Digital Privacy Perceptions of Asylum Seekers in Germany

An Empirical Study about Smartphone Usage during the Flight

ENNO STEINBRINK, LILIAN REICHERT, MICHELLE MENDE, and CHRISTIAN REUTER,
Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Germany

Since 2015, an increased number of asylum seekers is coming to Europe. These migration movements increasingly rely on digital infrastructure, such as mobile internet access and online services, in order to reach their targeted destination countries. Asylum seekers often use smartphones for information and communication purposes. Even though there are many positive aspects in the use of such technologies, researchers have to consider the perceived risks of this specific user group. This work aims at investigating the use of mobile information technologies by asylum seekers during their flight, especially taking privacy into account. Thus, it examines asylum seekers' digital privacy perceptions and identifies privacy protection behaviors by conducting a qualitative interview study with 14 asylum seekers who applied for asylum in Germany. The results show that asylum seekers are often aware of the various risks deriving from the use of smartphones and ICT, such as surveillance and persecution by state or non-state actors as well as extortion by criminals. Based on this, this work furthermore outlines different strategies used to manage these risks. Since the lack of privacy and trust leads to avoidance behavior, the insights of this study provide valuable information for the design of assistance apps and collaboration platforms, which appropriately address the specific needs for digital privacy in the context of flight, or for the conception of privacy-enhancing technologies helping to achieve this.

CCS Concepts: • **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → *Empirical studies in HCI*; *Empirical studies in collaborative and social computing*.

Additional Key Words and Phrases: digital privacy; ICT; smartphones; social media; refugees; migration

ACM Reference Format:
Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 382 (October 2021), 24 pages. https://doi.org/10.1145/3479526

1 INTRODUCTION

Due to the large number of political tensions and intensified by the conflict in Syria, the number of asylum seekers in Europe has been increased over the past years. In 2015, the number of asylum seekers more than doubled to 1,255,600 initial applications in member states of the European Union (EU), of which 35% – more than a third – applied for asylum in Germany. This represented an increase of 155% compared to the year before [17]. Although the number of asylum applications in Germany is declining since 2018, refugee and migration flows remain a challenge for German as well as European politics. The continual conflicts in Syria, South Sudan, Yemen, Afghanistan, and in many other countries cause that the flow of refugees is not likely to abate anytime soon. In this article, we refer to the term 'asylum seekers' as people who have submitted an application for

Authors' address: Enno Steinbrink, steinbrink@peasec.tu-darmstadt.de; Lilian Reichert; Michelle Mende; Christian Reuter, reuter@peasec.tu-darmstadt.de, Technical University of Darmstadt, Science and Technology for Peace and Security (PEASEC), Pankratiusstrasse 2, 64289, Darmstadt, Germany.

2573-0142/2021/10-ART382 $15.00
https://doi.org/10.1145/3479526

asylum on which a decision has not been made [21]. Thus, we include 'refugees' in accordance with the *1951 Refugee Convention* as well as 'economic migrants', meaning people who decided to leave their country of origin due to a lack of economic prospects and structural poverty [14, 16], that applied for asylum. When referring to flight, we refer to the journey to leave a country in order to apply for asylum in another one, involving (possibly multiple) illegal border crossings and often, but not necessarily, by the use of the services of people smugglers. These criteria are often met not only by the journeys of refugees, but also by the migration journeys of economic migrants as well, since they often move on the same routes using the same means, which is referred to as "mixed migration" [55].

With the emergence and increasing use of smartphones worldwide, accompanied by a surge of new communication tools as well as mapping technologies, social networks have become immensely popular. Not surprisingly, asylum seekers on their journey increasingly make use of these technologies as well [13]. They use their smartphones to be better informed, e.g. about their current location and further route, or to keep in touch with their friends and relatives. In addition to that, map services, such as *Google Maps*, do not only help refugees to find their way, but enable them to communicate their location for emergency calls at sea during their flight [61]. In the past years, various state and civil society actors have responded to the increasing use of technology in the context of flight by developing apps and other platforms specifically for asylum seekers on their way. The International Organization for Migration (IOM), for example, has designed the *MigApp*, an app which provides safety-relevant information on flight routes, visa requirements, health guidelines or migrant rights [35]. Hence, access to technology can be highly relevant for asylum seekers and contribute to their autonomy and self-empowerment [13, 61, 67]. But privacy concerns can affect the adoption of digital tools [45]. Especially considering the fact that vulnerable populations are more exposed to privacy risks [47], there is a need for privacy researchers and designers to consider the specific needs and challenges. In contrast to the average user, the consequences of surveillance and privacy breaches can be immediate and severe for someone who is politically persecuted.

