Exploring digital security and privacy in relative poverty in Germany through qualitative interviews

Anastassija Kostan
Paderborn University

Sara Olschar
Paderborn University

Lucy Simko
The George Washington University

Yasemin Acar
Paderborn University &
The George Washington University

Abstract

When developing security and privacy policy, technical solutions, and research for end users, assumptions about end users' financial means and technology use situations often fail to take users' income status into account. This means that the status quo may marginalize those affected by poverty in security and privacy, and exacerbate inequalities. To enable more equitable security and privacy for all, it is crucial to understand the overall situation of low income users, their security and privacy concerns, perceptions, behaviors, and challenges. In this paper, we report on a semi-structured, in-depth interview study with low income users living in Germany ($n = 28$) which we understand as a case study for the growing number of low income users in global north countries. We find that low income end users may be literate regarding technology use and possess solid basic knowledge about security and privacy, and generally show awareness of security and privacy threats and risks. Despite these resources, we also find that low income users are driven to poor security and privacy practices like using an untrusted cloud due to little storage space, and relying on old, broken, or used hardware. Additionally we find the mindset of a—potentially false—sense of security and privacy because through attacking them, there is "not much to get". Based on our findings, we discuss how the security and privacy community can expand comprehension about diverse end users, increase awareness and design for the specific situation of low income users, and should take more vulnerable groups into account.

1 Introduction

Poverty has been increasing wordwide during the past decades and is divided in two categories: *Extreme poverty* defines an income so low that it is impossible for the person or family to meet basic needs of life including food, shelter, safe drinking water, education, and healthcare. *Relative poverty* defines a household income that is below 60% of the median household income of a state or country, leading relatively poor people to struggle with all sorts of social marginalization [1], where technology use and security and privacy issues are not exempt.

Extremely valuable work by Redmiles et al. has shown that, statistically, low-income populations in the US do not experience *more* theft of personal information, account compromise, non-consensual posting of information, and scamming [2]. However, other aspects of security and privacy—which may be more difficult to study in a census-representative survey such as [2]—may affect low-income users differently, and inequitably. For example, consider the pay-for-privacy business model [3]. While many popular technologies have free versions, some offer better privacy to those who pay (e.g., offering an ad-free version), and others are entirely unavailable without payment (e.g., a paid VPN service). Paying for privacy presents a barrier to security and privacy to those in relative and extreme poverty.

The pay-for-privacy model [3] is not the only reason to consider the effect of poverty on users' security and privacy needs and experiences: prior work has shown that those accessing technology through intermediaries, or using shared technologies—factors which can coexist with poverty—directly face barriers to security and privacy specifically because of their technical practices, which are, in some cases, enforced by their economic situations [4]. This body of literature examines the security and privacy experiences, needs, and barriers of vulnerable or marginalized populations—many (but not all) of whom can experience poverty, e.g., refugees, sex workers [5, 6].

While the lack of resources is a theme in prior work about vulnerable populations, and appears as a factor (direct or indirect) that contributes to vulnerability, there is little work in our field with poverty itself as a primary focus [2], though some have found that certain demographic factors that tend to *correlate* with poverty (such as education) affect security and privacy needs, experiences, and mental models [7, 8].

We observe, thus, that there are many valuable studies that study security and privacy for people who experience poverty, but do not engage *directly* with the idea of poverty as a potential factor in vulnerability. In this paper, we begin to fill

this gap, by directly examining the effects of poverty on one's security and privacy technology use and threat model. In contrast to the valuable body of work about users in *extreme* poverty in the global south (e.g., [4, 9]), we focus on users in *relative* poverty in Germany in order to form a basis for understanding how income and security and privacy relate to each other in a rich country in the global north. We explore threat models and technology use in order to understand how those in poverty define security and privacy, and then to elicit technical and societal barriers to security and privacy. By focusing directly on poverty, we shed light on security and privacy related challenges of the growing number of people living in relative poverty in global north countries where more and more public and private services have moved online [10, 11], especially since during the pandemic internet use has become increasingly important to the population [12, 13], which reinforces income related divides that represent an important realm of social inequality [14, 15, 16].

We address the following research questions:

- **RQ1:** What security and privacy actions and practices do people living in relative poverty in Germany employ in their everyday lives?
- **RQ2:** What is important to them in the context of digital security and privacy?
- **RQ3:** What technology and assets do they use and/or seek to protect?

Through 28 in-depth interviews with relatively poor users in Germany, we find that they generally have a high level of security and privacy awareness—in line with Redmiles et al [2]—but they lack suitable instruments to protect themselves better, especially when it comes to resources like time, money to purchase state of the art hardware, and protective software, as well as resources to gain more specific knowledge about security and privacy. We find, for example, that users in relative poverty use technologies that cost less (e.g. second-hand phones, free cloud storage services) despite either having security and privacy concerns (e.g., about data privacy properties of free storage) or despite the practices putting them, objectively, at risk (e.g., use of second-hand devices that have not been sanitized properly [17, 18]).

We also emphasize that *poverty cannot be solved with technology:* there are underlying power and social structures that enforce generational or situational poverty; technology, even perfectly secure and usable technology, cannot solve these issues. However, we, as computer security researchers, have the obligation to ensure that our community produces technology that equitably distributes security and privacy, and we know, from our work and from prior work, that misalignments in technical design are inequitably distributed, often in ways that align with other forms of societal oppression. We have positioned this paper for the technical computer security community in order to show how many current technical designs

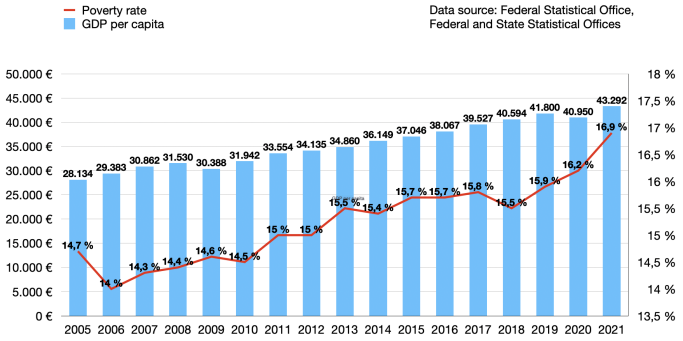

Figure 1: Poverty Rate - GDP per capita.[1]

[1]Retrieved from "Paritätische Gesamtverband", modified in color and format: https://www.der-paritaetische.de/themen/sozial-und-europapolitik/armut-und-grundsicherung/armutsbericht-2022-aktualisiert/#gallery-14783-1, accessed on April 4th, 2023 [25].

and paradigms present systematic barriers to security and privacy for people experiencing poverty, and to encourage this community to adapt to equitably serve people experiencing poverty. We do *not* mean to presuppose that people in poverty *should* be using technology, nor that technology will solve a sociological issue, and we emphasize that in *addition* to ensuring that technical designs align with poor people's needs, we must also advocate for other, non technical changes (e.g., policy changes) in order to address poverty itself.

2 Background

With its important low-wage-industry,[1] Germany is a prime example for the economies of western countries [21], characterized by labor market stratification [22], and increasingly deregulated welfare state policies and institutions [23]. Like other countries in the global north, Germany has a constant gain in poverty although economic performance and the GDP are continuously growing [24], as the latest poverty report indicates (see Fig. 1). The poverty report is published annually by an association of social movements (Paritätischer Gesamtverband) and is based on data from the micro census, which is collected annually by the Federal Statistical Office (Destatis) [26]. According to the poverty report, people are considered "poor" if their income is less than 60 percent of the median income of the country. For a single person living in Germany, this means a yearly income of about 15,000€; for a family composed of two adults and two children, the poverty rate limit is set at 31,500€ [1]. Of the approximately 84,3 million people living in Germany, 14,1 million are considered "poor"; they make up 16,9% of the whole population [27].

[1]More than one in five employees in Germany has a gross hourly wage of less than 11.40 Euros. No other European country with a comparable level of economic development has a low-wage sector that large and persistent: Between 1995 and 2020, the ten percent of the lowest incomes only increased by four percent, while the top ten percent achieved an increase of 50 percent [19, 20].

With some differences regarding the specifics in socioeconomic structure, we argue that overall Germany can be seen as an illustrative case for other countries in the global north, characterized by a strong economy combined with an increasing poverty rate where the population overall has access to technology and the internet, but a growing number of technology users face challenges associated with low income. People affected by poverty generally face barriers and challenges regarding technology and internet access [28]. They also benefit much less from internet use than affluent people [29].

3 Related Work

In this section, we discuss related work in three areas: income status and technology in general, low income in relation to digital security and privacy, and security and privacy behavior, attitudes, and threat models associated with low income.

As early as 2001, Pippa Norris described the entanglement of social, political, and digital inequalities between affluent technology users and users affected by poverty, both within distinct state populations as well as on a global scale [30]. Due to an overall increase in technological penetration and availability across the world [31], questions of technology and internet access are still important but the divide between the rich and poor now takes up plural dimensions that also fuel the interdependence between digital security and inequality [32].

A lot of insightful and valuable research focuses on technology related inequalities in the global south, describing how global digital disparities and access inequalities play out in Bangladesh [33], Georgia [34], the Arab world [35], Mexico [36, 37], Brazil [38], and many other countries. But in countries of the global north like the USA, South Korea [39], UK [40], Italy [41], Canada [42], Japan [43], and Germany [44], income related inequalities are also found to be constantly increasing [45]. These also affect and enforce already present inequalities between genders, age groups, and people living in different geographic locations [46].

Users of low income not only possess less powerful devices but also employ technology and use the internet in ways that give them significantly less financial and social advantages than users of higher income. For example, lower income individuals were shown to be more dependent on their smartphones, to have limited internet access, and to perform less news and information activity than higher income users [47].

