USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

"No, I Can't Be a Security Personnel on Your Phone": Security and Privacy Threats From Sharing Infrastructure in Rural Ghana

Emmanuel Tweneboah, *Max Planck Institute for Security and Privacy;* Collins W. Munyendo, *Max Planck Institute for Security and Privacy and The George Washington University;* Yixin Zou, *Max Planck Institute for Security and Privacy*

https://www.usenix.org/conference/usenixsecurity25/presentation/tweneboah

This paper is included in the Proceedings of the 34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the 34th USENIX Security Symposium is sponsored by USENIX.

"No, I Can't Be a Security Personnel on Your Phone": Security and Privacy Threats From Sharing Infrastructure in Rural Ghana

Emmanuel Tweneboah[1], Collins W. Munyendo[1,2], Yixin Zou[1]
[1]*Max Planck Institute for Security and Privacy,* [2]*The George Washington University*

Abstract

We examine how rural communities in Ghana adopt workarounds to access electricity and mobile networks and the impact of these workarounds on their digital security and privacy. Through 41 field interviews, we find that participants largely rely on intermediaries to charge their mobile devices and to perform activities that require a stable mobile network. These practices often result in concerns over device loss, unauthorized access of personal information, and eavesdropping. In response, participants adopt protective measures, such as using screen and app locks when handing their devices to intermediaries. Others speak in local languages to 'encrypt' verbal communication when sharing the same 'network zone' with others. Though economically prudent, the reliance on intermediaries introduces social friction where participants suppress their concerns to preserve social relations and continual support. We conclude with recommendations on how various stakeholders, including practitioners and researchers, can work toward improving the security and privacy of users in resource-constrained settings, e.g., by rethinking access control for community-level device and network sharing.

1 Introduction

People in developing regions are among at-risk technology users. Warford et al define at-risk users as people who experience risk factors that augment or amplify their chances of being digitally attacked and/or suffering disproportionate harms [104]. Amid infrastructural limitations in developing regions [63] and growing digitization of essential services, inadequate access to critical infrastructure and resources often creates conditions of heightened security and privacy risks [82]. For instance, in Kenya, many users access essential services through public computers at cybercafes, where risks emerge when cafe managers set simple passwords or directly manage passwords for their customers [69]. In Lebanon, unstable electricity access leads to reliance on generator cartels who exploit this population, generating increased financial insecurities among users [63]. Coupled with social norms in the Global South, access restrictions jeopardize women's autonomy in tech access, impacting their privacy [6, 29, 85, 93].

These challenges are exacerbated in more rural areas, where limited infrastructure and resources force residents to develop workarounds for their technology access [19, 40, 54]. For instance, rural residents in Sierra Leone charge their electronic gadgets at community charging centers [54]. Schoolers in rural Philippines traveled to neighboring communities for internet access during the COVID-19 pandemic [40]. Prior work on rural communities' coping mechanisms in the face of resource constraints [8] has covered contexts such as food security [43], disaster management [25, 59], health and education [1, 40], farming and shelter [1, 23]. However, much less is known about the security and privacy (S&P) implications of rural communities sharing access to infrastructure.

Our research focuses on the rural Ghanaian context. While Ghana has recently enacted several technology-related regulations [12, 33], the way Ghanaians perceive, understand, and manage their S&P remains largely unexplored. While Chen et al. studied the security perception of technology users in Ghana [28], the study was limited to *urban* areas and *internet* users. Yet, in recent years, technology usage has become more prevalent even in rural Ghana [70, 88]. Unfortunately, rural Ghana has limited coverage of electricity [15] and telecom infrastructure [39]. With access to electricity and mobile networks being the basic infrastructure for mobile device usage, we anticipate that any access limitation to such infrastructure forces users, particularly in rural Ghana, into adopting workarounds for access that may expose them to S&P risks. Thus, we seek to answer the following research questions:

RQ1: How do participants in rural Ghana access mobile networks and charge their mobile devices?

RQ2: What S&P challenges do they face, and what concerns do they have when adopting workarounds to access electricity and mobile networks?

RQ3: What protective behaviors do they adopt to address these challenges and concerns, if any?

To answer these questions, we conducted in-depth semi-

structured interviews with two sets of participants in rural Ghana: 10 providers (i.e., community members who provide charging services to others) and 31 clients (i.e., users who have limited access to mobile networks and electricity). We find that many clients rely on charging shops and/or families and friends in nearby communities, as a form of "human infrastructure" to secure charging access. To send and retrieve their devices from the charging places, many clients turn to other people (i.e., intermediaries) due to the transportation cost burden of doing it themselves. This, coupled with clients leaving their devices at the charging places (sometimes in the magnitude of days) exposes their devices to possible theft and unauthorized access of personal information.

For mobile network access, clients use vantage places (i.e., 'network zones') around their homes, nearby farms, and school compounds. Some clients rely on intermediaries to perform network-required activities (e.g., creating social media accounts) because of low digital literacy and because clients cannot always accompany the intermediaries. Additionally, network zones are shared by many clients at the same time, leading to concerns over eavesdropping and shoulder surfing.

While prior work has identified how cultural norms shape practices around resource sharing, such work primarily focuses on domestic settings [5, 29, 85]. Extending the inquiry to two public settings, our findings suggest that access limitations in rural Ghana as well as Ghanaian culture that emphasizes 'helping your neighbors' [41, 79] foster the prevalence of intermediaries in access workarounds. However, the reliance on intermediaries presents social friction [107], making clients suppress their concerns in the event of misuse or else risk not being helped. Consistent with prior work in resource-sharing settings, rural residents in Ghana adopt some access control measures [5,32,69,85], but the efficacy of some measures, such as screen locks and removing SIM cards, remains unclear. Ultimately, infrastructural failure subjects rural residents to threats beyond security and privacy threats, including amplified everyday insecurities [64], affecting their well-being and survival in their tech use. We conclude with recommendations and directions for future work to better support technology users in resource-constrained settings.

2 Background on Electricity and Mobile Network Coverage in Rural Ghana

Compared to other African countries, Ghana has a high electricity access rate of 89% [15]. Nonetheless, the country still experiences power instability due to unpaid utilities, maintenance failure, supply shortage, among others [3, 57, 95]. The persistent power outages between 2012 to 2024, sometimes lasting for about 12 hours a day [22], are captured by Akan[1] words such as *Dumsor* (meaning turn off and turn on).

[1] One of the largest tribal groups in Ghana

While Ghana continues its efforts to enhance power accessibility and stability, numerous rural regions remain unconnected to the national grid [55]. According to the World Bank, the rural electricity access rate in Ghana was approximately 77% in 2023 [15]. Although the government aims to achieve universal electrification by 2030 [31], the current pace of progress raises concerns regarding the attainability of this goal. In various parts of the country, rural inhabitants have expressed dissatisfaction over perceived neglect and prolonged delays in electrification projects [2, 78].

Ghana's mobile network industry is dominated by three operators: MTN, Telecel, and AirtelTigo. The country's highest mobile network standard currently available is 4G, with plans for 5G underway [76]. While the International Telecommunication Union (ITU) projects Ghana's network coverage to be 99% for at least LTE [71], local media report poor network experiences, causing frustration among users [42, 98, 101]. In rural areas, especially, low coverage continues to be a challenge, prompting local leaders and residents across the country to desperately appeal to the government and stakeholders for mobile network services [42, 52, 60, 101].

Despite government efforts to improve electricity and mobile network access, instability of critical infrastructure continues to impact many Ghanaians [74], especially rural residents.

3 Related Work

3.1 Security, Privacy, and Infrastructuring

Hussain et al. define infrastructure as "a coordinated combination or assemblage of humans and objects that are organized for accomplishing a certain task" [49]. Common examples of infrastructure are public transit systems, water supply, and telecommunications. We focus on electricity and mobile networks as two types of infrastructure in our study.

McClearn et al. conceptualize *infrastructuring* as "well-established practices developed to overcome particular institutional and systemic failures" when infrastructures fail or are lacking [63]. Prior work has examined infrastructuring practices adopted by various groups such as migrants [30], refugees [49, 84], activists [32, 45], women [18, 94, 105], domestic workers [92], LGBTQ+ [51], and people with low socioeconomic status [20, 46, 56, 69]. People across these contexts engage with infrastructuring work to secure access to information [45, 86], internet [32, 36], or electricity [63]; to construct and reflect on their identities [63, 89]; and to instigate and enact change [80]. For instance, people living in slums in India rely on social circles for information passage and device access [86, 87]. Faced with access limitations in Bangladesh, Rohingya refugees infrastructure their hopes through solidarity, leadership, and negotiation to secure their access to SIM cards, phone repair, and charging services [49].

While necessary to circumvent access limitations, prior work shows that infrastructuring practices introduce relational

tensions and insecurities such as misinformation, financial exploitation, and physical abuse [32, 45, 63]. McClearn et al. propose *security patchwork* as a concept to understand this phenomenon: "While infrastructuring contributes to everyday security through securing access to resources and services, it also foregrounds forms of insecurity, demonstrating the (security) fragility of the patches made through infrastructuring" [63]. By focusing on access practices by mobile users in rural Ghana in securing mobile network and charging services, we broaden this inquiry to populations who experience S&P threats as a result of infrastructural failure [63]. Depleted resources could potentially undermine their resilience in adopting secure practices in their tech access [82], and the S&P risks in their workarounds can be viewed as a new form of security patchworking in the rural Ghana context.

3.2 Resource Sharing in the Global South

S&P risks can manifest in negotiated access to shared resources, which encompass many things (e.g., online accounts, devices, cars, and homes) and happen in various settings (e.g., intimate relationships, families and households, social acquaintances, and in public) [107]. Resource sharing can be triggered by a wide array of factors, from trust building [58] to convenience [61] and a lack of ownership of personal devices [4, 5, 7, 16, 103]. Particularly in the Global South, economic constraints and cultural norms lead to shared use and patriarchal control of technological resources [5, 6, 29].