While past CSCW and HCI research frequently focused on the use of smartphones and information and communication technologies (ICT) of migrants and refugees at their target destination [11, 12, 33, 37, 44, 46] or on how these technologies are used in the Global South in general [5, 10, 65], the digital usage behavior of asylum seekers *during* flight is an increasingly relevant research area of CSCW. Given the specific risks and challenges to which asylum seekers can be exposed during the flight, such as border controls, governmental surveillance, and persecution in the country of origin [13], we assumed that the use of smartphones and the associated risk-benefit considerations differ strongly from the use of migrants in less threatening situations. Because of the increased vulnerability, we expected these differences to be especially pronounced for considerations regarding privacy. Due to the fact that privacy concerns can lead to self-restricted user behavior [5, 29] and thus impair the potential for digital collaboration, the specific requirements within this context need to be researched. As we will later find, the fear of stately persecution or extortion by criminals leads to specific smartphone usage patterns of asylum seekers aiming to protect their privacy. Thus, in order to support the protection of the private data during flight, it is necessary to explore these usage patterns as well as underlying privacy perceptions. By conducting interviews, our study examines the smartphone-related privacy challenges, perceptions and risks of asylum seekers during their flight. Our results contribute to the exploration of privacy related user behavior in ICT use during flight. Further, they confirm previous research results regarding the smartphone use of refugees in general. Last but not least, the results imply some generic design decisions for the conception of assistance apps and platforms, to adequately factor in the observed privacy strategies of asylum seekers.

We will, firstly, outline the state of research on the relevance of smartphones and privacy in the context of flight as well as related user behaviors (Section 2). Afterwards, a description of the research method will be given (Section 3) and the results of the analysis of the interviews will be presented (Section 4). Based on that, there will be a summary as well as a discussion of the findings (Section 5), followed by a conclusion (Section 6).

2 BACKGROUND AND RELATED WORK

The following section will first outline central studies on the smartphone usage behavior of asylum seekers or refugees as well as in the context of migration. Then it will present privacy strategies and issues in the flight context based on the existing literature. Thereafter, we will present findings on the importance and use of online platforms for and by asylum seekers on the flight. Lastly, we will work out the research gap and present the research questions of this work.

2.1 Smartphone Usage of Asylum Seekers and Refugees

Today, migration movements no longer depend solely on physical infrastructures (e.g. transportation) but increasingly on digital ones (e.g. social media, Wi-Fi hotspots) [23, 41]. As a result, refugees and asylum seekers are using various apps on their flight. Although smartphones are increasingly important for the journey, there are only a few studies that explicitly examine their use during the flight. Alencar [6] gives a general overview of previous research done in the context of refugees' smartphone use and Pannocchia et al. [50] summarize works on ICT usage in the context of migration in general. In the following, we mention the most important findings that provide a context to our study.

Emmer et al. [15] studied quantitatively the user behavior of refugees arriving in Germany before, during and after the flight. They found that about 80% of Syrian and Iraqi refugees were in the possession of a smartphone during the flight. Searching for information with the help of *Google Maps* was the most relevant functionality, followed by communication with relatives and friends, mainly via *WhatsApp*. [15] Comparable results have been pointed out by AbuJarour [1], Ullrich [61] as well as Köver and Tsianos [40]. Furthermore, Almohamed and Vyas [7] are pointing to the fact that smartphones and the use of technology remain important for refugees even after they have reached a safe country, for example when looking for work or finding other relevant information such as housing opportunities, language courses or other buddy programs.