Low Income, Security and Privacy: The security and privacy community has increasingly focused on understanding how marginalized and vulnerable populations experience security and privacy, deemed *inclusive security and privacy* [48, 49]. Prior work has focused on the technical use, non-use, needs, mental models, and issues faced by refugees in the US [6], undocumented migrants [50], survivor-victims of trafficking [51], and sex workers [5]—with nuanced findings specific to each group studied, as well as an overall sense that technology and security and privacy in particular do not often fit the needs of marginalized groups [52]. Others have explored the relationships of caretaking and assistance (or lack thereof) with security and privacy and technology, e.g., in libraries [53], during Covid-19 [13, 11], and for the elderly [54]. While many of the groups studied in our field experience poverty, and the lack of financial resources appears for some as connected to security and privacy behaviors, mental models, and experiences, our research community has yet to engage directly, holistically, and qualitatively with the idea of poverty and computer security.

People experiencing poverty are described to be part of "at risk populations" for disproportionate harms and a broad set of attacks like online hate and harassment [52], appear to be forced using less secure software like food sharing apps due to lack of money [55], or face surveillance issues, for instance, related to smart home technologies in public housing facilities [56]. Contrary to the assumption that security and privacy issues lie within the responsibility of low income users who show harmful usage patterns, attitudes, and little literacy, this work shows that security and privacy, moreover, are themselves subject to barriers that need further scrutiny [57].

As people of low income make up an increasingly vulnerable user group that is subject to intensive data gathering, predictive analysis and policing, comprehensive surveillance, and other frequent security and privacy violations [14, 58]—often lacking legal protection [59]—more research is needed to better understand their situation. Currently, the status quo in security and privacy research and design may marginalize users of a low income, both in their everyday lives and during many types of low wage work like gig work. It is shown that security and privacy issues are amplified by work related and private technology available to low income users as well as their specific usage patterns like a higher reliance on mobile connectivity and a greater social media use [59, 60, 61].

Low Income, Behavior, Attitudes, and Threat Models: Low income related challenges in security and privacy among other things are tied to specific threat models, beliefs, advice sources, and behaviors that depend on one another [7, 62]. Prior work has shown that low income users are very well aware of many security and privacy risks and exhibit at least some protective strategies, but are found to lack fitting instruments and suitable resources to better protect themselves [59]. It was highlighted for example, that security and privacy incidents are not causally tied to a low income but are equally distributed through users with differing socioeconomic status [62]. However, it was shown that people of lower income were more vigilant online than people of higher income [52], which surprisingly increased and amplified their already disadvantageous access and usage patterns, as they declined to use online services [63], thus it is important not to understand low income users as a homogeneous group, but to recognize

the characteristics and features of different members as well as their specific connections to other at-risk factors.

We decided on in-depth interviews for our research approach to gain detailed insights into participants' everyday security and privacy actions an practices, as well as their perceptions, behaviors, and reasoning related to security and privacy. We leveraged 28 in-depth interviews with German low income end users to investigate the broader picture of how security and privacy interacts with poverty in countries of the global north, specifically focusing on what is important to them in the context of digital security and privacy and what technology and assets they use and/or seek to protect.

Security, privacy, and sanitization of second-hand devices: For decades, through changing hardware, software, and UI standards, prior work has shown that when users get rid of computers (phones, computers, harddrives, etc), they do not fully sanitize them [64]. Garfinkel et al. showed, through forensic analysis of 158 harddrives in the early 2000s, that used harddrives are difficult to sanitize properly, citing inherent limitations of physical hardware on spinning disks [18]. A decade later, Glisson et al. analyzed 49 cellphones purchased from auctions and pawn shops, finding personal information on all "despite in some cases deliberate attempts by previous users to delete data" [65]. Recent work has also shown significant personal information left on Internet of Things devices [66], SD cards [67], and phones and tablets [68], with some evidence by the prior user to remove their information [67, 69]. Ceci et al. sampled users and found that users do indeed have security and privacy concerns when choosing whether to getting rid of old devices, and that they sometimes *try* to sanitize the devices, but are unable to do so fully because the tools they used were not sufficient [70]. Participants in our work focus on *acquiring* second hand devices—rather than selling or donating them, as in prior work—due to their significantly lower cost than new devices. Our work builds on this body of prior work, then, by understanding the mental model of those in the market for second-hand devices.

4 Interview Study

In this section, we outline the interview approach including the interview procedure. We will elaborate on the recruitment, the structure of our interview guide, the subsequent coding and analysis steps, as well as on ethical considerations, and potential limitations.

4.1 Study Setup

To investigate different employments, experiences, and concerns with security and privacy of low income technology users, we conducted semi-structured interviews ($n = 28$) with people from various backgrounds, education levels, and employment statuses that had 60% or less of Germany's median income at their disposal between May and September 2022. Because of the exploratory nature of the study, and because we focused our investigation on user trade-offs and behavior when using technology on an everyday basis, we opted for interviews as a qualitative approach. The interview as an instrument allows us to explore participants' experiences and concerns in-depth by asking follow-up questions.

Interview Guide: The interviews were conducted with an established interview guide based on our research questions that were tied back to an examination of previous and ongoing related work. First, participants consented to partake in the study before starting the interview, then we asked what devices, apps and other connected technology they are using on an everyday basis. We then asked the participants to describe important and private data, to talk about account sharing, and to report on possible security and privacy incidents in the past. If not mentioned, the remaining questions focused on perceived challenges with, worries about, and experiences with security and privacy.

The initial interview guide was tested with voluntary contacts from our professional network. After their feedback during the pilot phase, we performed minor changes regarding the question order for a better interview flow, and to improve question clarity. We also added follow-up questions to cover relevant areas in-depth until saturation was reached after the fifth interview.[2]

Recruitment and Inclusion Criteria: We based our recruitment approach around covering a diverse set of participants utilizing Open Source Components (OSCs), and employed multiple recruitment channels to better reach a diverse set of low income technology users from different age, educational, work-related, and national contexts. We recruited 28 participants, slightly over-sampling female participants (60% to 40%), from three different age groups (18-25: 18%; 26-34: 54%; 35-67: 28%), different education levels (no degree 4%; high school 46%; BA 22%; MA 28%), and varied employment statuses (no employment 25%; student 39%; self-employed 8%; employed 28%) offline via our professional network, local NGOs consulting unemployed people in Germany, as well as online through second hand goods advertising mailing lists, poverty related twitter hashtags, and Facebook groups:

1. Offline. For recruiting low income users that may not have high internet and technology literacy, we distributed recruitment posters throughout our professional network, and displayed recruitment material at relevant places like NGO offices.

2. Online. In addition to participants recruited offline, we recruited through a varied set of online spaces like second hand goods mailing lists, Facebook groups, and twitter

[2]The full interview guide can be found at https://osf.io/TJA6H/.

hashtags related to low income, poverty activism, and the experience of poverty.

For an overview of the interviewed participants' demographics see also Table 3 in the appendix. Through an invitation link or by scanning a QR code put on recruitment posters, participants were led to a short demographic Qualtrics survey determining whether they could be included in the study.[3]

Participants qualified if they were older than 18 and their household had at most 60% of Germany's net median income (the definition of relative poverty). Participants who were detected to have more than 60% of the median income were not included in the interview sample. As compensation for their valuable time as interviewees, we offered all participants an allowance of 40 €.

Interview Procedure: We conducted the *28* interviews virtually, mostly via our self-hosted instance, or any other tool of the participant's choice (e. g., *Zoom*), or through a phone call, which we recorded after the participant's consent. On the recruiting material, we advertised the interviews with a duration between 60 and 90 minutes depending on answer duration and scheduled all interviews with Calendly or through messaging via email, Facebook or twitter. All interviews were conducted in German and lasted between 40 and 90 minutes.

Overall, the interviews were based around non-leading, open questions, allowing the participants to develop their thoughts and answers. Each interview section started with general questions, allowing participants to freely state what they had on their mind. We asked follow-up questions to elaborate on specific topics if necessary. To avoid priming, we did not use technical or security and privacy specific vocabulary or suggestive argument patterns, and did not judge the answers regarding specific security and privacy practices.

4.2 Interview Structure

The interviews were structured in five main sections consisting of a set of one or two opening questions as well as follow-up questions. Before starting the interview, we provided participants with a general introduction of ourselves, our research project, and an explanation of our goals and the interview process, as well as the interview's role in that process. We emphasized that participation in the interview is voluntary, and that participants could skip any question for any reason without any negative impact on the interview procedure. We made clear that we were not judging their thoughts and knowledge about, behaviors with, and any reported incidents regarding security or privacy. We pointed out that their personal thoughts and opinions were of interest to us and that there was no right or wrong answer. Moreover, we guaranteed full de-identification of any quotes we might use.

[3] Survey questions can be found at https://osf.io/TJA6H/.

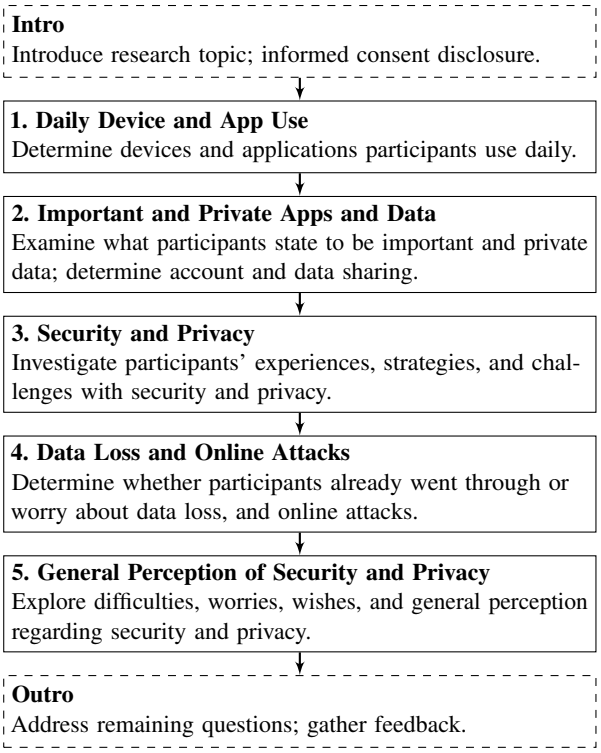

Figure 2: Overview of the interview sequences and procedure. Due to our semi-structured interview approach, participants were allowed to diverge from this interview flow at any time and elaborate on related topics.