Prior work has documented how device ownership and identity management are influenced by the hierarchical power structure in societies such as in Bangladesh [5, 6, 93], India [85], Malawi [29], and Saudi Arabia [7]. For instance, Ahmed et al revealed the use of male identity information in registering SIMs for their female spouses in Bangladesh, resulting in ownership tension [6]. In South Asia, cultural expectations dictate that women should share mobile phones with family members and that their digital activities be open to scrutiny by family members [85]. In studying women's perspectives on the use of smart home security systems in Malawi's patriarchal society, Chidziwisano and Jalakasi reveal women's concerns about their husbands using the system to regulate their food preparation and consumption level [29].

Similar to other countries in the Global South, cultural norms in Ghana compel people to help others when they are in need [79], for example by sharing food, shelter, and traditional medicine [21]. With rural residents in Ghana facing infrastructural limitations, we explore how social norms may shape their workarounds in accessing critical infrastructure.

4 Methods

We explain our selection of communities, participant recruitment, interview process, data analysis, and potential limitations. Figure 1 shows our study sites from the field work.

(a) Phones at a charging center.

(b) Residents at a network zone.

Figure 1: Pictures from field research in rural Ghana.

4.1 Selection of Communities

We selected five rural communities in Ghana with limited mobile networks and/or electricity access as potential sites for recruiting participants (see Appendix A). Four communities have limited access to electricity and mobile networks; one has a dedicated charging shop. The fifth community has access to public electricity (i.e., reliable electric service exists) but limited access to a mobile network. Within the rural community criterion (i.e., fewer than 5k inhabitants defined by the Ghana Statistical Service) [90], we prioritized rural communities with at least one basic public school (at any level from kindergarten to junior high school) to ensure there was still a sizable population for our recruitment. All communities are based in the Upper Denkyira West District in Southern Ghana. This location was chosen as the lead researcher, a Ghanaian, used to work there as a public school teacher and field officer, and was thus familiar with the area. The district had over 91k residents according to GSS census data in 2021 [90].

The lead researcher recruited at least one contact person from each community; all of them were public school teachers within their respective communities. The contacts helped introduce the lead researcher to the community leaders, or

Table 1: Client Demographics (n=31).

Demographic	Category	No.	%
Gender	Men	16	51.6
	Women	15	48.4
Age	18-30	16	51.6
	31-40	6	19.3
	41-60	9	29.1
Occupation	Farming	11	35.5
	Trading	6	19.4
	Gold Mining	6	19.4
	Auto Mechanic	3	9.7
	Teaching	1	3.2
	Hairstyling	1	3.2
	Tailoring	1	3.2
	No Occupation	2	6.5
Education	Primary	8	25.8
	High School	16	51.6
	Diploma	1	3.2
	Bachelor	1	3.2
	No School	5	16.1
Mobile Device Ownership	Smartphones	23	53.5
	Feature Phone	16	37.2
	Laptop	3	7.0
	Smart watch	1	2.3

"elders".[2] The contacts also assisted in recruiting participants, as well as explaining the study's purpose and getting consent. A day before formal interviews, the lead researcher and their designated contact visited the community's elders to introduce the researcher. During these visits, the lead researcher familiarized themselves with the community while arranging the interview dates with participants. While we did not engage the participants through the elders, meeting with the elders before the field interviews aligns with the protocol that field officers in Ghana follow during data collection. It also aligns with best practices adopted by prior studies in rural Africa [72, 73, 106], which emphasized the importance of identifying community liaisons to enhance trust.

4.2 Recruitment of Participants

We recruited two participant groups: *clients* and *providers*. Clients have limited access to electricity and/or mobile networks while providers offer charging services to those living in areas with limited electricity access, for a fee or for free. We recruited 31 participants for the client group (see Table 1). Participants skewed toward younger adults, with about half (51.6%) of them being men. They had all lived in the selected community for the past six months.All participants had at least one type of mobile device, including a feature phone, smartphone, tablet, or laptop.

We recruited 10 participants for the provider group. Providers' age ranged from 21 to 50 years old, and eight of them were men. Eight providers had completed high school, and the remaining two had primary and college education. Nine of them provided their charging services in towns outside their communities. Thus, their services were located in nearby towns, and only one community had a dedicated charging shop. The average distance between the client and provider communities is about 5 km. The primary means of commute is via commercial motorbikes, which cost between 10 and 30 Ghanaian cedis. Half of the providers offer their services at a standard fee to all clients, while the other half do it for free. For the free providers, all of them were private residences of a client's family members or friends. For the paid providers, they primarily offer the services through a charging shop.

4.3 Interview Process

The lead researcher conducted 41 in-depth semi-structured field interviews in June 2024. Given the exploratory nature of our research questions, we adopted a qualitative approach to give us insight into the access experience of participants. Additionally, our research site's limited network necessitates the use of in-person field interviews. Given the study's focus on infrastructure, field interviews provided the researchers with lived experiences of infrastructural failure and a deeper understanding of participants' access challenges.

Iteratively, we designed interview protocols for the two groups of participants. The client protocol covered questions about the clients' demographics, general use of mobile devices, electricity access, and mobile network access. Specifically, we inquired about how they accessed electricity and mobile networks, experiences when charging devices, and concerns and protective measures as they adopted workarounds to meet their needs.[3] The provider protocol covered questions about the provider's demographics, the charging process at their facilities, and any concerns and measures they adopted to protect the mobile devices they managed. We provide the full interview protocol in an online repository.[4]

Due to travel logistics, the lead researcher conducted interviews in the communities linearly, one community after another. Within each community, interviews were conducted with clients and providers alternately, depending on the participant's availability. The clients' and free providers' interviews were all conducted at their residences, while the paid

[2] The leaders included chiefs, unit committee members, and a secretary to a chief. While Ghana has a statutory definition for these portfolios, we do not claim that the leaders we met are or are not the rightful people to be in such positions. Rather, we refer to them as elders — "custodian of wisdom, experience, and tradition ... with significant weight of opinions in a community decision-making processes" [99] — with whom the lead researcher met to discuss our study's purpose prior to the field interviews.

[3] Four clients lived in a community with public electricity and had access to it in their residences; we skipped the electricity questions for these clients. Since none of the communities had total network coverage, we interviewed all clients on mobile network access.

[4] https://osf.io/rbuv6?view_only=074e13b405324afcbb90d47f7aa6db4c

providers' interviews occurred at their shops. Among all interviews, 39 were conducted in Twi – the most widely spoken local language in Ghana [50] – and two in English.

The interviews were conducted in two phases. During the first phase, seven participants were interviewed, including five clients and two providers. The research team then met to discuss the preliminary findings based on translated English transcripts to ensure alignment with the research questions. During the second phase, the same protocols were used to interview an additional 34 participants, including 26 clients and eight providers. The lead researcher conducted all interviews, providing them with insights into the saturation of the data. After the 36th interview, no new insights emerged. Five additional interviews were conducted to confirm saturation.

With participant consent, we audio-recorded all the interviews. Each interview lasted an average of 30 minutes (min: 10; max: 56). Upon consultation with designated contact persons, we compensated participants 60 Ghanaian cedis for a half-day, equivalent to two to three hours of farm labor around the research sites. This was an appropriate figure considering that participants had to wait for the researcher, potentially affecting their day's economic activities. By mutual agreement, each contact person was compensated with 100 Ghanaian cedis for each day they assisted us, covering activities from recruitment through to data collection.

4.4 Data Analysis

Since almost all interviews were conducted in Twi, the lead researcher simultaneously transcribed and translated the first six interview recordings to English. The remaining 35 audio files were transcribed and translated with the help from a freelancer we contracted in Ghana. The lead researcher coordinated with the freelancer to ensure accuracy and consistency.

Using MAXQDA, we then analyzed the interview data qualitatively using open coding and axial coding [83], assigning codes to individual segments of a transcript and categorizing codes into broader categories or themes. The lead researcher worked with the second author to code the first transcript together and establish the structure of the codebook. Then, the lead researcher coded all transcripts. Since the lead researcher has lived experiences in Ghana and the second author has conducted extensive research on other developing countries, the goal of the coding process was to develop themes and concepts instead of seeking agreement [65]. Thus, we triangulated our coding and analysis, frequently discussing, reconciling, and clarifying potential confusion and disagreements. Thus, there was no need to compute inter-rater reliability. We include our detailed codebook in an online repository.[5]

When presenting findings, we refrain from showing the exact frequency of codes or quantifying different patterns as doing so might imply our findings are generalizable. Instead, we present the general themes that emerged. Similar to prior work [17, 37, 109], we describe the prevalence of themes as follows: a few (0-20%), some (21-40%), about half (41-60%), many (61-80%), and almost all (81-100%).

[5] https://osf.io/aqxb5?view_only=d1575225a62e47f1ac9d0eb28ced1497

4.5 Limitations

Typical with interviews, participants might over- or under-report their experiences. Demand characteristics bias (i.e., adjusting responses to the investigator's expectation) could be more salient in studies with underprivileged populations when a 'foreign' researcher is actively involved [35]. Given our focus on rural populations, we mitigated this by allowing the contact persons and only the lead researcher (who had lived experience in rural Ghana) to engage with participants. To avoid priming, we asked generic questions at the beginning (e.g., "What are the things you do not like about this [charging] place?") before probing into the security and privacy aspects later in the interview. Sampling bias might also have been influential, as the lead researcher's access to prospective participants was limited by geographic and language barriers. We mitigated this by recruiting participants from five different rural communities within Ghana, with varying sizes and facilities, for diverse participant insights.

5 Results

Here, we present findings related to participants' access to electricity for charging their mobile devices (§5.1 to §5.3), drawing on both clients' and providers' perspectives, followed by access to mobile networks (§5.4 to §5.6), which only applies to clients. For both settings, the findings cover participants' general infrastructuring practices, S&P risks and concerns, and protective measures. When presenting participant quotes, "C" represents clients while "P" represents providers.