AbuJarour and Krasnova [3] and AbuJarour et al. [2] found that smartphone usage after arriving in a safe country is essential for the inclusion process of refugees. Smartphones represent a centerpiece of refugee ICT use, with refugees using a multitude of different apps on their phones, including *Facebook*, *WhatsApp* and *Google Maps*. Coles-Kemp et al. [12] highlight the importance of smartphones for asylum seekers and refugees to adapt and orientate in a new country by granting them access to digital services, while also creating new threats and vulnerabilities. Also, Coles-Kemp and Jensen [11] come to the conclusion that under precarity of arriving in a new country accessing the benefits of digital services are the primary concern, rather than averting negative consequences. But the utility of smartphones is not limited to the use after the arrival: Especially due to the limited resources that refugees have access to when crossing multiple borders, smartphones are an important and useful tool, as AbuJarour and Krasnova [3] note. Moreover, due to the banishment of international calls in some areas by certain governments, for some refugees communication apps provide the only accessible option to get in touch with their family and friends who stayed at the place of origin [1, 3, 4].

Refugees are often suspicious towards ICT since they fear the surveillance by traditional institutions as well as by other refugees [30]. This might affect the work of aid organizations such as the UN Refugee Agency (UNHCR), which has developed a standardised approach to registration in

refugee camps [18, 28]. In this context, humanitarian organizations as well as other actors wrongly assumed that refugees in need of assistance would be willing and happy to provide personal data to receive offers of assistance [30]. However, Hayes [30] concluded this assumption was wrong and that refugees prefered to remain anonymous, being concerned about a possible surveillance by state and non-state actors. Thus, communication would be mainly conducted on closed networks such as *WhatsApp* instead of *Twitter* or *Facebook*.

2.2 Privacy Strategies of Asylum Seekers and Refugees Using Smartphones

When referring to the privacy strategies of refugees, privacy is understood as "the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others" [63]. Especially due to the spread of mobile apps on smartphones and other devices, privacy has become one of the most widespread topics [66], since many users do not want to share data with certain entities, but are unaware of the data they share by using smartphones and apps [31]. When referring more precisely to personal data in the case of refugees, these include data that can be used to identify them such as physical, social and financial data [9]. In a qualitative study conducted by Dekker et al. [13], interviewed refugees have reported that they restricted their smartphone use when suspected of being monitored by government-related organizations or border patrol. Moreover, they were afraid of their signal being traced back [13]. These results indicate that the refugees were aware of the risks of digital surveillance and developed strategies to avoid them, such as turning off their smartphones or avoiding the use of certain privacy threatening social media apps [13].

Against this backdrop, Rohde et al. [53] examined specific patterns in the use of social media emerging during wartime in HCI. Concerning the special environment, they found that communication was generally limited to a familiar environment due to the fear of surveillance. They further pointed out the tendency to create anonymous avatars and aliases as their social media profiles, which proofed the existence of some understanding of privacy [53]. Nevertheless, Kaurin [38] outlined that even when refugees are aware of the possibility of government surveillance, they still rely on social media as an important source of information and connectivity. Newell et al. [49] found that undocumented migrants on the Mexican-US border perceived the use of smartphones to be risky. Because of their fear that their smartphones could be confiscated, they preferred using *Facebook* for communication, which they considered less risky than mobile communication apps [49]. In a study on communities of undocumented migrants in the USA, Guberek et al. [29] find that the reliance on social media conflicts with privacy and leads to self-censorship for some, while others are meet the risks with resignation.

Many refugees rely on the use of apps and thus face the risk of involuntarily sharing data [30]. Within a study conducted by the International Rescue Committee, refugees were specifically asked about the relevance of privacy. 33% of the respondents said that they had been asked for personal information that they would rather have kept to themselves. 30% have had concerns about sharing personal information on *Facebook*, 52% said it was safe and 15% of respondents were unsure. Respondents considered their phone numbers, *WhatsApp* messages, and their names as sensitive information but not their location data and date of birth [36]. Gillespie et al. [22] find the reasons for this mistrust lie in the fear of state persecution or oppression, and also in the danger of being arrested or deported. As Simko et al. [57] state, refugees face several hurdles regarding their privacy such as a lack of technical knowledge or simply prioritizing other tasks such as establishing themselves in a new country over privacy concerns. Furthermore, they point out that the aspect of digital privacy is already being discussed to a greater extent in the USA. Since they assume that refugees are less informed in their interaction with technologies such as mobile apps and might have to face language barriers, possible challenges for the development mobile apps have to

be considered. Thus, refugees should be categorized as a highly vulnerable group that requires a responsible approach [57].