After answering and clarifying any remaining questions and obtaining consent for the interview procedure, recording, and data handling, we started recording and began the actual interview with the following structure:

1. Apps and Devices: In the first interview section we asked participants to talk about the devices and apps they use on an everyday basis. This section intends to first gather information on the specificities of low income users' devices and usage patterns. If addressed by the participants, we also discussed old, broken, or already used devices. We report these results in Section 5.1.

2. Important and Private Apps and Data: This section investigates what participants classify as important and private apps and data. It serves to determine which data and apps low income participants describe as important and private, whether they share those data with anyone, and whom they would not want these data and apps being shared with. It also determines participants' experiences and practices of account sharing. We report these results in Section 5.3.

3. Security and Privacy: The third block of questions covers the experiences, behaviors, and challenges with security and privacy participants report about. We asked our interviewees whether they have tried to make themselves more secure

and private in the past, and what makes them sure whether they are secure and private or not. This section serves to determine the security and privacy literacy of low income users as well as their everyday security and privacy strategies. We report these results in Section 5.2.

4. Data Loss and Online Attacks: The fourth section focuses on whether the participants were subject to data loss or online attacks in the past or are worried about online attacks or losing data in the future. Our questions covered aspects such as whether participants worry someone might have access to their important and private data, and if participants think that their person would play a special role regarding online attacks. We also asked how safe and private our participants feel overall and why. We report these results in Section 5.4.

5. General Perception of Security and Privacy: In our final interview section, we investigate our participants' general views on the importance, impacts, and significance of security and privacy in their everyday lives. We were interested in whether our participants would like to change anything regarding their overall security and privacy and how they would make these changes possible. We report these results in Section 5.4.

Following the interview sections, we asked our participants if there was any topic we did not address so far as well as for any additional insights and aspects that we might have missed or they wanted to talk about. We also offered them the opportunity for questions and comments, and after completing the interview, we thanked them for their valuable time and the effort they took while participating in the study.

4.3 Coding and Analysis

Before evaluating, we recorded the interviews digitally, and transcribed them via a GDPR-compliant service, and manually reviewed all transcripts for potential mistakes. We analyzed all interview answers in an iterative open-coding approach [71, 72, 73]. One researcher coded the interview recordings and developed an initial codebook based on the interview guide as well as impressions gained during the interview procedure. The codebook was progressively discussed with other team members, and the feedback was implemented in the codebook, resolving conflicts by consensus or by introducing new (sub)codes after each iteration. The interviews were coded according to the codebook in multiple rounds until saturation was reached and no new codes or themes emerged [74, 75]. Although saturation can be problematic when not well defined [76], we felt it fit our data and it was clear to us when no new codes or themes emerged [74, 75]. The presentation of the paper and the research questions evolved together, explaining the similarities in structure. We did inductive coding [77], iteratively defining research questions, codes, and themes during our analysis: We conducted the interviews with open questions, and generated analysis from data. We took memos during the interviews to find themes and discussed them within the research team. We developed analysis from individual codes to interpretation and theorizing through thematic analysis [78]: Once a topic repeatedly appeared in the interviews, it became a theme. For example, participants repetitively report using old, broken and/or already used hardware, as shown in Table 1, which became the theme *old, broken, and already used devices*. Multiple themes contribute to answering research questions. For example, the theme *old, broken, and already used devices* contributes to RQ3, which is aiming to shed light on the technology and assets participants use and/or seek to protect. As surfaced in the interviews, the use of old, broken and/or already used hardware leads participants to mix private and work related device use (Section 5.1), and to opt into distrusted cloud services (Section 5.2), or into Google services although they mostly do not feel good about it (Section 5.4), because old hardware does not have enough storage space. Also, broken hardware influenced participants' evaluation of assets they seek to protect: As their data is either stored by untrusted cloud services or on hardware tending to break easily, as it is old or already broken, participants show resignation towards protecting their data.

Themes correspond with our results section: use of second hand devices out of necessity; ubiquitous use of broken or/and old devices; mix of private and work devices; Google as a quandary (e.g. little storage space forces into cloud computing); insufficient security and privacy resources other than money related to poverty; a strong feeling of being tracked; false feeling of safety a) because of living in Germany and b) until a security or privacy issue happens; high impact of data loss despite of low risk. Our approach does not necessitate the reporting of intercoder agreement, as each conflict was resolved in situ when it emerged, which resulted in a hypothetical final agreement of 100% [79]. The final codebook of 81 items is included at `https://osf.io/TJA6H/`.

4.4 Ethical Considerations & Data Protection

Our study was realized following the ethical principles for computer security and privacy research involving information and communication technologies outlined in the Menlo report [80], and was positively reviewed by our institution's ethics board and data protection office. The research plan, study procedure, and all involved research parties adhered to the strict German data and privacy protection laws, as well as the General Data Protection Regulation (GDPR). All data was collected, handled, and stored in compliance with the EU GDPR; personally identifiable data was stored using a secure cloud collaboration software. To transcribe the interviews, we commissioned an EU-based, fully GDPR-compliant transcription service.

We provided the participants thorough information about our study procedure and data handling, and offered to answer

any questions they might have before signing up for interviews. We stressed that participants could skip any question for any reason such as not knowing an answer, not wanting to answer, not being allowed to answer, or not feeling comfortable with the question, and told them that they could drop out of the interview process at any time.

To protect participants' identities, we did not ask for granular demographic data: in our pre-survey, we only asked for age groups, and income brackets (monthly, related to the German median income). However, many participants mentioned more granular income data unprompted during the interviews. We asked participants their gender, and did not systematically ask for race or migration history; again, many participants shared this information unprompted during the interview. We similarly did not ask for but often received information on chronic diseases, disabilities, as well as other circumstances and life events relevant to participants' socioeconomic status.

4.5 Limitations

Our study has several limitations that are typical for this kind of interview study, including potential over- and under-reporting, self-report, recall, and social-desirability biases, as well as sampling bias. Our sample is a convenience sample which may not be representative of the larger population of low income technology users. As many participants were recruited online, we may not have studied low income users that do not use the internet on an everyday basis or do not possess technological devices.

The household sizes ranged from one person households, families with up to 1 child to two or multiple adults living without children. Following the qualitative and explorative nature of the study, the demographics are not representative of people living in poverty in Germany. We sampled relatively highly educated people, and we were unable to reach people that do not use technology.

Interviewees who agreed to participate in our study might be more or less aware of the overall problematic revolving around living with a low SES, as some were members of Facebook groups or twitter hashtags tackling poverty as a social problem to be solved.

We conducted our interviews in German, so we have no insight into non-German-speaking low income technology users. As German is the de-facto "common language" in Germany, we consider this to be a negligible drawback still allowing us to reach a meaningful set of low income technology users. We attempted to mitigate social desirability bias by emphasizing that there are no right or wrong answers to our question about security and privacy, and that what matters is the everyday practice and experience of the respective user. We made clear that we were not going to judge the participants or their answers in any way but were genuinely interested in their experiences and thoughts. At any suitable moment, we also reminded our participants that they could skip questions without giving a reason.

5 Results

Our data focuses on how relative poverty affects (or does not affect) one's threat model and technology usage. As discussed, prior work finds that certain sub-populations experiencing poverty encounter certain barriers to security and privacy that are anecdotally related to poverty; our work engages, deeply and qualitatively, with specific reasons that poverty can present a barrier to security and privacy: old and second-hand hardware may have insufficient storage space (Section 5.1) or may be technically unsupported or improperly sanitized (Section 5.1), the use of untrusted software because it is free (e.g., free cloud backups of personal data, Section 5.2), and the feeling that poverty lowers the value of their data to a potential attacker (reflecting a misunderstanding of how and why many identity theft and cyber attacks occur, Section 5.3). We also explore how participants conceptualize *adversaries* (Section 5.4), amplifying their concerns about ad tracking and being unable to pay for privacy by using products for which they do not feel they trade privacy for access/cost (Section 5.4). Finally, also lacking financial, time and emotional resources related to poverty may impede security and privacy (e.g. participants don't want to deal with something they cannot afford anyway (Section 5.4)).

5.1 Hardware: Mixed Use, Typically Older, Secondhand, or Cheap Hardware

Although new smartphones, tablets, and laptops cost hundreds or thousands of euros (a significant fraction of the annual 15000€ income of someone in relative poverty in Germany), they are effectively required for modern day life in a rich industrialized country like Germany. Employers may require workers to be available via telephone and computer without providing either device. Additionally, social technology use is a critical part of our personal lives and exclusion from technology use (e.g., exclusion from social media, connections with far-away loved ones) can be painful [81]. We thus begin by exploring the *hardware* ownership and usage of people in relative poverty, for whom the cost of hardware may be a burden. We observe that both *mixed use* and *second hand* devices can present security and privacy risks to users and prior owners, since they are often improperly sanitized.

We observe that the hardware they use is influenced by poverty as most interviewees rely on old, used, and broken hardware because they cannot afford new devices. The hardware influences what is important to them and what they seek to protect: Although they find pictures, work and health related documents, and private communication data important, interviewees report that they cannot afford to protect them properly. They try their best to protect data that is important to them but always choose the cheapest options. One participant

explicitly and unprompted stated to use a hard drive regularly (P4). Finally, they simply accept the idea and the occurrence of losing data. Additionally, their devices must be affordable and thus do not have much storage space, which forces them to opt into cloud solutions they do not really trust.