5.1 Infrastructuring Access to Charging

5.1.1 Client Considerations and Provider Motivations

Reliance on social circles and charging shops for charging access. To secure access to charging services, client engage in infrastructuring practices – the everyday work of sustaining and adapting shared resources [63] – by turning to their social circles and charging shops. Clients in communities with no dedicated charging shops charge their mobile devices at their friends' and relatives' homes in nearby communities. Even in the community with a charging shop, clients there still go to adjacent communities to access charging services. This happens when clients travel to the community for other business or when charging fees are unaffordable, prompting them to turn to social circles in cities at no or low cost. C03 described, *"There will be some days I may not have money*

to go and charge it over here. So I give it to someone I know who lives in town [with electricity] to charge for me."

Some paid providers operate other businesses such as a mobile money services, tailoring, and a printing press as their main activities while providing the charging service on the side. As a result, these providers have a higher number of customers, including clients seeking charging devices. The charging cost ranges from one to five Ghanaian cedis, depending on the location, device type, and the power source. Explaining this pricing dynamics, P01 remarked:

> *"It's three cedis for every phone. But when the main electricity goes off, and we turn on our generator, the Android phone is five cedis. The keypad [feature phone] is three cedis."*

Clients mostly travel to the charging communities using commercial motorbikes. While all our studied communities have public basic schools, many of the schools are up to primary level (grade 12), forcing the students in the higher levels to attend schools in nearby towns. These students usually walk to school in nearby towns each day, and some clients rely on them to take their devices for charging.

As free providers mostly charge devices for their friends and family, none of them mentioned charging a fee. Similarly, some clients mentioned their relatives would charge their devices for free. This behavior aligns with Ghanaian society's expectation that one should support their family [41], making it morally unacceptable to collect money from one's immediate relatives for charging "just a phone."

Trust, cost, and trade-off in clients' choice of charging place. Due to the limited number of providers, clients' primary consideration when choosing providers is accessibility, indicating they mostly don't have an option. For those who rely on free providers, they mainly consider their personal relationships and the trust established with the provider. As C28 recounted: *"At my friend's place, I enter myself and plug it in. At this place, it's almost like I'm charging it in my own room."* In the community with a local charging service, clients frequently mentioned the cost and security implications of distance, time, and transportation fees as key factors. Thus, nearly all clients prefer to charge their devices in their communities. Explaining the benefits of proximity, C02 shared:

> *"If there should be something important, I can just go for it, but if I send it to Nkotimso (next town), I would have to wait till the next morning. Or you will have to pay for a motorcycle at an amount of 30 cedis. So I prefer charging it here."*

Notwithstanding the close proximity and presence of the charging shop in the community, some clients still face difficult trade-offs when navigating the charging process. For instance, C04 shared she had to occasionally leave her infant child alone in a room at home to go and charge her device, potentially putting the child's safety at risk.

Social responsibility and financial benefits drive charging provisioning. On their motivations for establishing the charging services, providers mentioned doing it as a way of providing social support to others in less privileged communities and for economic benefits. On the social factor, free providers often had lived in the same or other communities with similar electricity access challenges; as such, they were motivated by the experience and developed a responsibility to support others now that they are more privileged. P07 shared:

> *"I was once with them [clients] here, and I moved to rent a room in the town [with electricity]. That is also the community I work in. So, when I go to work and upon returning, they say their phones are off, I must take the phones, go and charge. "*

For paid providers motivated by financial gains, their services are largely influenced by the frequent power outages in Ghana. Hence, their services do not target only rural residents but also people in towns where they operate, attracting more charging devices with higher charging fees during power outages.

Device identification is based on tagging, name writing, and memory. In managing the charging services, paid providers commonly issue identification tags to clients. These tags must be presented during the collection of the devices, as narrated by P01: *"I write the number on a card or sticker and fasten it at the back of the phone and write the same number on another sticker for you [client] to take it home."* Some paid providers also write the names of the individuals who bring devices for charging. Among these identification measures, providers allow some flexibility in their operations, e.g., some regular or familiar clients can charge their devices without providing any tags. Also, some providers allow this in situations where they run out of tags, relying on clients' ability to identify the devices during collection.

For free providers, they often charge mobile devices for relatives and close contacts. As such, they naturally form the knowledge of the specific devices a client uses or brings – rendering formal identification mechanisms largely unnecessary. While this embedded knowledge supports providers' operations, they are not sufficient in securing clients' devices. Identification based on informal recognition can still lead to mix-ups, and uncertainties arise out of a heavy reliance on intermediaries, as we discuss next.

5.1.2 Trust and Tensions When Using Intermediaries

Dependence on intermediaries to overcome mobile charging constraints. In navigating access to charging services, clients mostly rely on intermediaries – family members,

friends, neighbors, or motorcycle riders – to send and retrieve devices from the charging services. The intermediaries here function as a form of human infrastructure [87] to fill the gap when clients themselves cannot access the charging services. While many intermediaries are trusted contacts, some clients also rely on people they barely know or have no personal relationship with. As such, clients sometimes *"do not know where the motor riders send the phone when I give it to them"* (C06) or *"can not tell [the device] being at [a] friend's house or any other places"* (C24). As a result, there can be extended periods during which intermediaries or their providers have control of the phones. Explaining why they use intermediaries, clients mentioned the high cost of transportation and demands from work as the main reasons. Other factors — such as the provider's working hours, the client's health situation, and the trusted relationship between the client and their intermediary — also influence clients' decisions to seek support in charging their mobile devices. Rationalizing the convenience of using intermediaries versus the transportation cost, C13 remarked:

> *"It is very disturbing to take a motorbike for 30 Ghana cedi to go and charge your mobile phone for 2 cedi. If someone is going, you have to give it to the person [to take the device for charging]!"*

Trust forming based on knowledge of the intermediary. Trust was often mentioned among the reasons for using intermediaries, as C19 shared, *"I make sure I trust the person."* Clients form this trust from their knowledge of the intermediary's place of residence, family members, and social relations, as noted by C25: *"We greet ourselves when we meet."* Knowing the character or familial ties of their supporters gives clients a sense of implicit security as a necessary first step. Additionally, these communities are small, and members often know one another well. As C08 shared: *"Because we are all in the same area, I know you. You are good . . . [and] not a thief."* C21 elaborated on the considerations:

> *"Before I give it to you, I have to know you . . . and your house. I should already know your mother, most of the relatives you are living with them here."*

Specifically, when clients refer to knowledge of intermediaries' relatives, it is not intended to imply that they will automatically hold these relatives responsible in the event of theft or other incidents. Rather, such references serve as a form of 'informal security' — reflecting an implicit belief that the intermediary will eventually return to the community or that the relatives could assist in resolving any issues.

Regardless of these considerations, individuals who meet the requirements are not always available. As such, clients still engage in risk-taking and occasionally rely on any available person to transport the device. In this case, they form their trust from the intermediary's assurances and in the hope that the individual will demonstrate good character.

5.1.3 Device Retrieval: Constraints and Other Factors

Clients prioritize economic activities over device security. As a typical practice, clients leave their devices at the charging places. In the community with a charging shop, clients usually send their mobile devices to the shop in the morning and collect them by the evening, often after work. However, for the remaining communities with no charging access, clients leave their mobile devices for a longer time, ranging from two to three days. When clients decide between waiting and leaving the devices at the charging places, they usually consider personal priorities, such as work hours, but there are also external factors outside their control.

For personal prioritization, clients often mentioned having *"important work to do"* or otherwise they would risk *"wasting the time"* (C09). Some clients occasionally misplace their collection cards, posing challenges when collecting their devices. This challenge becomes even more concerning at charging stations that operate additional businesses (§5.1.1), where high customer inflow creates further delays. In such cases, clients are often told to *"go and come back later"* multiple times, until the place is less crowded and providers have time to assist them. Clients who had such experiences often do not want to charge their devices at the same place, as shared by C22: *"I struggled before I got the phone . . . For that reason I do not send my phone there anymore."*

Externalities contribute to longer device retention times at the charging place. External factors, primarily providers' practices and power outages, contribute to extended periods of device possession by charging providers. For instance, when clients hand over their devices to providers or intermediaries and an outage occurs, both parties often agree that returning an uncharged phone is unreasonable. As a result, the device remains with the provider until it can be charged at a later time. Providers can contribute to the extended period when they have multiple operators managing the charging place, limited opening hours, insufficient sockets, or implement strict device collection policies. For providers with multiple operators managing the charging place, they usually have a protocol that the operator who received the device must be the same person to hand over the phone when it is fully charged. Thus, when the operator who received the device is unavailable, devices are withheld for extended durations.

Intermediaries also contribute to the delays as they sometimes forget to return the devices to the clients. This becomes more concerning when intermediaries send the mobile devices to their own social circles (free providers) with no collection card for the clients to retrieve the devices by themselves. The power then lies in the hands of the intermediaries until they return to the providing community or place, as C24 recounted:

> *"My phone can be there for about four to six days . . . Sometimes the person who sent the phone there*

[charging town] does not return to the town sooner until the day the person decides to go there again."

As clients negotiate and rationalize intermediaries' support, challenges and concerns related to security and privacy also arise, as we discuss next.

5.2 Challenges and Concerns in Charging

5.2.1 Device Insecurities

Loss of mobile devices. When describing their experiences with charging, clients shared many negative experiences, including loss or damage of devices and accessories such as phones, chargers, batteries, SD cards, and power banks. While recounting his experience, C26 remarked: *"It wasn't even up to two weeks [old]! . . . I gave it to him to charge for me . . . The next morning, when I returned, the phone was not there."* These incidents occur not only at charging places but also in transit, whether handled by intermediaries or by the clients. For example, a device may fall from the transporter's pocket while riding a motorbike, be inadvertently left behind in a vehicle, or be misplaced by an intermediary. Consequently, there is amplified insecurity during the charging period until the client receives their device, as C06 reflected *"Sometimes I am afraid. I think about it: what if it does not come again?"* Insecurities also arise from the inherent fragility of trusting intermediaries, as clients have no way to verify whether the intermediary was truthful in the event of loss or damage. C21 shared: *"The person [intermediary] can keep the phone and come and tell me that the phone is lost."*.