Generally, it should be noted that digital technologies are increasingly being used by actors like the European border regime or UN agencies to control and steer migration movements [30, 38]. Due to this, Hayes [30] speaks of a "securitization of international migration". During the asylum process, refugees are expected to provide a large amount of personal and biometric data [38]. It has become common practice in some EU member states to confiscate refugees' devices to access sensitive data on social media verifying their identity or to perform a "safety check" on them [8, 30, 48]. The collected data include information on the applicant's country of origin, age, denomination and marital status and aims to uncover contradictory information [38, 41, 48]. The data obtained can have a negative effect on the refugees' asylum procedure if there is any doubt about the credibility of the reasons for flight [30].

Despite the mentioned aspects of privacy behavior towards state actors and other institutions, additional privacy issues can arise from sharing devices whilst being on the move. Ahmed et al. [5] found that, while sharing smartphones is common practice in some regions of the Global South, even within a family it can lead to privacy issues and consequently to self-restrictive user behavior, for example to avoid being subject to blackmail. Privacy issues were also reported for working migrants that had to share devices [46]. These findings might be likewise valid for ad hoc refugee groups forming during flight and sharing devices, especially considering the lower familiarity between group members.

2.3 Online Platforms for Asylum Seekers

When developing apps or platforms specifically for asylum seekers, the provided information must be relevant, available for the target group in a timely manner and adaptable for changing contexts [36]. This is supported by the findings of Talhouk et al. [60] who state that apps aiming to help refugees on their journey are mostly used by volunteers, rather than by the target group itself. Therefore, there is a gap between the expectations regarding the use and functionality of these apps and the actual use by their target group. Talhouk et al. [59] pointed out a need to explore how HCI research fits within wider humanitarian research and digital humanitarianism. It has to be explored, how technologies are currently used and how they could be used better to address refugee needs. By this, technology could potentially contribute to the prevention of unnecessary human suffering or exploitation, e.g. by traffickers.

Some studies point to the existence of *Facebook* groups named, for example, "Smuggling Into the EU" or "How to Emigrate to Europe". In these groups, refugees can access information, offers from smugglers and compare different routes, destinations and costs with each other. AbuJarour and Krasnova [3] notice that relevant information changes frequently for refugees. Therefore, social media platforms are used by refugees for information management through "crowdsourcing". This crowd, they argue, is usually organized in specialized groups on social media sites [3]. On the basis of easily available, inexpensive information refugees are able to make decisions after a cost-benefit analysis. At the same time, it bears the difficulty of assessing the reliability of the offers and information on these platforms [61]. Within social media, traffickers can target potential victims more quickly [39, 41]. Also, since there are hardly any legal entry possibilities to Europe for many people from the Global South, asylum seekers often depend on non-verified information on illegal border crossings. This can also lead to highly unrealistic expectations about their target destinations based on rumors circulating on social media [15].

Given the relevance of global refugee movements and the precarious situation in which people put themselves, besides the scientific interest, there is a sociopolitical relevance to improve the quality of smartphone apps [60]. Especially for refugees, it is crucial to have access to up-to-date

and reliable information. The better informed refugees are about their rights, legal status, escape routes and support services, the more likely they are to manage risks and make sovereign decisions [36]. Access to online technologies can contribute to the self-empowerment of refugees since it enables them to use helpful features of interactive technologies. Thus, it is important to ensure the protection of their personal data.