Old, Broken, and Already Used Devices: Few participants report using new devices. Most participants report to take over old, broken or already used devices (Table 1) from friends and family members or to buy second hand hardware online, as they prioritize buying food, clothing, and saving for unexpected expenses (P9; P12; P18; P20), like a broken fridge or washing machine (P26). Participants also report often replacing their acquired devices as they break easily, which influences them not to trust the hardware they use:

> "*You must know that I have a very stupid history if you look at the last four or five years. My biography with smartphones is not particularly good, because I never get a new one, but always used ones. And then they usually don't last.*" — *P19*

We find that relying on broken, used, or old devices fills an important connectivity gap for low income users, giving them an opportunity to stay connected professionally and privately (P2; P26). However, these previously used devices can present a security and privacy risk. Prior work has shown that phones and other devices are often improperly sanitized before being passed to a second owner, presenting risks of malware and unwanted programs from the prior owner, and putting the onus on the new owner to ensure that all settings, accounts, data are *their* own in order to avoid tracking between owners. Additionally, Roberts et al. showed that pre-owned devices can contain illegal data or evidence of crimes, which could implicate second owners [17]. Older devices also can present security and privacy concerns, as there is a point at which developers stop issuing security updates, or the old hardware cannot run the newest versions of software.

Mixing Private and Work Related Smartphone Use: Most participants report to use their smartphones for almost everything, including online banking (P10), or even to rely on smartphone use exclusively (P18). Some participants distinguish hardware use between professional and private (P19), but almost every participant mixed private and professional device use (P24). A reason for mixed use is the technical insufficiency of participants' old devices, as P2 reports:

> "*I do have a work laptop, so to speak, but connecting to the office server doesn't work so well and that's why I actually use my own laptop for everything. But that's also why I'm using my cell phone right now, because I don't have a webcam on my old laptop and that's why I've always used the work laptop for Zoom.*" — *P2*

While the mix of work and personal use is not uncommon, as a number of employers expect employees to use their own phones and computers for work—particularly during the pandemic—it can be dangerous for both employee and employer. Employees may be required to sign invasive contracts that give employers control over *all* the data on their device (subjecting them to loss of personal data if the employer exercises the option to wipe the device), while employers' company data may become compromised from something the employee does on their personal time, on their own device.

5.2 Software: Shared Paid Streaming Accounts, Coerced Free Cloud Storage, Online Second Hand Platforms

Not all software and services are free and so those that are not can create a financial burden for relatively poor people. We find that participants' use of *free* communication apps and social media is not remarkably different: all participants report to mostly use communication apps like mailing, WhatsApp, Signal, Telegram, as well as social media apps like Instagram and Facebook. However, we find that in response to the need to back up and store their personal data, participants may turn to free cloud storage services because they are unable to buy hardware with an appropriate amount of storage space. Significantly, they *may not trust these free cloud services to not violate their privacy* but use them because they are free. Additionally, we find that participants frequently use online second hand platforms that require sharing private information with strangers. This may adversely impact their privacy, and even physical safety.

The Risks of Online Secondhand Goods Trading Services: Almost all participants report using online platforms for secondhand goods trading on an everyday basis because they cannot afford new merchandise (P3, P5, P6, P13, P17, P22, P26, P28). Platforms like Vinted, Kleiderkreisel, or Ebay Kleinanzeigen connect a buyer and a seller of secondhand goods, offering a shipment or a personal pickup option, as well as an option to pay through the platform's own payment system or via PayPal, banking, and in cash. There is also the option to give away things for free. To use these platforms, participants must create an account, filling in personal information like the home or any other shipment address, telephone number and email as well as banking or banking app data. Sharing this information with strangers is usually based on the mutual trust that everybody will only use shared data to complete the trade in question and for no other reasons.

One person reported to only search for giveaway things that they pickup in person as they could never afford to buy anything through these platforms including shipment costs.

Table 1: Daily technology use reported by participants. "Old" and "new" as subjectively reported by participants.

	Smartphone	Laptop	PC	Tablet
Old	P1, P2, P5, P7, P16, P18, P20, P21, P23	P4, P10, P16, P21, P23	P16, P18, P21, P26, P28	P3, P16
Used	P19, P25	P3	-	-
Little storage	P7, P11, P20, P25	P21, P25	-	-
Broken	-	P21	P7	-
New	P15, P24, P28	-	P15, P19	P8, P17, P25

To them, this is also part of a security and privacy action: for picking up free handouts, they never expose their own personal information like banking data or their home address, which gives them increased anonymity, security, and privacy *because* they are poor:

> "*I: Do you pass on your bank account details? P: No, no bank account details. I only pick these things up. I: And then you just hand over cash? P: Yes. But I mostly look for things to give away. I'm unemployed, so there's not much to buy.*" — *P26*

Little Storage Space Forces Users into Cloud Computing: The use of old, broken, and pre-owned hardware (Section 5.1) may push users towards more frequent or thorough backups of their personal data (P3; P8) because they are afraid the hardware will break, or because the hardware has minimal storage (P9; P13). Participants expressed that they lack storage space on their smartphones and notebooks, forcing them to either delete data on a regular basis, to store data on external hard drives, or to use cloud services (P9; P13). Some participants perceived physical or offline storage as the best way to protect data from unwanted access—though other participants report not to use cloud systems at all due to safety reasons (P14, P16, P23, P27).

> "*I don't use cloud systems; I don't upload my personal data to iCloud or similar programs and service providers now. Yes, of course it's nice, but then Apple just has all your pictures all the time. And you don't know what they do with them. And why would you also upload the photos there?*" — *P14*

However, although they distrust cloud services like Google Cloud or iCloud, they report that physical hard drives are a financial burden, and so cloud services are the go-to opportunity to receive free or affordable extra storage (P6; P7; P9; P10; P18; P20; P25). This is why they choose to put their data in a cloud or simply do not disable the automatic cloud backup pre-set on their smartphones (P6, P18, P20, P25), but report that they would not use cloud services if they could afford it financially:

> "*If I had more money to buy hard drives, I would change to that and quit the cloud.*" — *P20*

Other interviewees state that the benefits of greater storage space outweigh the costs of potential privacy loss:

> "*My laptop is full, now I can put new stuff on it again. That's the only reason I did this.*" — *P6*

In the face of their mostly cheap and old hardware that does not have much storage space, opting into cloud services seems to be the only solution to store data. Additionally, other interviewees describe that their data is automatically backed up and stored by Google, whether it is private photos, photos of important documents, important files, or (artistic) work files, and that it is impossible or very complicated to shut down this automated backup (P18; P20; P22; P23; P26). Either they describe it as a burden because they cannot access their data offline (P20), or they wish for a "Google-free" phone that they cannot afford (P18):

> "*It would be cool to get a Google-free phone, at all, with a lot of storage space. There are people who can do that.*" — *P18*

> "*Well, my cell phone does that automatically. Yes, I turned this function on myself. And my photos are saved on my Google account. On Google Cloud. And if I don't have internet and want to open photos from 2015, 2016, that doesn't work. I always have to be connected to the internet because it's stored on my Google account.*" — *P20*

Participants' skepticism of cloud storage for privacy reasons is in line with prior work on user attitudes towards cloud storage [82, 83]. While it is beyond the scope of this paper to comment on the security and privacy practices of any one cloud provider, complete deletion [84] and isolation [85] of data in distributed systems are difficult due to data replication and shared hardware. Additionally, prior work shows that cloud UIs can be confusing, and lead users to improperly delete or retain data [86, 87].

5.3 Data: Loss of Personal Data Considered Low Risk but High Impact due to Poverty

Separate from software and hardware is *data*, and how poverty affects what people consider to be their assets (and non-assets), as well as how they perceive threats to their data privacy like data breaches, tracking, and identity theft. We find that participants, in general, consider their personal data as important assets, but in many cases assign it low value specifically because they themselves are poor. The sense that they will not be "worth" an attacker's time because they do not have expensive assets was pervasive. This betrays a potentially dangerous incomplete mental model about how and why data breaches occur: they may be targeted, and user-centric, but they also often occur en masse, by no fault of the user's own, as an online service is breached (and therefore the financial assets of the user are no consideration) [88, 89]. Yet participants explained that if they *did* experience a data breach, e.g., identify theft, the impact would be *high*, also directly because of poverty. Here, we report the *types* of data assets and non-assets that users defined, and discuss their perceived sensitivity and value; we discuss the feeling of "not much to get" further in Section 5.4.

Photos, Mailings, Messages: We find that participants report photos, mailings and messages as important and private data. They consider some photos low-value assets, or even non-assets, while others are considered high value assets. Participants report disuse of social media in response, in line with some prior literature and philosophical non-use [90].

> "*I have the feeling that there is a lot of sharing or oversharing. ... That's already a habit.*" — *P25*

Indeed, pictures showing children mark a threshold and are considered to be extremely sensitive content to avoid posting online (P26). The same applies to photos showing party pictures (P11) or nudes including faces (P20). Generally, oversharing posts and photos through social media was considered an undesirable tendency (P25). A sufficiently secure and private alternative for sharing sensitive photos either does not exist or does not feel usable to participants (e.g., it is not already used by their social group, it costs money, they are skeptical of it). We observe, however, that participants' use of self-deleting messages shows a positive example of a security and privacy feature addressing their concerns and being used.

Banking Data: All participants mentioned their online banking accounts to be important, but were ambivalent regarding the idea of losing their banking data or being scammed (P11; P19; P20; P21). While some participants described feeling safe because they do not have a lot of money and thus do not think of themselves as attractive targets, at the same time they fear losing all their money at once (P2; P3; P6; P11). This is directly related to poverty, as participants have exactly one (instead of multiple) bank accounts, and have no savings nor other financial fallbacks.