An external factor contributing to possible device loss is that many charging places are often occupied by other people, exposing client devices to customers or relatives of the provider. Some clients assess the charging place before sending their devices to be charged. C19 charges his phone at the cinema, and sometimes *"goes there to check how the place looks like . . . [because of] the number of people who go there."*

Unauthorized access to mobile devices. In addition to possible device loss, some clients had their mobile devices accessed by the providers or the intermediaries during the charging process. C31 was not surprised by the possibility: *"I know that they access phones at the charging places."* A few clients suspected the relatives of providers to be responsible for the unauthorized access or use. C29 and C30 shared that their phones are regularly used for borrowing airtime and making unknown calls, while C22 encountered unauthorized mobile money transfers. C26 deduced that charging places are the culprit due to the many parties and risks involved in the charging process: *"It is only [at] those [charging] places that my phone can be with a second person."*

These speculations were validated by providers who mentioned how their relatives or acquaintances could have access to the devices due to shared accommodations or delegation of roles. P01 narrated that *"My siblings may come here and I will tell them [to] look after the place for me. Then they can take the phones to access them."* When busy, P08 asks the client to go to her room and put the mobile device on charge themselves — the same room where all other devices are, heightening the insecurity of other clients' devices, stating: *"If I'm busy doing something, I will not stop and check your phone for you. No! I can't be a security personnel on your phone while you don't pay me."*

Mix-ups of devices. Incidental device exchanges at charging locations are among the challenges clients encountered during the charging process. This issue primarily stems from providers' practices. Inconsistent tagging and device mix-ups are common, often due to insecure device identification methods, unavailable tags, and name duplications, as well as increased workload from additional non-charging businesses operated by some providers (§5.1.1).

Another contributing factor is the complexity of intermediaries embedded in the charging processes (§5.1.2). For instance, the individual who delivers a phone to the charging center may not be the same person who retrieves it, increasing the risk of mix-ups. Sharing a similar incident, P09 recounted: *"Because the person who came for it wasn't the owner of the phone, the person went with the phone."* Device mix-ups result in the potential misuse of other clients' mobile devices. In C07's and C31's cases, they completely lost the device as the person who received the wrong devices earlier decided not to return to the charging place again.

5.2.2 Everyday Insecurities

Emotional, financial, and physical insecurities. In addition to digital security threats, many clients shared heightened anxiety during the charging process from the moment they relinquish their devices until they are retrieved. This occurs when thinking about potential device damage or loss, when there is a delay in retrieving the device, and when navigating the social relations in the charging process. The timing of the device being returned is often uncertain, especially among clients in communities without dedicated shops. During the charging period, factors such as power outages, intermediaries forgetting to return phones, adverse weather conditions, and spoilage can all contribute to this uncertainty while waiting. Clients are also constrained in their phone usage when their devices are being charged, which heightens the emotional insecurity. As C05 shared, *"We are not able to use the phone as we want it."* C31 reflected, *"I'm a businessman . . . When my phone is off [and] isn't with me, I can't think straight."*

In the event of device loss or damage, clients often have to bear the financial cost. The cost can even go beyond the device itself. For instance, if a SIM card is blocked after repeated attempts of trying to unlock a phone, rural residents would have to travel a considerable distance to reach the

network operators' main office, mostly in cities, to unblock it. Sometimes, the absence of an intermediary can lead to critical trade-offs, e.g., clients traveling to charge mobile devices means leaving a baby alone in a room (§5.1.2).

Social and reputational insecurities. While some clients build trust with their intermediaries (§5.1.2), when negative incidents happen, clients cannot hold the intermediaries responsible, to maintain relationships and continual support. Providers also shared similar insecurity at the social relation level. For the paid providers, their major concerns are around device loss and their duty to replace the device. Free providers, though, face reputational and emotional insecurity should they lose or damage clients' devices. Reflecting on a hypothetical incident, P08 shared an instance when a client may *"stand somewhere to say, I gave my phone to this person, and it has gotten lost."* Hence, she even prefers her personal items in her room to be stolen rather than a client's phone on charge.

5.3 Protective Practices in Charging Devices

5.3.1 Practices from Clients

Using screen and app locks. Due to concerns about unauthorized access, about half of the clients employ technical authentication mechanisms, such as screen and application locks, to secure their devices. Furthermore, as device loss commonly occurred, these security features were perceived as potentially aiding in the recovery of devices, particularly if the devices were sent to an honest technician for unlocking.

The use of screen and app locks is inconvenient at times, forcing clients to share their PINs with their intermediaries or social circles for their own needs. Other times, a malicious provider or intermediary intentionally blocks the devices via multiple trials. C14 shared concerns over such attacks: *"Some people . . . instead of stopping when they try [to unlock] once . . . will intentionally keep trying and get the phone blocked."* A similar incident happened to C21, who had her phone blocked and suspected that it was due to repeated attempts to break the lock at the charging place; even worse, when she finally recovered the phone, she lost valuable information: *"There were so many things on the phone that I couldn't get them back. When I went to flash the phone, everything was lost."*

In Ghana, feature phones are colloquially referred to as "yam" phones [13, 77] and are used primarily for calls, flashlight functions, radio, and mobile money transactions. Despite the simplicity, these phones have long-lasting batteries suitable for rural residents and were used by many participants. While advanced security measures such as app locks were widespread among smartphone users, feature phones have limited functionality, and users of feature phones rarely activate locking mechanisms beyond the default screen lock.

Removing SIM and SD cards. A few clients remove mobile accessories such as SIM and SD cards as additional low-tech physical measures to prevent theft, loss, and unauthorized access. One might question the relevance of these practices by comparing the monetary value of accessories to that of the entire mobile device. However, beyond their monetary worth, SD cards often store sensitive personal information. Additionally, resolving SIM card-related issues in Ghana, particularly for rural residents, can be cumbersome due to the required trips and stress associated with the process. Moreover, news reports about identity information being stolen for pre-registering SIM cards — often by roadside vendors — means that there could be mismatches between the registered details and one's actual name or date of birth for a SIM card holder [24, 38]. Consequently, when SIMs are lost or blocked due to repeated unlocking attempts, users risk losing access to both the SIM and associated mobile money accounts. As C14 explained: *"If the phone is lost and I have money on the SIM, would I lose that too? . . . I remove them so that even if the phone gets lost, I know my SIM is safe."*

Using power banks. Since devices staying overnight at the charging place can increase the chances of theft or unauthorized access to information on the devices, using power banks could help clients reduce the number of times they need to send their devices to charging places. C26 described that using a power bank enabled him to avoid leaving their phone with the provider: *"I do not even want my phone to be there [charging place]."* While some clients wanted to use power banks, they cited the cost of these devices as a barrier.

Other measures adopted by clients include using a unique phone cover or personal pictures as screen savers, switching devices off, and activating the device's tracking features like 'Find My' for iPhones. Clients take these measures to prevent device mix-ups and to track the device if lost. C29, a feature phone user, further shared that she hides her important messages by forwarding them to her Messenger's outbox. She explained the threat model behind:

> *"Not everyone will go to your outbox, but with inbox, immediately someone picks up your phone and sees a new message, the person will start reading . . . and even continue with the previous messages."*

5.3.2 Practices from Providers

Exercising caution with intermediaries. All providers permit intermediaries to present mobile devices to them to be charged. However, to prevent impersonation, some providers do not allow intermediaries to collect mobile devices even if an intermediary brings the collection card and a supposed message from the client. Sharing such a practice, P01 remarked, *"When we are charging phones, the person who brought the phone must be the same person who should come and collect*

it . . . Even if you are sick, you cannot send someone." While this practice addresses the risk of attackers impersonating the legitimate device owner or intermediary, it leads to delays and presents challenges to some clients who cannot return to the charging place, e.g., because of economic constraints, work demands, or sickness. As described by C09:

> *"I may not also get money for transportation . . . but if I give my number to someone to go and collect (my phone) for me, they (the provider) won't give it to the person . . . It is a problem!"*

While some free providers exercise similar discretion, they often allow a client's close relatives to collect devices via informal arrangements. For example, the free providers could be on the lookout for the client's relatives or students from rural communities schooling in the towns to give the charged phones to. The flexibility shown by free providers is often influenced by their familiarity with clients and their relatives.

Physical safeguards around the devices. In addition to using tags, some providers, particularly paid providers secure their charging environment by using padlocks and cages. P04 described, *"I normally put the phone on a shelf or a cage . . . It is enclosed so that no one can just go there."* Since free providers mostly charge devices in their bedrooms, locking the room is a major measure in securing the clients' devices. In some cases, others seek intervention from their relatives to look over their charging places in their absence, although this increases the risk of unauthorized access from the providers' relatives. Due to previous incidents of theft from his bedroom when he was asleep, P06 purchased a long extension board to position the charging devices closer to him when sleeping.

5.4 Infrastructuring Access to Networks

We now present findings related to access to mobile networks. Since there are no providers in this setting, the findings only apply to the 31 clients.

