–20:11. https://doi.org/10.1145/2909609.2909655

[144] Aditya Vashistha, Fabian Okeke, Richard Anderson, and Nicola Dell. 2018. "You Can Always Do Better!": The Impact of Social Proof on Participant Response Bias. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM. https://doi.org/10.1145/3173574.3174126

[145] Aditya Vashistha, Pooja Sethi, and Richard Anderson. 2018. BSpeak: An Accessible Voice-based Crowdsourcing Marketplace for Low-Income Blind People. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 57:1–57:13. https://doi.org/10.1145/3173574.3173631

[146] Daniel Wagner, Andrew Rice, and Alastair Beresford. 2013. Device Analyzer: Large-scale Mobile Data Collection. In *Proceedings of the Big Data Analytics workshop (in conjunction with ACM Sigmetrics)*. http://www.cl.cam.ac.uk/~acr31/pubs/wagner-bigdata.pdf

[147] Marion Walton, Gary Marsden, Silke Hassreiter, and Sena Allen. 2012. Degrees of Sharing: Proximate Media Sharing and Messaging by Young People in Khayelitsha. In *Proceedings of the International Conference on Human Computer Interaction With Mobile Devices and Services (MobileHCI)*. ACM, 403–412. https://doi.org/10.1145/2371574.2371636

[148] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. ACM, 11:1–11:16. https://doi.org/10.1145/1837110.1837125

[149] Rick Wash and Mary Ellen Zurko. 2017. Usable Security. *IEEE Internet Computing* 21, 3 (May 2017), 19–21. https://doi.org/10.1109/MIC.2017.69

[150] Max L. L. Wilson, Paul Resnick, David Coyle, and Ed H. Chi. 2013. RepliCHI: The Workshop. In *Proceedings of the Conference on Human Factors in Computing Systems: Extended Abstracts (CHI EA)*. ACM, 3159–3162. https://doi.org/10.1145/2468356.2479636

[151] Marisol Wong-Villacres and Shaowen Bardzell. 2011. Technology-mediated Parent-child Intimacy: Designing for Ecuadorian Families Separated by Migration. In *Proceedings of the Conference on Human Factors in Computing Systems: Extended Abstracts (CHI EA)*. ACM, 2215–2220. https://doi.org/10.1145/1979742.1979877

[152] Susan P. Wyche, Thomas N. Smyth, Marshini Chetty, Paul M. Aoki, and Rebecca E. Grinter. 2010. Deliberate Interactions: Characterizing Technology Use in Nairobi, Kenya. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2593–2602. https://doi.org/10.1145/1753326.1753719

[153] Jing Xie, Heather Richter Lipford, and Bill Chu. 2011. Why do Programmers Make Security Errors?. In *Proceedings of the IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, 161–164. https://doi.org/10.1109/VLHCC.2011.6070393

[154] Ed Yong. 2016. Psychology's Replication Crisis Can't Be Wished Away. *The Atlantic* (March 2016). https://www.theatlantic.com/science/archive/2016/03/psychologys-replication-crisis-cant-be-wished-away/472272/

[155] Mary Ellen Zurko and Richard T. Simon. 1996. User-centered Security. In *Proceedings of the Workshop on New Security Paradigms Workshop (NSPW)*. ACM, 27–33. https://doi.org/10.1145/304851.304859