> "*I think that's very unlikely for me, because there's not much to get. For example, that someone has the access data for my PayPal account and then somehow steals money from me for small amounts or something.*" — *P3*

> "*Well, if someone stole all my money, I mean, it's not that much. But then of course I'd have a problem and then I'd have no more money. ”* — *P3*

Even though there are legal protections and insurances for the loss of data from a bank [91], and users would likely get their money back in a few days, it is reported to be a source of strong discomfort (P2; P3; P7; P8; P9; P11; P21; P28) because of the lack of financial fallback possibilities that those with higher (relative) income may not experience.

> "*So even if that could be arranged somehow, it's just not a situation I want to get into in the first place. Unfortunately, I only have one account and that's where most of the money is. And if that's gone, then it's not fun. Even if it's only a few days.*" — *P15*

Non-banks, such as PayPal, are not regulated in the same way, and thus a breach can lead to financial loss; however, they remain commonly used for purchasing items, e.g., from online swap/sale sites, and are also used between friends and partners. Interviewees reported PayPal-like phishing emails leading them to uninstall PayPal completely (P11; P21). One participant reported a friend for whom getting money back was impossible after the account has been hacked (P20):

> "*A few months ago, someone hacked into a friend of mine's PayPal account and stole a lot of money from her. And that made me feel pretty insecure about using PayPal. I think she contacted PayPal and they followed up on it. And they said it would take a few months. I don't know yet whether she got her money back.*" — *P20*

We observe that financial regulations *do* protect people from loss if their bank account is breached. However, people experiencing relative poverty may be unable to fulfill their everyday needs—e.g., buying food, paying rent—while they wait for the bank to return their money to their account. We also observe that the use of money-sharing apps, only some of which are regulated as banks, contribute to financial loss that relatively poor people cannot easily withstand, and we bookmark both as opportunities for improvements in technology and policy to protect poor users.

5.4 Adversaries and Risk Perception: States, Criminals, and Companies don't Come for Me

Complementary to hardware, software, and data *assets* and *non-assets* are *adversaries*. We now turn to the *actors* and *adversaries* in participants' threat models, as well as the level of risk that participants believed they posed to their previously defined assets. Participants define different adversaries including state regimes, criminals, and companies crawling data. While many express a high awareness of these adversaries as threats in general, at the same time they do not see themselves personally at risk. Reasons to personally feel safe included living in Germany, which is perceived to be a safe country, as well as not to possess financial means or sensitive data worth getting stealing (in line with their discussion of *non*-assets, in Section 5.3). These threat models may lead to a false feeling of safety. Also we find that participants report financial, emotional and time reasons prohibiting them from gathering more information about security and privacy that would enable them to better protect themselves.

Government Actors: Living in Germany is Perceived to be Safe: Some interviewees have expressed not to perceive any given government-related security and privacy risks while living in Germany. Drawing comparisons to other countries, like the persecution of LGBTQI+ people in Poland (P2), the political system in Iran (P20) or Russia (P12), and the strong social control systems in China (P16; P18), participants reported to feel free in Germany while performing tasks like critical journalism (P5), being unemployed (P16), or politically engaging to move freely through the internet (P18). Others voiced concerns about nation states like Russia influencing the votes in Germany, pointing out that incidents like these were at least publicly discussed (P9). This leads participants not to engage deliberately in security and privacy action like anonymizing their personal data or traces surfing the internet, as the following citation exemplifies. Asked whether they would take action to increase their online security or privacy, P12 replies:

> "*It would have to be something bad where I say: 'No. I can't go on; I have to make myself anonymous now.' In China or Russia, people do it because they know that their data is completely controlled, and here in Germany, at least I don't think that's the case, I think our data is free.*" — *P12*

The feeling of being safe and secure that is connected with living in a democratic constitutional country like Germany might lead to an inaccurate or incomplete assessment of personal security and privacy, as every government may unjustifiably gather personal information or violate digital security of its residents. Also, data gathered can have an unproblematic status now and become a threat in the future, e.g. when the political system undergoes substantial changes.

Targeted Attacks by a Non-State Criminal: Feeling Safe as There is Not Much to Get—Unless Something Happens: Participants generally felt well protected from targeted criminal attacks because of the simple fact that there is "not much to get" from them because they do not possess large amounts of money or important data or information (P13; P15; P19; P22; P23; P25; P27; P28). Participants hypothesized that cybercriminals would be more likely to target public figures, people with significantly more money, or people with substantial social media followings (P2; P8; P9; P14; P16; P17; P18; P23), assuming that "*if this data somehow gets to someone, they cannot do anything with it*" (P16).

Thus in general, we found that participants do not see the urgency or necessity to protect themselves better as long as nothing specific happened to them (P2; P3; P7; P10; P13; P18) — thinking that "*the probability that someone will attack*" would be "*one in a million*" (P28). On the other hand, some interviewees also refer to this perception as an "*illusion of security,*" letting them "*feel safe"* generally, but only "*as long as no one tells me, 'Oh, you've been hacked',*" or until an incident really happens.

Companies: Personalized Ads Lead to a Strong Feeling of Being Tracked: Participants had substantial concerns about online ad tracking and the invasion of their privacy (P10; P18), echoing prior work about user concerns with personalized ads [92]. However, some concerns were technically inaccurate (e.g., ad tracking very likely does not occur due to apps secretly listening via the phone's microphone [93]) and revealed inappropriate coping mechanisms e.g., only rejecting cookies, or changing their behavior in an irrational way:

> "*What actually bothers me is that the algorithm is now so blatant that there is this 'eye tracking' thing or whatever it's called. You can google it. And since then, I've been like no, I no longer look there. It actually stresses me out.*" — *P6*

Another interviewee protected themselves against tracking through rejecting all cookies which "*didn't help much*" (P2) and another put their "*phone on airplane mode during sex because I don't want my privacy to be exploited*" (P20). While these strategies may give them some protection, the myriad strategies that online trackers use for advertising content has extreme depth and will rarely be thwarted by one simple trick. We observe, at a high level, that participants are deeply uncomfortable with tracking, and also are ill-equipped to avoid it, both because of inaccurate mental models regarding how it happens, and because they cannot "buy" their privacy.

Getting personalized ads is often described in relation to big online companies like Instagram, Youtube, Amazon, and Google (P2; P14; P20) and is reported to fuel a strong discomfort due to personalized content being displayed without prior action: Eight participants believed private conversations were tracked by their smartphones (P2; P6; P7; P13; P20; P23;

P26; P27) as they have been shown personalized content after talking with a friend about a product without having actively interacted with the smartphone, e.g., googling for the product.

Some users think it is standard to be tracked by their smartphones, either worrying because they heard about it—"*You keep hearing rumors about how cell phone microphones listen. For example, if you talk about a certain product, you later get advertisements for it or something similar*" (P27)—or because they believe they experience it (P2; P23; P26):

> "*If you think about the fact that I'm talking to a friend on WhatsApp about, I don't know, let's say, foot cream, and then the advertising for foot creams pops up directly on social media. ... We only talked about it via WhatsApp. ... There was no other way. Interestingly enough, the advertising was then displayed to me on Amazon as well.*" — *P26*

We find that mostly Android and a few iOS users reported experiencing situations making them think they were being "eavesdropped" (P2; P6; P7; P20; P23; P26; P27, see: Table 4 in the Appendix). We observe that there is no evidence that modern apps listen for content to feed into advertising algorithms without being otherwise turned to "listen" mode [93].

Google as a Trade-Off: Out of 28 participants, 21 talked about Google unprompted, mostly reporting ambivalent feelings about it, which is why we choose to elaborate on that matter in more detail. Interviewees report using Google as a search engine, saying that 'googling something' is an integral part of their everyday technology use (P13; P16; P18). At the same time, participants voice a general feeling of unease using Google, because it is gathering and harvesting their data (P2; P3; P7; P12; P23; P25).

> "*I also know that companies like Meta and Google or whatnot make their profits by exploiting data. And I still support them, I'm basically giving them the data even though I know it and that bothers me.*" — *P7*

While all participants say that Google is very user friendly and has generally a high amount of usability, some of them are generally convinced that using Google is not safe (P7; P17; P23). Other participants express that leaving Google is the only option that would make their data safer and more private. One participant expresses complete abstinence from Google as an effective security and privacy practice: "*I don't have Google Play Store on my phone. I use a 'Shiftphone' and I have consciously tried not to use Google services*" (P4).

At the same time, leaving Google is reported to be a difficult endeavor, as using Google services is often described as a necessity on four levels: the technical level for Android smartphone users who have to use a Google account in order to use the Play Store (P23; P28). Second, interviewees report that it is very difficult to get rid of Google and shut Google services down, both because either Google trackers are enabled again or because they don't manage to shut off Google connectivity (P14; P15). Third, Google services are reported to be highly usable, participants express to be too 'lazy' to use something else as this would be more complicated (P22; P23) and fourth Google services are connected with many other services the interviewees use in their everyday technology use (P1; P18):

> "*I first tried to uninstall it, to see whether I can uninstall it ... uninstalling is not enough, because you are in this so to speak ... And I tried to write an email and there have been totally complicated answers ... I already talked to people who also have the problem. It's super hard to get out of Google again.*" — *P18*

Even interviewees who manage to shut down Google trackers on a technical level report that they are automatically re-enabled at some point again which one interviewee reports to have been "*annoyed by very much*" (P23). The default Google backup function leaves interviewees wondering why their data are automatically sent to Google which makes them feel uncomfortable and unsafe (P26).