5.4.1 Negotiating Shared Access to Network Zones

Sharing access to network zones is common. Clients without mobile network in their living or working places repurpose other available spaces for connectivity. We use 'network zones' to refer to the places where clients can access network connectivity. About half of the clients reported using network zones near their homes, often in open spaces like yards used for drying clothes or cocoa. However, these locations typically offer only weak signals, and thus, clients' mobile activities are largely limited to voice calls. C22 explained:

> *"For calls, you can even be at this place where we are sitting to make a call. But if you want to switch on data, like [going on] WhatsApp, Facebook, or TikTok, you go to someone's cocoa farm."*

Some other network zones with strong signals include nearby farms, areas alongside the main roads, and town squares. A few clients also mentioned using church and school premises for mobile network access. Due to the limited network zone with strong signals, clients share these zones. Evenings have a higher number of users after clients return from work. Communities that have fewer access zones also have a higher number of clients grouped at the same time to use the network. C06 described a typical night: *"Mostly, in the evening, around 8 PM to 10 PM, you will see many people . . . about 30 people at a moment!"*

Using intermediaries to perform network activities. To navigate barriers such as distance from network zones and limited tech literacy, many clients rely on intermediaries to perform network-related activities on their behalf. Common tasks include creating social media accounts, downloading multimedia content, and conducting mobile money transactions. As C05 explained: *"If I want to make some money transactions and I cannot go, I could send my children to go and withdraw money for me."* Because of the weak network signal, intermediaries often take the devices to the network zones for these activities, sometimes in nearby towns. For instance, unable to create an account by herself, C04 sought help from an intermediary; however, at the time she got support, she *"was also washing, so I could not follow him."* While these practices promote clients' digital access, the intermediation exposes clients to security and privacy risks. To grant intermediaries access, clients often remove their passwords or share them as described by C07: *"Whenever I am giving the phone to them [intermediaries], I remove the screen lock. When they return the phone, I then activate the screen lock."*

Intermediaries can also organically form in the network zone. Some clients occasionally borrow mobile devices from others to complete transactions or calls when they run out of airtime or when their own devices are unavailable due to charging constraints. C31 recounted his experiences: *"I sometimes collect someone's phone to log in my betting account, and someone can also take my phone to log in his/her account to place a bet."* Due to the social relations among rural residents [26], clients cannot refuse these requests, as explained by C21:*"I cannot be hard on them while I'm holding the phone . . . I have to give it to them."*

Leaving mobile devices at network zones. Similar to how clients leave their mobile devices at the charging places (§5.1), some clients sometimes leave their devices at the network zone to wait for their calls or complete their downloads. Additionally, because the network signals at these nearby zones are weak, clients are sometimes unable to communicate when they receive calls, prompting them to move to places with more stable network when they are called *"to call the person back"* (C20). Although this practice increases the risk of the

device being stolen, some clients find security in the close proximity of these zones to their residences.

5.5 Challenges & Concerns in Network Zones

Proximity-based eavesdropping and shoulder surfing. As a result of sharing the network zone, clients can listen to the conversations of other users, which leads to proximity-based eavesdropping. These coverage areas are often not large enough to encourage physical distancing, making private communications almost impossible, as described by C04,

> *"If there were a network everywhere in this community, everyone could sit at their homes, and no one would hear what you talked about. If I am making a call over there, it is in the ears of another."*

Some clients shared that the eavesdropping sometimes escalates to interruptions of active calls by other users who may not like the conversations. For instance, C25 recounted her interruption of a man's live conversations because she did not like how the man was speaking to his girlfriend on the phone; her words infuriated the man, leading to a physical altercation between them. In addition to eavesdropping, clients mentioned shoulder surfing when other users attempt to look over their devices peeping through mobile activities *"with one eye"* (C08). Shoulder surfing is concerning for clients when performing mobile money transactions, as they have to find ways to hide their PINs.

Unauthorized use of mobile devices. As clients sometimes require intermediaries to perform network-requiring activities at the network zones, often without the client's presence, their mobile devices and files are almost entirely exposed to intermediaries. To grant intermediaries access to the devices, clients may also temporarily lower the security measures of their device, as in the case of C07: *"Whenever I am giving the phone to them [intermediaries], I remove the screen lock."* Intermediaries' access to devices means that they can, in theory, copy sensitive files from the phones. Also, the shared network zones indirectly promote device sharing as clients find it difficult to refuse requests from people who share social relations [26], such as community members.

Perceptions of secrecy related to isolated network zones. Since network zones with stable signals are often isolated from clients' usual residences, this leads to concerns among clients about how passersby may interpret their behavior. Perception of them having secret conversations could be misinterpreted as infidelity, leading to physical abuse and family breakdown [10]. While such incidents had not happened to any clients, many were still concerned, as C14 said:

> *"If the network is here, I will be in my room for calls. Who will hear what I talk about? Maybe the person just heard a piece of the conversation, and [it] will be on the person's mind: Ehh, I saw this person making a call; the person was calling her lover."*

Physical insecurities out of tensions with farm owners. Clients encounter physical security threats, including health risks, financial exploitation, and the danger of gunshots. In one community, residents' frequent use of a nearby farm for network access, coupled with littering, hindered the farm's productivity. To deter clients, the farm owner resorted to firing warning shots and invoking curses, such as *"When you go to the farm . . . Snakes should bite you"* (C06). If caught, clients face penalties including weeding a portion of the farm, having their phones confiscated, or paying a fine of 200 Ghanaian cedis. Consequently, as C19 posited, accessing the farm for network connectivity *"has become risky."*

Despite these deterrents, most clients continue to use the farm, particularly in the evenings when the owner is not around. As C06 noted: *"The time he is not around, you go there. Else you wait in the evening around 10 pm, then you go there."* However, nighttime visits expose clients to additional hazards, such as encounters with wild animals and mosquito bites, further endangering their well-being. P30 shared her experiences navigating these challenges during evening hours: *"When you go there in the evening, reptiles might bite your leg, and that could cause another problem."*

5.6 Protective Practices at Network Zones

Physical avoidance. Given that proximity-based eavesdropping is a key concern for several clients, many adopt protective measures that aim at mitigating this risk, e.g., timing their network usage period for hours when many residents may not be at home. Since farming is the predominant economic activity in rural communities, many residents leave these communities in the morning and return by evening, leaving the communities and the network zones less crowded during the afternoon, especially during the weekdays. As such, some clients use these periods for private communications in the network zones. Clients who cannot bear the interference during a crowded period had to end their usage earlier, as shared by C11: *"When you come and I am making a call, I stop and leave there. When the person finishes, then I go back."*

To prevent shoulder surfing, some clients hide their screens by tilting their mobile phones to a certain angle or shielding their screens. For example, C08 stated: *"When you are coming to send money. You will turn . . . like trying to hide the phone small and then enter your PIN so that no one can see."*

Using a different language to 'encrypt' conversations. Ghana is highly multilingual, with over fifty languages spoken [11]. Furthermore, migrations between the north and south occur as a result of fertile soils in the south and underdevelopment in the north; many northern migrants have settled

in southern regions for economic activities like farming and mining [48, 102]. Thus, language use in southern communities, including our study sites, is heterogeneous, which affords some clients at network zones a degree of conversational privacy, as described by C02: *"I will be speaking my own language and the others will be speaking their own."* However, given the predominance of the Twi language in the southern part, and because settlers have to adapt to this language, some clients perceive conversations in Twi as susceptible to interception. Thus, clients lower their voices or use semi-word feedback signals [100], as C06 demonstrated: *"You will say 'mmm', 'aah', 'mmm', 'yoo'–[meaning I hear in Twi]."*

Non-verbal communications. A few clients adapt to the situation by using text instead of voice communications or pre-recording messages before going to the network zone. However, some clients view physical avoidance as the only option. Reflecting on the typical situation at the network zones, C04 doubted that there is any feasible measure:

> *"Even if you do anything, you will still be closer to another person. Even if you want to use an earphone, [even] if what the one at the end of the call says will not be heard by the person standing beside you, what you say the person will hear. So?"*

6 Discussion

In this section, we first situate our key findings in prior work, then discuss our work's implications for researchers, policymakers, and technologists to join forces in creating more inclusive and safer technologies for rural communities.

6.1 Key Insights

Infrastructuring practices and security patchworking in rural Ghana. Prior work has established that when infrastructures and systems fracture and fail, the affected population engages in social and collaborative practices to build, maintain, or adapt infrastructure, referred to as *infrastructuring work* [36, 63, 81]. Our study sheds light on how infrastructuring practices unfold in rural Ghana where, due to systemic electricity outages and limited mobile network coverage, clients infrastructure their access by relying on local shops and social circles for charging (§5.1) and going to network zones (§5.4). In particular, clients' use of their social circles, and occasionally even strangers, as providers and intermediaries in securing access to technology forms what Sambasivan and Smyth describe as *human infrastructure* [87].

Although necessary to access resources, prior work has revealed that infrastructuring practices can generate new forms of insecurity. The concept of *security patchworking* [63] offers a useful analytical lens for interpreting our findings, where clients are patching their access to electricity and mobile networks, yet the very process of patching exposes them to new risks. In McClearn et al.'s study [63], people in post-conflict Lebanon rely on unregulated 'generator cartels' to secure electricity, but the reliance costs large sums of money and contributes to further financial insecurity. Our findings draw parallels by showing how the charging workarounds in rural Ghana, which rely on human infrastructure and charging shops, introduce threats to not only participants' devices but also to their everyday financial, social, and emotional security.

Power relationships and tensions in infrastructuring. Prior work in the Global South setting reveals how social relations and power dynamics shape infrastructuring and resource sharing, often reinforcing control and introducing privacy concerns [6, 28, 53, 87]. For example, Dye et al. documented how continued access to the Internet in Cuba relies on the maintenance of harmonious social relations, without which individuals risk disconnection [36]. In our study, power dynamics also emerge between clients and providers. Clients sometimes have to endure long waits at the providers' place for assistance, especially when clients misplace their collection cards or when multiple operators manage the charging place (§5.1.3). Power asymmetries are also evident in clients' relationships with the intermediaries who essentially control the timeline for returning mobile devices, particularly when intermediaries route the devices to their own social circle (§5.1.2). Due to the number of actors involved, it becomes almost impossible for clients to hold any single person accountable for the negative events they experience.

Sociocultural norms in resource sharing. The power relationships and tensions often boil down to sociocultural norms in a society. Prior work in Global South settings has documented how patriarchal norms, coupled with resource constraints, shape men's control of women's tech use – for example, when husbands regularly check their wives' call history and duration of conversations to uphold community values [5, 85]. While in our study, we do not observe any influence from patriarchal norms, the tensions and insecurities due to other sociocultural norms in the Ghanaian society are evident. For instance, due to existing social ties, clients are often unable to hold intermediaries or providers accountable for device loss or damage, forcing them to choose between withholding their grievances or breaking the human infrastructure they rely on. Moreover, when clients share the network zones, social expectations make it difficult for someone to refuse offering help – for example, when clients receive requests from others to use their phone in the shared network zone (§5.5), even if the request is from a stranger [79].