Insufficient Financial, Emotional and Time Resources While Managing Uncertainty: All interviewees self-evaluate to lack deeper knowledge about digital security and privacy and state they could use improvement in knowledge, skill, and protective strategies. Participants connect financial, emotional, and time resources with their security and privacy behavior. Some describe never caring about security and privacy except "*for financial reasons or something like that*", for instance if their banking account would be at risk (P6). Other participants report not to *"have the energy"* to learn more about (P26) or to have *''too much on their plate*" to invest more time in security and privacy although they think that it would be important (P20; P25), as P25 explains below:

> "*I certainly have no good conscience about it, so it's not that I say I feel totally good or something! In the back of my head, I always think that it is actually not so good, but I have just other priorities in life somehow, than to put so much time into it, although it is super important, that is clear to me.*" — *P25*

The interviewees also give other emotional or mental reasons to desist security and privacy action. Many participants report not wanting to think too much about security and privacy as they fear to become "paranoid" about it (P2; P3; P4; P8; P10; P11; P14; P16): "*The more you read into it, the more you drift off into some paranoid conspiracy theories*" (P11). Other participants report not being able to discern whether they appropriately assess security and privacy issues they

read, hear, or know about (P3; P12; P13; P14) which leaves them with a feeling of unease and incompetence, wondering whether "*everything is actually that bad or just okay as it is* " (P12; also P3; P11; P13; P14). Another interviewee linked their lack of engagement with security and privacy directly to their financial situation: They stated that in order to inform themselves more about digital security and privacy, they would "*have to deal with things that I can't afford. And that makes me sad, so I don't do that*" (P26). While poverty is certainly not the only barrier to having an accurate and complete threat model and being able to match one's actions to that threat model, we thus observe, again, directly, that *poverty itself is a barrier to security and privacy*.

6 Discussion

Persistent social structures often prevent upward social mobility [94], especially in Germany [95]. Even for those leaving poverty, the effects of security and privacy practices adopted during times of poverty may persist (e.g., data being hard to remove from the cloud). Our findings, through 28 interviews with low-income users in Germany, show that poverty directly and indirectly impacts security and privacy needs, experiences, and mental models, and that poverty influences what is important to users in the context of digital security and privacy, and what technology and assets they use and seek to protect. We now synthesize key *technical* and *research* recommendations from our work, towards better supporting and understanding those experiencing poverty.

Securing the Use of Old and Second-Hand Devices As we found that the everyday security and privacy actions and practices of people living in relative poverty in Germany are often tied to the use of old, broken or pre-used hardware, we suggest to improve the security of old and second-hand device use. There is extensive prior work showing that old and used devices can be sources of potential security and privacy harms because users often do not properly sanitize their discarded devices, and there is no guarantee that even a wiped device is completely reset and e.g., malware free [96, 18, 17, 64, 65, 67, 70]. An already-used device may also lead to unwillingly sharing identification information like in taking over the Apple ID from a previous user who failed to properly uninstall their information, and certain hardware identifiers that may be used for (ad) tracking cannot (easily) be changed. Additionally, hardware and software ceases to be supported at some point [97, 98], and old devices will not be supported with security updates, leaving potentially exploitable vulnerabilities forever.

We urge manufacturers to expand the lifetime of security update availability, since deprecated operating systems and hardware disproportionately affect low-income users. As relying on old and used devices is standard among low income users, we also recommend developing and establishing usable practices for digitally sanitizing devices before use. We observe that to truly sanitize a device, the functionality must be implemented at the OS level rather than by a third party, and thus strong sanitization practices, with cross-OS usability and recognizability for users, requires coordinated industry support.

However, there are also other actors that may be able to support (or nudge) users and manufacturers into better sanitization practices: there is space for policy to require sanitization, or an agreement of non-sanitization, between old and new device owners, as well as a discussion of non-sanitized data. We also imagine that second hand goods trading platforms may play a role in enforcing and enabling sanitization.

Ensuring Cloud Security is (and Feels) Sufficiently Secure, Private, and Usable: Participants expressed that they use free cloud storage for data because physical (personally owned) hard drives are financially out of reach. However, some participants also expressed discomfort with storing their personal data on a corporately owned and managed cloud, uncomfortable with the access that gives the cloud provider to their personal data. We observe two key tensions that arise here. First, there is a tension between *free* and *not private* manufactured by the business model of free cloud storage. Second, it is tempting to simply recommend technology and policy that puts users in charge of their data when it is in the cloud (e.g., how GDPR allows users a right to be forgotten), yet we recognize that such technology and policy will inherently burden users who are already busy and may not have technical expertise. As our interviews show that people living in poverty are vulnerable at this point, because they *have to* opt into cloud services *and* do not have sufficient resources to ensure (or generate the feeling of) secure cloud use, we recommend researchers technologists and policymakers consider how to move towards improving *secure and usable free cloud services*, as a public utility. More concretely, for example, tools exist to encrypt one's data and move them to the cloud, but there remain open questions about their use, usability, and in-practice security and privacy properties.

Empowering Users With Accurate and Complete Threat Models: Prior work shows that financial poverty does not necessarily correlate with information-poverty or capability [99], and our data also demonstrates that low income users may very well be highly educated and possess a high amount of tech literacy. But this still is not enough to always have adequate security and privacy strategies implemented in their everyday technology use, not only because what users consider important assets they seek to protect is—at least in part—shaped by the scant hardware and software available to them. Also, we observe that poverty may make users feel a false sense of safety because there is "not much to get."

We thus remark on the importance of supporting users in developing accurate and complete threat models including, for example, an understanding of how data breaches happen *to companies* in addition to individuals [88, 89] and thus, for untargeted attacks, "not much to get" should not affect one's mitigation strategies. While a recommendation for user education ultimately puts the burden on users, we argue that it also empowers them to take collective, non-technical action for themselves: to pressure technologists, researchers, and policy-makers through democracy, to take legal action against those who mishandle data, and to boycott services that mistreat users without the intention of doing better. We observe, however, that the burdens of user education can be variable, and with proper design, we would hope they would be manageable.

Prior work has found that people learn cybersecurity behaviors and threat models socially, through their communities [100] as well as in their workplaces or school [62], and in apps [62, 101]. Thus, looking beyond social sources of cybersecuity advice [100], we turn to employer/school practices [62], apps [101], and any other sources of cybersecurity knowledge that people have access to. Prior work has found that IoT device manuals and support pages communicate cybersecurity advice [101], but IoT may be prohibitively expensive for those experiencing poverty, or, as our dataset showed, users may reject IoT for privacy cocnerns, but then also not learn new technical behaviors and mental models through the installation process.

More Work is Necessary to Understand and Alleviate the Impact of Poverty on Security and Privacy: Finally, we implore computer security and HCI researchers to continue to study poverty, particularly employing participatory and qualitative methods, and having an emphasis on doing research *with*, not *about* low income users. Despite tackling a topic that may seem "abstract," we observe that by asking people—experts in poverty through their lived experiences—*directly* about the effects of poverty, they told us *directly* what the effects were.

We also imagine numerous directions for technical and measurement research to measure and further elucidate the effects of poverty on security and privacy, as well as to support users with better technologies. In order to better support poor users, we must first understand the technical security and privacy properties of the platforms they use. Future work could measure and analyze the security and privacy properties of technology that poor people depend on, e.g., government services, second-hand goods trading platforms, third-party payment services. Mixed use device policies ("bring-your-own-device (BYOD) policies") may also be of interest. Such measurement and analysis will provide a basis on which to develop policy and technology that empowers users rather than puts them at risk and makes them feel discomfort.

We emphasize that anything that alleviates the burdens of poverty, including increasing access to security and privacy mechanisms and mental models, helps decrease the marginalization caused by poverty.

7 Conclusion

Although not only internet access and technology penetration but also poverty rates are growing, low income end users are not well studied but make up a growing set of end users with specific experiences, behaviors, and challenges in security and privacy. To address some of these challenges, and to elaborate on experiences, and strategies with security and privacy as well as on threat models low income users have, we conducted *28* in-depth, semi-structured interviews. Focusing on the everyday security and privacy actions and practices of users living in relative poverty in Germany, on the technology and assets they seek to protect, and on what they find important in the context of digital security and privacy, we find that our participants are subject to a series of possible security and privacy threats related to their low income. Because they rely on old, used, and broken devices, frequently engage in online second hand trading, possess little storage space, do not perceive themselves as attractive S&P targets, they may thus falsely feel safe, and do not have the financial, emotional, and time resources to improve their security and privacy, we offer recommendations to the research community, developers, and policy makers that can help better protect low income users and make security and privacy affordable to everybody.

Acknowledgements

We want to thank the anonymous reviewers and shepherd who gave us constructive feedback and helped us making this paper better. We thank the Max Planck Institute for Security and Privacy as well as The George Washington University for financial support. We thank Anna Lena Rotthaler, Marcel Fourné, and Christian Sperneac-Wolfer for their helpful comments to earlier versions of this paper. We want to thank all the the interviewees, as well as our colleagues and friends Clément Dreano, Marisa Kruchen, and Justus Pötzsch who piloted our study and gave constructive feedback.

References

[1] Paritätischer Gesamtverband. *Poverty report*. https://www.der-paritaetische.de/fileadmin/user_upload/Schwerpunkte/Armutsbericht/doc/Armutsbericht_2022_aktualisierte_Auflage.pdf. 04.04.2023. 2023.

[2] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. "Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI '17. Denver, Colorado, USA: Association for Computing Machinery, 2017, pp. 931–936. ISBN: 9781450346559.

[3] Kenneth A Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On, and Irwin Reyes. “Can you pay for privacy? consumer expectations and the behavior of free and paid apps”. In: *Berkeley Tech. LJ* 35 (2020), p. 327.

[4] Susan P Wyche, Sarita Yardi Schoenebeck, and Andrea Forte. “" Facebook is a luxury" an exploratory study of social media use in rural Kenya”. In: *Proceedings of the 2013 conference on Computer supported cooperative work*. 2013, pp. 33–44.

[5] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. “" It’s stressful having all these phones": Investigating Sex Workers’ Safety Goals, Risks, and Practices Online”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 375–392.

[6] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. “Computer security and privacy for refugees in the United States”. In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2018, pp. 409–423.

[7] Rick Wash and Emilee Rader. “Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users”. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, July 2015, pp. 309–325. ISBN: 978-1-931971-249.

[8] Marina Micheli. “Social networking sites and low-income teenagers: between opportunity and inequality”. In: *Information, Communication & Society* 19.5 (2016), pp. 565–581.

[9] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. ““Desperate Times Call for Desperate Measures”: User Concerns with Mobile Loan Apps in Kenya”. In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2022, pp. 2304–2319.

[10] Loris Caruso. “Digital innovation and the fourth industrial revolution: epochal social changes?” In: *Ai & Society* 33.3 (2018), pp. 379–392.

[11] Amelia Morris, Lizzie Coles-Kemp, and Will Jones. “Digitalised welfare: Systems for both seeing and working with mess”. In: *Companion Publication of the 12th ACM Conference on Web Science*. 2020, pp. 26–31.

[12] Tobias Bürger and Andreas Grau. *Digital Souverän 2021: Aufbruch in die digitale Post-Coronawelt?* Bertelsmann Stiftung, 2021. DOI: 10.11586/2021115.

[13] Lizzie Coles-Kemp, Nick Robinson, and Claude PR Heath. “Protecting The Vulnerable: Dimensions of Assisted Digital Access”. In: *Proceedings of the ACM on Human-Computer Interaction* 6.CSCW2 (2022), pp. 1–26.

[14] L Robinson, SR Cotten, H Ono, A Quan-Haase, G Mesch, and W Chen. *Digital inequalities and why they matter. Information, Communication & Society*. 2015.

[15] Martyn Warren. “The digital vicious cycle: Links between social disadvantage and digital exclusion in rural areas”. In: *Telecommunications policy* 31.6-7 (2007), pp. 374–388.

[16] Ahmad Rahmati, Chad Tossell, Clayton Shepard, Philip Kortum, and Lin Zhong. “Exploring iPhone usage: the influence of socioeconomic differences on smartphone adoption, usage and usability”. In: *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services*. 2012, pp. 11–20.

[17] Richard Roberts, Julio Poveda, Raley Roberts, and Dave Levin. “Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones”. In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. 2023, pp. 3332–3346.

[18] Simson L Garfinkel and Abhi Shelat. “Remembrance of data passed: A study of disk sanitization practices”. In: *IEEE Security & Privacy* 1.1 (2003), pp. 17–27.

[19] Markus M Grabka and Konstantin Göbler. “Der Niedriglohnsektor in Deutschland”. In: *Falle oder Sprungbrett für Beschäftigte* (2020).

[20] Markus M Grabka. “Niedriglohnsektor in Deutschland schrumpft seit 2017”. In: *DIW Wochenbericht* 91.5 (2024), pp. 67–76.

[21] Jan Brülle, Markus Gangl, Asaf Levanon, and Evgeny Saburov. “Changing labour market risks in the service economy: Low wages, part-time employment and the trend in working poverty risks in Germany”. In: *Journal of European Social Policy* 29.1 (2019), pp. 115–129.

[22] Marcel Garz. “Labour market segmentation: Standard and non-standard employment in Germany”. In: *German economic review* 14.3 (2013), pp. 349–371.

[23] Bruno Palier and Kathleen Thelen. “Institutionalizing dualism: Complementarities and change in France and Germany”. In: *Politics & Society* 38.1 (2010), pp. 119–148.

[24] European Commission. *Economic forecast for Germany*. https://economy-finance.ec.europa.eu/economic-surveillance-eu-economies/germany/economic-forecast-germany_en. 04.04.2023.

[25] Paritätische Gesamtverband. https://www.der-paritaetische.de/themen/sozial-und-europapolitik/armut-und-grundsicherung/armutsbericht-2022-aktualisiert/#gallery-14783-1. 04.04.2023.

[26] Destatis. https://www.destatis.de/EN/Home/_node.html. 04.04.2023.

[27] Paritätischer Gesamtverband. https://www.der-paritaetische.de/themen/sozial-und-europapolitik/armut-und-grundsicherung/armutsbericht-2022-aktualisiert/. 04.04.2023.

[28] E Carlson and J Goss. *The state of the urban/rural digital divide. National telecommunications and information Administration, United States Department of Commerce*. 2016.

[29] Eszter Hargittai and Kerry Dobransky. “Old dogs, new clicks: Digital inequality in skills and uses among older adults”. In: *Canadian Journal of Communication* 42.2 (2017), pp. 195–212.

[30] P NORRIS. “Digital divide. Civic engagement, information poverty, and the internet worldwide”. In: *Cambridge: Cambridge University* (2001).

[31] Michele E Gilman. “Poverty lawgorithms: a poverty lawyer’s guide to fighting automated decision-making harms on low-income communities”. In: *Data & Society* (2020).

[32] Jawed Siddiqi, Ja’far Alqatawna, and Mohammad Hjouj Btoush. “Do insecure systems increase global digital divide?” In: *Global Business: Concepts, Methodologies, Tools and Applications* (2011), pp. 2102–2111.

[33] Muhammad Nazrul Islam and Toki Tahmid Inan. “Exploring the fundamental factors of digital inequality in Bangladesh”. In: *SAGE Open* 11.2 (2021), p. 21582440211021407.

[34] Ellada Gamreklidze. “Cyber security in developing countries, a digital divide issue: The case of Georgia”. In: *Journal of international communication* 20.2 (2014), pp. 200–217.

[35] Fathiya Al Izki and George Weir. “Information security and digital divide in the Arab world”. In: *Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics*. 2014, pp. 15–24.

[36] Judith Mariscal. “Digital divide in a developing country”. In: *Telecommunications policy* 29.5-6 (2005), pp. 409–428.

[37] Pablo Arredondo Ramírez. “Connectivity and digital inequality in Jalisco, Mexico”. In: *Comunicación y sociedad* 30 (2017), pp. 129–165.

[38] David Nemer, Shad Gross, and Nic True. "Materializing digital inequalities: the digital artifacts of the marginalized in Brazil". In: *Proceedings of the Sixth International Conference on Information and Communications Technologies and Development: Notes-Volume 2*. 2013, pp. 108–111.

[39] Woochun Jun. "A study on the current status and improvement of the digital divide among older people in Korea". In: *International Journal of Environmental Research and Public Health* 17.11 (2020), p. 3917.

[40] Morgan Harvey, David P Hastings, and Gobinda Chowdhury. "Understanding the costs and challenges of the digital divide through UK council services". In: *Journal of Information Science* (2021), p. 01655515211040664.

[41] Giorgio Di Pietro. "Changes in Italy's education-related digital divide". In: *Economic Affairs* 41.2 (2021), pp. 252–270.

[42] George Sciadas. *The digital divide in Canada*. Science, Innovation and Electronic Information Division, Statistics Canada . . ., 2002.

[43] Tetsushi Nishida, James B Pick, and Avijit Sarkar. "Japan' s prefectural digital divide: A multivariate and spatial analysis". In: *Telecommunications Policy* 38.11 (2014), pp. 992–1010.

[44] Katrin Schleife. "What really matters: Regional versus individual determinants of the digital divide in Germany". In: *Research Policy* 39.1 (2010), pp. 173–185.

[45] Fausto Colombo, Piermarco Aroldi, and Simone Carlo. "Nuevos mayores, viejas brechas: TIC, desigualdad y bienestar en la tercera edad en Italia= New Elders, Old Divides: ICTs, Inequalities and Well-Being amongst Young Elderly Italians". In: *Nuevos mayores, viejas brechas: TIC, desigualdad y bienestar en la tercera edad en Italia= New Elders, Old Divides: ICTs, Inequalities and Well-Being amongst Young Elderly Italians* (2015), pp. 47–64.

[46] Wenhong Chen and Barry Wellman. "The global digital divide–within and between countries". In: *IT & society* 1.7 (2004), pp. 39–45.

[47] Eric Tsetsi and Stephen A Rains. "Smartphone Internet access and use: Extending the digital divide and usage gap". In: *Mobile Media & Communication* 5.3 (2017), pp. 239–255.

[48] Yang Wang. "The third wave? Inclusive privacy and security". In: *Proceedings of the 2017 new security paradigms workshop*. 2017, pp. 122–130.

[49] Yang Wang. "Inclusive security and privacy". In: *IEEE Security & Privacy* 16.4 (2018), pp. 82–87.

[50] 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*. 2018, pp. 1–15.

[51] Christine Chen, Nicola Dell, and Franziska Roesner. "Computer security and privacy in the interactions between victim service providers and human trafficking survivors". In: *28th USENIX Security Symposium (USENIX Security 19)*. 2019, pp. 89–104.

[52] 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: *2022 IEEE Symposium on Security and Privacy (SP)*. 2022, pp. 2344–2360.

[53] Nora McDonald, Rachel Greenstadt, and Andrea Forte. "Intersectional thinking about PETs: A study of library privacy". In: *Proceedings on Privacy Enhancing Technologies* 2 (2023), pp. 480–495.

[54] Nora McDonald and Helena M Mentis. "Building for 'we': safety settings for couples with memory concerns". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021, pp. 1–11.

[55] Ame Elliott and Sara Brody. "Straight talk: New Yorkers on mobile messaging and implications for privacy". In: *Technical report, Simply Secure* (2015).

[56] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, and Christopher A Le Dantec. "Spaces and traces: Implications of smart technology in public housing". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 2019, pp. 1–13.

[57] Michael Rosenberg. "The Price of Privacy: How Access to Digital Privacy is Slowly Becoming Divided by Class". In: *UCLA JL & Tech.* 20 (2016), p. i.

[58] Virginia Eubanks. *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press, 2018.

[59] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick. "Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans". In: *Wash. UL Rev.* 95 (2017), p. 53.

[60] Marina Micheli, Christoph Lutz, and Moritz Büchi. "Digital footprints: an emerging dimension of digital inequality". In: *Journal of Information, Communication and Ethics in Society* 16.3 (2018), pp. 242–251.

[61] Kendra Albert. "Gig Work and the Digital Security Divide". In: *Enigma 2018 (Enigma 2018)*. 2018.