Nevertheless, sociocultural norms also function as the backbone of infrastructuring practices and can offer benefits to the stakeholders involved. For instance, Hussain et al. studied how naturalized Rohingya refugees in Bangladesh leverage

their legal status to help unnaturalized refugees gain SIM cards [49]. The power of social connections also manifests in our study, especially among free providers who formerly lived with clients and thereby use their access privilege to support the less privileged. The sense of social responsibility that motivates providers to provision electricity reflects the broader norms of communal support and a cultural belief in the reciprocity of good deeds in the Ghanaian society [41].

Everyday insecurities going beyond the digital context.

> *"It is in the mundane that we can observe and question the tensions between security and insecurity that shape people's lived experiences . . . "* – McClearn et al. [64]

Security exists in many shapes and forms beyond technological contexts. McSweeney posits a sociological thinking of security as the freedom to live without fear and protection from harm [66]. Along this line, the concept of *everyday security* seeks to capture how security exists in "mundane spaces, routine practices, and affective/lived experiences" [75]. Prior work has documented how everyday insecurities manifest when undocumented immigrants in the US grapple with government surveillance in day-to-day routines of using social media and interacting with employers [44], or when marginalized groups in Lebanon have to rely on informal money exchange platforms during an economic collapse [63].

Our study shows everyday insecurities during infrastructure failure in a previously unexplored context. The broader everyday insecurities in charging and network access affect not only clients but also service providers. During power outages, paid providers often raise their charging fees (§5.1.1), exacerbating financial insecurity for clients. Providers can also experience financial insecurity, as in the case of a farm owner whose property is persistently used as a network zone. As the provider resorts to firing gunshots to deter clients, it further exposes clients to physical insecurity (§5.5). The loss of a device leads to financial insecurity for clients, while providers and intermediaries grapple with emotional distress and reputational harm (§5.2.2). These findings contribute to the growing call for researchers and practitioners to expand security research beyond cyber [64] to rigorously interrogate and meaningfully address the mundane, daily insecurities of people who lack technology access. The access limitations expose rural residents to digital S&P risks but also heightened everyday insecurities that impact their broader well-being.

6.2 Implications and Recommendations

New access controls needed for community-level network sharing. In comparing our findings with prior work [61, 62, 91], we observe that existing access control mechanisms for domestic households may not be practical in the setting of community-level resource sharing in rural Ghana. Even with controls that anticipate familiar people sharing smart home devices, previous work shows that unauthorized access and misuse of these devices are fairly common and highly contextual [67]. While fine-grained access control systems in home IoT settings enable users to refuse access (e.g., by specifying who can use which capabilities of the device) [47], refusal is often not an option in our study. Clients may need to ask for help with technology in the shared network zone, and coupled with other social norms around sharing and reciprocity, it is hard for them to refuse others' ask to use their phone. While our study is not designed to envision how access control mechanisms in shared network zones could look like — as coming up with any proposals for solutions also requires long-term and careful engagement with the local communities — we highlight this as an important direction for future work.

Mitigation against shoulder surfing. Zooming in on the sharing of network zones, one primary concern is the threat from shoulder surfing. While using a privacy screen protector could mitigate this threat, none of the clients mentioned adopting this measure, and it remains unclear whether it is due to unawareness or constraints from other factors, such as cost. Past S&P research has also proposed a few systems aimed at combating shoulder surfing, such as Eyeshield [97], iAlert [9], and HideScreen [27]. A critical question to be answered by future work is to what extent the affordance of these solutions matches the needs of rural communities. For example, mismatches might occur when most existing solutions operate around smartphones only, while feature phones are commonly used in rural Ghana and by many clients in our study.

Device management protocols at the charging site. Our findings highlight that the device identification and tagging practices at charging places are rudimentary and chaotic (§5.1), leading to device mix-ups (§5.2). Manually tagging mobile devices with sticky notes and markers is inefficient and unreliable. Tags can also be easily forged. When devices outnumber available tags, providers may charge them without proper identification. These findings inform the design space for improved device management protocols to be explored in future work — ideally reducing the manual burden on providers while accommodating the social and financial realities of clients [68]. A potential low-cost offline solution involves pairing phones with plastic tags and issuing tokens containing provider-specific QR code identifiers. Upon drop-off, the provider records the token number and the sender's name, along with a mutually agreed-upon PIN. To retrieve a device, the intermediary must present both the QR-coded token and the correct PIN as a form of two-factor authentication. However, for free providers, fostering mutual trust is more appropriate, as they operate in informal settings where clients rely on social ties and frequently shift between providers.

Rethinking security advice for resource-constrained settings. Prior work on security advice suggests that in situations that involve resource sharing, one should log out after using public computers [69], use screen and app locks when sharing devices [85], and remove SIM cards when sending devices to repair [4]. Participants in our study report adopting similar practices (§5.3). Akin to the low-tech defense strategies adopted by activists during the 2018-2019 Sudanese revolution [32], clients in our study used mundane, non-technical strategies – such as speaking quietly or switching languages – to avoid being eavesdropped in shared network zones (§5.6).

Crucially, while low-tech workarounds are largely sufficient against the adversary's surveillance, arrest, and physical device seizure among Sudanese activists [32], we cannot say the same about our study's participants. For instance, it is not guaranteed that a bystander can not understand the conversation simply because the person is not from the same tribe and thus will not understand the language. Removing SIMs, while effective in mitigating mobile money theft, is cognitively demanding [85]. It also presents the security versus usability tradeoff, as removing SIM cards can also result in loss of call history, or sometimes even the SIM cards. Moreover, when devices get mixed up at the charging place (§5.2), providers may call the client's phone number to verify, which would further be impossible if the SIM card is removed. All of these edge cases call for a reflection on existing security advice in light of the realities in resource-constrained settings.

Going beyond educational interventions for rural communities. Calls for educational interventions or security awareness training are not new in security research, though prior work has mostly focused on organizational settings, drawing from Western samples [14, 96]. Bringing such initiatives to rural communities, such as those we work with in Ghana, presents both promise and complexities. While these communities can benefit from understanding the specific risks and tradeoffs of protective measures (e.g., the benefits and limitations of removing SIM cards, as shown in §5.3), such efforts should address notions such as "I've got nothing to lose" [108] or there's "not much to get" from attacking them, which are particularly prevalent among low-income populations [56].

Crucially, educational interventions have limitations, particularly in our study's setting. The key issues we observe boil down to one's access — whether to infrastructure, financial resources, or digital literacy that extends beyond basic security awareness. For instance, while rural residents may be taught not to share devices or PINs, practical constraints often require them to do so. Many rely on intermediaries to charge phones or create accounts in network zones, often leaving their devices physically out of their control. Hence, limited infrastructure access becomes a key barrier to achieving meaningful security and privacy without risking exclusion in a technology-driven society [34]. Thus, more efforts, whether from the government, researchers, practitioners, or advocacy organizations, should be directed toward improving infrastructure, technological access, along with digital literacy in rural communities.

Ethics Considerations

This study was approved by our Institutional Review Board (IRB). We developed an informed consent form, which was shared with all study participants. The informed consent form explicitly stated the purpose of the study, which is about exploring the security and privacy threats in participants' workarounds when accessing electricity and mobile networks. Participants were informed about the voluntary nature of the study, and consent was obtained from each participant before the interviews. Participants were also notified of their right to skip any questions they felt uncomfortable answering or did not know the answer. To protect participant privacy, we did not collect any personally identifiable information. We sought participants' consent to audio record the conversations. However, participants were assured that opting out of audio recording would not affect their participation or any benefits, such as compensation. The full disclosure of the study's purpose and informed consent occurred in two cycles: during the recruitment and before each interview, since the recruitment occurred a few days before the interview period.

Before engaging with a freelancer for transcription and translation of our interviews, our sponsoring institution formally signed a contractual agreement with the freelancer. The contract emphasized the confidentiality of the materials they would handle. To ensure confidentiality, all files shared with the freelancer were anonymized using pseudonyms without a visible clue to the participants' community. Additionally, the transcriber lives outside the study's region and does not have personal contacts with the studied communities, which further reduces the risks of deanonymization.

The lead researcher, coordinating with local contact persons, visited all study communities beforehand to explain the purpose of the study to community leaders and obtained their consent for using their communities as study sites. The visits also served to ensure safety and build rapport with community members. Given the study's focus on electricity and mobile network access, community elders often expressed hopeful expectations. We empathetically explained the study's purpose in managing these expectations effectively. All community leaders consented to their communities' participation.

Positionality. The study team consists of three researchers. The lead researcher is a native Ghanaian while the second author has done extensive research in African contexts. The third author is from outside Africa but has done extensive research on cross-cultural security and privacy. Collectively, these researchers brought diverse perspectives that enriched our study approach and the analysis of results.

Compliance with Open Science Policy

We include our study's interview protocol and codebook (see §4.3 and §4.4, respectively) to facilitate the reproducibility and replicability of our study. However, we do not share the actual interview transcripts from participants, given that all communities in our study are extremely small and anonymized transcripts can still lead to re-identification of individuals.

Acknowledgments

We thank the reviewers and shepherd for their feedback. We extend our immense gratitude to all participants, the community leaders and contacts, the statisticians at the Upper Denkyira West District Assembly, and our contractor, who provided valuable insights and made this work possible. This work was partially funded by the Max Planck Society and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972. Collins W. Munyendo acknowledges support from the US National Science Foundation under Grant Number 1845300 and a Google PhD Fellowship.

References

[1] Arkum Thaddues Aasoglenang, Samuel Z Bonye, and E Owusu-Sekyere. Rural livelihoods diversity: Coping Strategies in WA West district in Northern Ghana. *European Scientific Journal*, 9(35):139–156, 2013.