[62] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. "How I learned to be secure: a census-representative survey of security advice sources and behavior". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pp. 666–677.

[63] William H Dutton, Grant Blank, and Egle Karpauskaite. "A Digital Privacy Divide: How Privacy Concerns Reinforce Inequalities Online". In: *Available at SSRN 4177311* (2022).

[64] William Bradley Glisson, Tim Storer, Andrew Blyth, George Grispos, and Matt Campbell. "In The Wild Residual Data Research and Privacy". In: *arXiv preprint arXiv:1610.03229* (2016).

[65] William Bradley Glisson, Tim Storer, Gavin Mayall, Iain Moug, and George Grispos. "Electronic retention: what does your mobile phone reveal about you?" In: *International Journal of Information Security* 10 (2011), pp. 337–349.

[66] Peiyu Liu, Shouling Ji, Lirong Fu, Kangjie Lu, Xuhong Zhang, Jingchang Qin, Wenhai Wang, and Wenzhi Chen. "How iot re-using threatens your sensitive data: Exploring the user-data disposal in used iot devices". In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2023, pp. 3365–3381.

[67] Andrew Jones, Olga Angelopoulou, and L Noriega. "Survey of data remaining on second hand memory cards in the UK". In: *Computers & Security* 84 (2019), pp. 239–243.

[68] Olga Angelopoulou, Andy Jones, Graeme Horsman, and Seyedali Pourmoafi. "A Study of the Data Remaining on Second-Hand Mobile Devices in the UK". In: *Journal of Digital Forensics, Security and Law* 17.2 (2022), p. 5.

[69] S Diesburg, C Adam Feldhaus, M Al Fardan, Jonathan Schlicht, and Nigel Ploof. "Is your data gone? Measuring user perceptions of deletion". In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. 2016, pp. 47–59.

[70] Jason Ceci, Hassan Khan, Urs Hengartner, and Daniel Vogel. "Concerned but ineffective: User perceptions, methods, and challenges when sanitizing old devices for disposal". In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 2021, pp. 455–474.

[71] Kathy Charmaz. *Constructing Grounded Theory*. Sage, 2014.

[72] Anselm Strauss and Juliet M Corbin. *Grounded theory in practice*. Sage, 1997, p. 288.

[73] Juliet Corbin and Anselm Strauss. “Grounded theory research: Procedures, canons and evaluative criteria”. In: *zfs* 19.6 (1990), pp. 418–427.

[74] Cathy Urquhart. *Grounded theory for qualitative research: A practical guide*. Sage, 2012.

[75] Melanie Birks and Jane Mills. *Grounded theory: A practical guide*. Sage, 2015.

[76] Michelle O’reilly and Nicola Parker. “‘Unsatisfactory Saturation’: a critical exploration of the notion of saturated sample sizes in qualitative research”. In: *Qualitative research* 13.2 (2013), pp. 190–197.

[77] Juliet M Corbin and Anselm Strauss. “Grounded theory research: Procedures, canons, and evaluative criteria”. In: *Qualitative sociology* 13.1 (1990), pp. 3–21.

[78] Gareth Terry, Nikki Hayfield, Victoria Clarke, and Virginia Braun. “Thematic analysis”. In: *The SAGE handbook of qualitative research in psychology* 2 (2017), pp. 17–37.

[79] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. “Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice”. In: *Proceedings of the ACM on human-computer interaction* 3.CSCW (2019), pp. 1–23.

[80] Erin Kenneally and David Dittrich. “The Menlo Report: Ethical principles guiding information and communication technology research”. In: *SSRN Electronic Journal* (Aug. 2012).

[81] Alexander Seifert, Matthias Hofer, and Jörg Rössel. “Older adults’ perceived sense of social exclusion from the digital world”. In: *Educational Gerontology* 44.12 (2018), pp. 775–785.

[82] Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. “Home is safer than the cloud! Privacy concerns for consumer cloud storage”. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 2011, pp. 1–20.

[83] Dominik Wermke, Nicolas Huaman, Christian Stransky, Niklas Busch, Yasemin Acar, and Sascha Fahl. “Cloudy with a chance of misconceptions: exploring users’ perceptions and expectations of security and privacy in cloud office suites”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 2020, pp. 359–377.

[84] Roxana Geambasu, Tadayoshi Kohno, Amit A Levy, and Henry M Levy. “Vanish: Increasing Data Privacy with Self-Destructing Data.” In: *USENIX security symposium*. Vol. 316. 2009, pp. 10–5555.

[85] Sultan Aldossary and William Allen. “Data security, privacy, availability and integrity in cloud computing: issues and current solutions”. In: *International Journal of Advanced Computer Science and Applications* 7.4 (2016).

[86] Kopo Marvin Ramokapane, Awais Rashid, and Jose Miguel Such. “{“I} feel stupid I {can’t}{delete...”}: A Study of {Users’} Cloud Deletion Practices and Coping Strategies”. In: *Thirteenth symposium on usable privacy and security (SOUPS 2017)*. 2017, pp. 241–256.

[87] Yijing Liu, Yan Jia, Qingyin Tan, Zheli Liu, and Luyi Xing. “How Are Your Zombie Accounts? Understanding Users’ Practices and Expectations on Mobile App Account Deletion”. In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 863–880.

[88] Dinei Florêncio, Cormac Herley, and Baris Coskun. “Do strong web passwords accomplish anything?” In: *HotSec* 7.6 (2007), p. 159.

[89] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. “An {Administrator’s} Guide to Internet Password Research”. In: *28th large installation system administration conference (LISA14)*. 2014, pp. 44–61.

[90] Morgan G Ames. “Managing mobile multitasking: The culture of iPhones on Stanford campus”. In: *Proceedings of the 2013 conference on Computer supported cooperative work*. 2013, pp. 1487–1498.

[91] Norbert Pohlmann and Norbert Pohlmann. *Sichtweisen auf die Cyber-Sicherheit*. Springer, 2019.

[92] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. “What makes a “bad” ad? user perceptions of problematic online advertising”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021, pp. 1–24.

[93] Rich Haridy. *Facebook isn’t secretly listening to your conversations, but the truth is much more disturbing*. Sept. 2019. URL: https://newatlas.com/computers/facebook-not-secretly-listening-conversations/.

[94] ORGANISATION FOR ECONOMIC CO-OPERATION and DEVELOPMENT. *Broken Social Elevator?: How to Promote Social Mobility*. Organization for Economic, 2018.

[95] Fabian Stephany. “It deepens like a coastal shelf: Educational mobility and social capital in germany”. In: *Social Indicators Research* 142.2 (2019), pp. 855–885.

[96] Laurent Simon and Ross Anderson. “Security analysis of android factory resets”. In: *4th Mobile Security Technologies Workshop (MoST)*. 2015.

[97] *Android OS*. Oct. 2023. URL: https://endoflife.date/android.

[98] Martyn Casserly. *iOS versions: Every version of iOS from the oldest to the newest*. Sept. 2023. URL: https://www.macworld.com/article/1659017/ios-versions-list.html.

[99] Manir Abdullahi Kamba and Yushiana Mansor. “From information-poverty to information-rich: ICT as enabler”. In: *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*. IEEE. 2010, F–21.

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

[101] John M Blythe, Nissy Sombatruang, and Shane D Johnson. “What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?” In: *Journal of Cybersecurity* 5.1 (2019), tyz005.

[102] Statistisches Bundesamt. *Penetration rate of selected information and communications technology devices among private households in Germany from 2014 to 2022 [Graph]*. In Statista, Oct. 27, 2022. URL: https://www.statista.com/statistics/468876/ict-devices-household-penetration-rate-germany/ (visited on 04/04/2023).

Appendix

Below we present supplementary data and tables for our work.

Table 2: Penetration rate of selected information and communications technology devices among private households in Germany from 2014 to 2022 [102].

	2014	2015	2016	2017	2018	2019	2020	2021	2022
Mobile phone	93.6%	93.5%	95.1%	95.5%	96.7%	97%	97.5%	97.6%	98.1%
Internet connection	78.8%	88.2%	89.3%	91.1%	92.7%	93.5%	94.3%	94.7%	95.5%
PC total	87%	88.3%	88.6%	90%	90.4%	91.6%	91.9%	92.3%	92%
Smartphone [1]	—	—	—	—	—	—	—	—	88.1%
Mobile PC (laptop, netbook, tablet)	68.3%	73.5%	75.4%	79%	81.2%	82.4%	83.4%	84.8%	85.2%
Landline phone	91.5%	91.5%	91%	90.9%	84.9%	86.4%	85.3%	84.3%	82.9%
Desktop PC	54%	51.3%	49.4%	48.6%	44.2%	44.6%	44%	44%	42.9%
Navigation device	48.3%	49.7%	50.8%	50.6%	45.8%	46.2%	44.4%	41.2%	39.3%

[1] There is no data available regarding the penetration rate of smartphones among private households in Germany from 2014 to 2021.

	Men		Women		Total	
	No	**%**	**No**	**%**	**No**	**%**
Age	11	40	17	60	28	100
18-25	1	4	4	14	5	18
26-34	6	22	9	32	15	54
35-67	4	14	4	14	8	28
Education	11	40	17	60	28	100
No degree	0	0	1	4	1	4
High School	5	17	8	29	13	46
Bachelor's	2	8	4	14	6	22
Master's	4	14	4	14	8	28
Employment	11	40	17	60	28	100
Student	4	14	7	25	11	39
Unemployed	3	11	4	14	7	25
Self-Employed	1	4	1	4	2	8
Employed	3	11	5	17	8	28

Table 3: Participant demographics.

Smartphone Total participants N=28	**iPhone** N=13	**Android** N=14	**Shift-Phone** N=1
Feeling tracked	1	7	-
No mention of feeling tracked	12	7	1

Table 4: Reported feelings of being tracked by their Smartphone.