[2] Ananpansah B Abraham. Frafra Youth Declare 'No Electricity, No Vote!', 2019. https://www.modernghana.com/news/920568/frafra-youth-declare-no-electricity-no-vote.html.

[3] Ishmael Ackah. The Latest Power Supply Challenges In Ghana. *IEA Ghana, Energy for Growth Hub*, 2021. https://energyforgrowth.org/wp-content/uploads/2021/08/The-Latest-Power-Supply-Challenges-In-Ghana-2.pdf.

[4] Syed Ishtiaque Ahmed, Shion Guha, Md. Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, ICTD '16. Association for Computing Machinery, 2016.

[5] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.*, 1, 2017.

[6] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 906–918, New York, NY, USA, 2017. Association for Computing Machinery.

[7] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 297–308, 2015.

[8] Emad B Algorani and Vikas Gupta. Coping Mechanisms. In *StatPearls [Internet]*. StatPearls Publishing, 2023.

[9] Mohammed Eunus Ali, Anika Anwar, Ishrat Ahmed, Tanzima Hashem, Lars Kulik, and Egemen Tanin. Protecting mobile users from visual privacy attacks. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, UbiComp '14 Adjunct, page 1–4, New York, NY, USA, 2014. Association for Computing Machinery.

[10] John Garin Isaac Ameyaw, Shirley Dankwa, and Isaac Eshun. Factors that contribute to marriage breakdown among young couples in the Ghanaian context. *Journal of Scientific Research and Reports*, 2023.

[11] Akosua Anyidoho and Mary Esther Kropp Dakubu. Ghana: Indigenous languages, English, and an emerging national identity. *Language and national identity in Africa*, 141:157, 2008.

[12] Cyber Security Authority. About us. Technical report, Cyber Security Authority Ghana, 2024. https://www.csa.gov.gh/about-us.php.

[13] Seyram Avle. Radio via mobile phones: The intersecting logics of media technologies in Ghana. *Media, Culture & Society*, 42(5):789–799, 2020.

[14] Maria Bada, Angela M Sasse, and Jason RC Nurse. Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? *arXiv preprint arXiv:1901.02672*, 2019. https://doi.org/10.48550/arXiv.1901.02672.

[15] World Bank. Access to Electricity, Rural (% of Rural population) - Ghana. Technical report, World Bank Data Group, 2023. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS.

[16] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A. Brewer. Computing security in the developing world: a case for multidisciplinary research. In *Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions*, NSDR '11, page p.39–44. Association for Computing Machinery, 2011.

[17] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 687–706, 2022.

[18] Nicola J. Bidwell. Women and the Sustainability of Rural Community Networks in the Global South. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*, ICTD '20, New York, NY, USA, 2020. Association for Computing Machinery.

[19] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the internet goes down in Bangladesh. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page p. 1591–1604. Association for Computing Machinery, 2017.

[20] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the internet goes down in bangladesh. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page 1591–1604, New York, NY, USA, 2017. Association for Computing Machinery.

[21] Yaw Agyeman Boafo, Osamu Saito, Godfred Seidu Jasaw, Kei Otsuki, and Kazuhiko Takeuchi. Provisioning ecosystem services-sharing as a coping and adaptation strategy among rural communities in Ghana's semi-arid ecosystem. *Ecosystem Services*, 19:92–102, 2016.

[22] Nana Ama Boansi Boakye, Frank BK Twenefour, and Mary McArthur-Floyd. The impact of power outage "Dumsor" on the hotel industry: Evidence from Ghana. *Journal of Energy Technologies and Policy*, 6(8):39–47, 2016.

[23] David Boansi, Victor Owusu, Enoch Kwame Tham-Agyekum, Camillus Abawiera Wongnaa, Joyceline Adom Frimpong, and Kaderi Noagah Bukari. Responding to harvest failure: Understanding farmers coping strategies in the semi-arid Northern Ghana. *Plos one*, 18(4), 2023.

[24] Owusu Nyarko Boateng, Boadu Nkrumah, Victoria Boafo, Akwasi Amponsah, Lord Anortei Tetteh, Justice Aning, Kornyo Oliver, Adebayo Felix Adekoya, Isaac Kofi Nti, Faiza Umar Bawah, et al. A fraud prevention and secure cognitive SIM card registration model. *Indian Journal of Science and Technology*, 15(46):2562–2569, 2022.

[25] Samuel Ziem Bonye and Jasaw Seidu Godfred. Traditional coping mechanisms in disaster management in the Builsa and Sissala Districts of Northern Ghana. *Eur J Soc Sci*, 25(2):204–218, 2011.

[26] Kirstie Cadger, Andrews K Quaicoo, Evans Dawoe, and Marney E Isaac. Development interventions and agriculture adaptation: a social network analysis of farmer knowledge transfer in Ghana. *Agriculture*, 6(3):32, 2016.

[27] Chun-Yu (Daniel) Chen, Bo-Yao Lin, Junding Wang, and Kang G. Shin. Keep Others from Peeking at Your Mobile Device Screen! In *The 25th Annual International Conference on Mobile Computing and Networking*, MobiCom '19, New York, NY, USA, 2019. Association for Computing Machinery.

[28] Jay Chen, Michael Paik, and Kelly McCabe. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages p.129–142. USENIX Association, 2014.

[29] George Hope Chidziwisano and Maureen Jalakasi. Understanding Women's Perspectives on Smart Home Security Systems in Patriarchal Societies of Malawi. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 1078–1092, New York, NY, USA, 2023. Association for Computing Machinery.

[30] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a new land: mobile phones, amplified pressures and reduced capabilities. In *Proceedings of the 2018 chi conference on human factors in computing systems*, pages 1–13, 2018.

[31] Ghana Energy Commission. National statistiscal bulletin, 2023. https://www.energycom.gov.gh/newsite/files/2023-energy-Statistics.pdf.

[32] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *Proc. IEEE S&P*, 2021.

[33] Dominic N. Dagbanja. The right to privacy and data protection in Ghana. *African data privacy laws*, pages 229–248, 2016.

[34] Partha Das Chowdhury, Andrés Domínguez Hernández, Kopo Marvin Ramokapane, and Awais Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive pets. In *Proceedings of the 2022 New Security Paradigms Workshop*, NSPW '22, page 60–74, New York, NY, USA, 2023. Association for Computing Machinery.

[35] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. "yours is better!": participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 1321–1330, New York, NY, USA, 2012. Association for Computing Machinery. https://doi.org/10.1145/2207676.2208589.

[36] Michaelanne Dye, David Nemer, Neha Kumar, and Amy S. Bruckman. If it rains, ask grandma to disconnect the nano: Maintenance & care in havana's streetnet. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[37] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019. https://doi.org/10.1145/3290605.33007.

[38] Bonney Emmanuel. Stolen identity! Many at risk from SIM card re-registration. https://www.graphic.com.gh/news/general-news/stolen-identity-many-at-risk-from-sim-card-re-registration.html.

[39] Global System for Mobile Communications. Up to 50,000 people from rural communities gain access to mobile coverage through newly deployed network sites in Ghana and Uganda. Technical report, Global System for Mobile Communications, 2021. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/https-www-gsma-com-solutions-and-impact-connectivity-for-good-mobile-for-development-gsma-innovation-fund-rural-connectivity/.

[40] Rizalin Francisco. Virtual learning: Challenges and coping mechanisms of language learners in rural areas. *Journal of Learning and Development Studies*, 1(1):40–52, 2021. https://doi.org/10.32996/jlds.2021.1.1.59.

[41] Devin M. Geary. Transnationalism and Identity: the Concept of Community in Ghanaian Literature and Contemporary Ghanaian Culture. Master's thesis, Bucknell University, 2012.

[42] Enyan obontser: Central region town without 'signal' cries for mobile network services, 2024. https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Enyan-Obontser-Central-Region-town-without-signal-cries-for-mobile-network-services-1928638.

[43] Dhruba R Ghimire. Household food security and coping strategies: Vulnerabilities and capacities in rural communities. *International Journal of Scientific and Research Publications*, 4(9):p.1–8, 2014.

[44] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–15, 2018.

[45] Laura Gianna Guntrum. Keyboard Fighters: The Use of ICTs by Activists in Times of Military Coup in Myanmar. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[46] Sumair Ijaz Hashmi, Rimsha Sarfaraz, Lea Gröber, Mobin Javed, and Katharina Krombholz. Understanding the Security Advice Mechanisms of Low Socioeconomic Pakistanis. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery.

[47] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home Internet of things). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, 2018.

[48] Gavin Hilson, Richard Amankwah, and Grace Ofori-Sarpong. Going for gold: transitional livelihoods in Northern Ghana. *The journal of modern African studies*, 51(1):109–137, 2013.

[49] Faheem Hussain, Abdullah Hasan Safir, Dina Sabie, Zulkarin Jahangir, and Syed Ishtiaque Ahmed. Infrastructuring Hope: Solidarity, Leadership, Negotiation, and ICT among the Rohingya Refugees in Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*, ICTD '20, New York, NY, USA, 2020. Association for Computing Machinery.

[50] Global Vision International. How many languages does Ghana have?, 2023. https://www.gvi.ie/blog/smb-how-many-languages-does-ghana-have/.

[51] Anne Jonas, Stefani Vargas, and Jean Hardy. 'better than google': Information activism for lgbtq+ young adults in a rural community. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW2), November 2024.

[52] Menuso residents appeal for telephone network connectivity, 2024. https://www.myjoyonline.com/menuso-residents-appeal-for-telephone-network-connectivity/.

[53] Zoe Kahn, Meyebinesso Farida Carelle Pere, Emily Aiken, Nitin Kohli, and Joshua E Blumenstock. Expanding Perspectives on Data Privacy: Insights from Rural Togo. *arXiv preprint arXiv:2409.17578*, 2024. https://arxiv.org/abs/2409.17578.

[54] Preston Kemeny, Paul G Munro, Nicole Schiavone, Greg van der Horst, and Simon Willans. Community Charging Stations in Rural Sub-Saharan Africa: Commercial Success, Positive Externalities, and Growing Supply Chains. *Energy for Sustainable Development*, 23:p.228–236, 2014.

[55] Ahogle Arcadius Martinien Agassin Kipkoech Rogers, Takase Mohammed and Ocholla Gordon. Opportunities and challenges in Ghana's renewable energy sector. *Discover Applied Sciences*, 6(10):530, 2024. https://doi.org/10.1007/s42452-024-06148-x.

[56] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in Germany through qualitative interviews. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2029–2046, Philadelphia, PA, August 2024. USENIX Association.

[57] Ebenezer Nyarko Kumi. The Electricity Situation in Ghana: Challenges and Opportunities. *Center for Global Development*, 2017. https://www.cgdev.org/ publication/electricity-situation-ghana-challenges-and-opportunities.

[58] Junchao Lin, Jason I Hong, and Laura Dabbish. "It's our mutual responsibility to share": The Evolution of Account Sharing in Romantic Couples. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–27, 2021.

[59] Victor Lolig, Samuel A Donkoh, Francis Kwabena Obeng, Isaac Gershon Kodwo Ansah, Godfred Seidu Jasaw, Yasuko Kusakari, Kwabena Owusu Asubonteng, Bizoola Gandaa, Frederick Dayour, Togbiga Dzivenu, et al. Households' coping strategies in drought-and flood-prone communities in Northern Ghana. *Journal of Disaster Research*, 9(4):p.542–553, 2014.

[60] Kinsley Mamore. Sixteen communities in old Agou appeal for telecom network. *Ghana News Agency*, 2023.

[61] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just Grab any Device that's Closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 5921–5932, New York, NY, USA, 2016. Association for Computing Machinery. 10.1145/2858036.2858051.

[62] Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, et al. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 645–654, 2010.

[63] Jessica Mcclearn, Rikke Bjerg Jensen, and Reem Talhouk. Security patchworking in lebanon: Infrastructuring across failing infrastructures. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1), April 2024.

[64] Jessica McClearn, Reem Talhouk, and Rikke Bjerg Jensen. The Everyday Security of Living With Conflict. *IEEE Security & Privacy*, 23(2):95–100, 2025.

[65] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[66] Bill McSweeney. *Security, identity and interests: a sociology of international relations*. Number 69. Cambridge University Press, 1999.

[67] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L Mazurek. Characterizing everyday misuse of smart home devices. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2835–2849. IEEE, 2023.

[68] Eyitemi Moju-Igbene, Hanan Abdi, Alan Lu, and Sauvik Das. "How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 881–898, Boston, MA, August 2022. USENIX Association.

[69] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *Proc. IEEE S&P*, 2023.

[70] National Communication Authority and Ghana Statistical Service. Household Survey on ICT in Ghana. *Abridged Report*, 2020. https://nca.org.gh/2020/11/02/household-survey-on-ict-in-ghana-2019-abridged-report/.

[71] International Communication Network. Ghana: Population coverage, by mobile network technology.

[72] Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava. Towards the use of Participatory Methods in Cybersecurity research in Rural Africa: A grassroots Approach. In *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pages 1–7. IEEE, 2021.

[73] Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava. Cybersecurity practices of Rural underserved communities in Africa: A case study from Northern Namibia. In *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, pages 1–7. IEEE, 2023.

[74] Ivy Kesewaa Nkrumah, Ewald Neumann, Eric Anane, Lebbaeus Asamani, and Eunice Torto-Seidu. E-learning in the post-covid era: Experiences of tertiary students. *Journal of Policy and Development Studies (JPDS)*, 3(1):62–77, 2024.

[75] Jonna Nyman. The everyday life of security: Capturing space, practice, and affect. *International Political Sociology*, 15(3):313–337, 2021.

[76] Ministry of Communication and Digitalisation. Ghana launches 5g network: A historic leap towards digital advancement. *www.moc.gov.gh*, 2024.

[77] Graphic Online. 'Yam' phones on hot demand at Kwame Nkrumah Circle, 2023. https://www.graphic.com.gh/lifestyle/yam-phones-on-hot-demand-at-kwame-nkrumah-circle.html.

[78] MyJoy Online. No light, no vote Residents of Amansie South District demonstrate over lack of electricity, 2020. https://www.myjoyonline.com/no-light-no-vote-residents-of-amansie-south-district-demonstrate-over-lack-of-electricity/.

[79] Annabella Osei-Tutu, Vivian A Dzokoto, Katja Hanke, Glenn Adams, and Faye Z Belgrave. Conceptions of love in Ghana: An exploration among Ghanaian Christians. *Journal of Psychology in Africa*, 28(2):83–88, 2018.

[80] Firaz Peer and Carl DiSalvo. The work of infrastructural bricoleurs in building civic data dashboards. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1):1–25, 2022.

[81] Volkmar Pipek and Volker Wulf. Infrastructuring: Toward an integrated perspective on the design and use of information technology. *Journal of the Association for Information Systems*, 10(5):1, 2009.

[82] Karen Renaud and Lizzie Coles-Kemp. Accessible and Inclusive Cyber Security: a Nuanced and Complex Challenge. *SN Computer Science*, 3(5):346, 2022.

[83] Kathryn Roulston. *Analysing interviews*. The SAGE handbook of qualitative data analysis, 2014.

[84] Dina Sabie and Syed Ishtiaque Ahmed. Moving into a technology land: exploring the challenges for the refugees in canada in accessing its computerized infrastructures. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 218–233, 2019.

[85] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.

[86] Nithya Sambasivan, Nimmi Rangaswamy, Ed Cutrell, and Bonnie Nardi. Ubicomp4D: infrastructure and interaction for international development–the case of urban indian slums. In *Proceedings of the 11th International Conference on Ubiquitous Computing*, UbiComp '09, page 155–164, New York, NY, USA, 2009. Association for Computing Machinery.

[87] Nithya Sambasivan and Thomas Smyth. The human infrastructure of ICTD. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development*, ICTD '10, New York, NY, USA, 2010. Association for Computing Machinery.

[88] Doris Doku Sasu. Ownership rate of selected digital devices in Ghana 2020-2023. Technical report, Statista, 2024. https://www.statista.com/statistics/1171486/ownership-rate-of-selected-digital-devices-in-ghana/.

[89] Bryan Semaan. 'routine infrastructuring' as ' building everyday resilience with technology' when disruption becomes ordinary. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[90] Ghana Statistical Service. Ghana 2021 population and housing census: General report. Technical report, Ghana Statistical Service, 2021.

[91] Amit Kumar Sikder, Leonardo Babun, Z Berkay Celik, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. Who's controlling my device? Multi-user multi-device-aware access control system for shared smart home environment. *ACM Transactions on Internet of Things*, 3(4):1–39, 2022.

[92] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "they look at vulnerability and use that to abuse you'': Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 323–340, Boston, MA, August 2022. USENIX Association.

[93] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[94] Sharifa Sultana, Ilan Mandel, Shaid Hasan, S.M.Raihanul Alam, Khandaker Reaz Mahmud, Zinnat Sultana, and Syed Ishtiaque Ahmed. Opaque Obstacles: The Role of Stigma, Rumor, and Superstition in Limiting Women's Access to Computing in Rural Bangladesh. In *Proceedings of the 4th ACM SIGCAS Conference on Computing and Sustainable Societies*, COMPASS '21, page 243–260, New York, NY, USA, 2021. Association for Computing Machinery.

[95] Maxwell Suuk. Ghana's dumsor crisis: blackouts plague homes and businesses. *DW*, 2024. https://www.dw.com/en/ghanas-dumsor-crisis-blackouts-plague-homes-and-businesses/a-68719530 (Accessed on 16/04/2025).

[96] Shuhaili Talib, Nathan L Clarke, and Steven M Furnell. An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security*, pages 196–203. IEEE, 2010.

[97] Brian Jay Tang and Kang G. Shin. Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5449–5466, Anaheim, CA, August 2023. USENIX Association.

[98] The Ghanaian Times. Fix problems before expanding coverage, 2025. https://ghanaiantimes.com.gh/fix-problems-before-expanding-coverage.

[99] The Sudan Times. The vital role of elders in African communities, 2024.

[100] Jürgen Trouvain and Khiet Phuong Truong. Comparing non-verbal vocalisations in conversational speech corpora. In *4th International Workshop on Corpora for Research on Emotion Sentiment and Social Signals (ES3 2012)*, pages 36–39. European Language Resources Association (ELRA), 2012.

[101] Simon Unyan. Searching for mobile phone signal – how sanguli residents struggle with poor network. *Graphic Online*, 2025.

[102] Kees Van der Geest. North-South migration in Ghana: what role for the environment? *International Migration*, 49:e69–e94, 2011.

[103] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, COMPASS '18. Association for Computing Machinery, 2018.

[104] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *Proc. IEEE S&P*, 2022.

[105] Nicola Wendt, Rikke Bjerg Jensen, and Lizzie Coles-Kemp. Civic empowerment through digitalisation: The case of greenlandic women. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[106] Heike Winschiers-Theophilus, Tariq Zaman, and Alvin Yeo. Reducing" white elephant" ICT4D projects: a community-researcher engagement. In *Proceedings of the 7th International Conference on Communities and Technologies*, pages 99–107, 2015.

[107] Yuxi Wu, W Keith Edwards, and Sauvik Das. SoK: Social Cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879. IEEE, 2022.

[108] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 197–216, Baltimore, MD, August 2018. USENIX Association.

[109] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Privacy-Enhancing Technologies (PoPETs)*, 2024.

Appendix

A Community Demographics

Table 2: Selected Communities. Population estimate based on 2024 data received from the Statistics Department of Upper Denkyira West district [90]. **E** stands for *Electricity* and **M** stands for *Mobile Network*.

Community	Population	Participant	Acc. Challenge
Aboaboso	340	4	E & M
Adwenpaye	450	5	E & M
Akrofuom	730	10	E & M
Mensakrom	450	8	E & M
Bethlehem	2842	4	M