2.4 Research Gap and Questions

In European refugee policy, Germany has been a major player in dealing with refugees in recent years and it has been one of the most selected destination countries [17]. Against this background and the increasing use of ICT for communication, information and collaboration within this context, it is a highly relevant research environment for CSCW. While there is a rich body of HCI and CSCW research within the context of the Global South and on ICT use for integration and adaption of asylum seekers in a new country [1, 3, 11, 12] or within refugee camps [42, 62], the literature specifically focusing on the user behavior during the journey is limited. Previously conducted studies provide a rough overview of the digital user behavior of refugees [15, 24, 42]. There are some qualitative studies that have examined how Syrian refugees use social media for migration decision making [13] and how ICT contributes to the collective agency of refugee groups during flight [61]. However, these studies did not focus on the issue of privacy, therefore specific details regarding this topic were not asked for and the contextual knowledge of refugees was not captured. Thus, a comprehensive understanding of the refugees' perception of digital privacy is missing in the research process (*research gap 1*). Latonero et al. [42] mention that refugees had "nuanced views on privacy and information sensitivity" and highlight the need to understand them. Also, it has been outlined that there is an imperative need to further understand the role of ICT in serving refugees information needs [51]. In this context, research is needed to identify the reasons behind the user behavior of people on the run (*research gap 2*). In the context of the civil war in Syria, it was shown that the political context is of great relevance for the understanding of digital privacy, since factors such as surveillance, security and trust have a strong impact on the usage behavior of technology [53]. Rohde et al. [53] identify a lack of research in context of the use of mobile media during the flight from civil war. This lack of empirical research is affecting organizations that develop interactive refugee support technologies [42].

Considering these research gaps, this paper will try to find out how relevant digital privacy is for asylum seekers and how privacy related knowledge is acquired during the flight (*research question 1*). Further, we will work out how it impacts their phone usage behavior during their journey and what strategies emerge among asylum seekers to protect their digital privacy during the journey (*research question 2*). Without detailed empirical knowledge about the micro-level of actors, there is a danger that technological approaches will be ineffective and unused by the target group [42]. The present work aims to address this knowledge gap and provides an important foundation for the responsible development of interactive technologies in the context of flight.

3 METHOD

In course of the study we carried out 14 partially standardized, semi-structured guideline interviews. This qualitative approach was chosen to generate detailed information and complement existing quantitative research that mostly used closed-ended question formats. In the following, we will describe the specifics of the research method. First, Section 3.1 describes the sampling strategy and the way interviews were conducted, followed by an description of the data collection process (3.2) and an explanation of the data analysis (3.3).

Table 1. List of Selected Interview Partners.

Code	Country of Origin	Gender	Interview Language	Reason for Flight
P1	Afghanistan	m	German	Conflict
P2	Afghanistan	m	German	Conflict
P3	Afghanistan	m	German	Conflict
P4	Turkey	m	German	Persecution
P5	Afghanistan	m	German	Conflict
P6	Turkey	m	English	Persecution
P7	Turkey	m	English	Persecution
P8	Iran	m	German	Persecution
P9	Syria	m	German	Conflict/Persecution
P10	Ghana	m	English	Economic
P11	Syria	f	German	Conflict
P12	Turkey	m	German	Persecution
P13	Syria	m	German	Conflict/Persecution
P14	Ethiopia	m	Amharic	Conflict/Economic

3.1 Sampling Strategy

Since most refugees who arrived in Germany between 2015 and 2017 were male and in the age span of 16 to 35 years, as the statistics by the Federal Office for Migration and Refugees state [19], the sample was selected accordingly in order to uncover typical characteristics of the smartphone use of this group. Hence, in the beginning of the study, young, single men between the ages of 16-35 years, who have left their country of origin due to political persecution, violent conflicts and / or a lack of economic perspective, applied for asylum in Germany and that were living in Germany at the time, were sought for as typical cases. Later, additional participants differing in age and gender were selected, so that the final average age of the interviewees was $M = 30.7$ years with a range from 19 to 48 years. Table 1 gives an overview of the characteristics of the selected interview partners for our sample. Following the principles of the theoretical sampling [25], the sample size was not predefined, but was increased until an adequate level of data saturation was reached. Consequently, the selected sampling criteria do not ensure representativity [20]. However, to take the variation and diversity in the field into account, the researchers have also selected cases that differ regarding the level of education, the degree of digitization, the age and the country of origin. Most participants were acquired by giving a short introduction and handing out lists before a voluntary language class. Partly, interviewees could refer to other asylum seekers who were willing to do interviews.

3.2 Data Collection

In general, most interviews lasted an hour and were conducted in German refugee accommodations in January and February of 2019. A few interviews were slightly shorter and lasted only 10-30 minutes. All interviews were recorded and transcribed for the analysis. To safeguard the privacy rights of interviewees, personal data has been formally anonymized during the transcription. The interview languages were mainly German and English depending on the language in which the interviewee felt more comfortable. Further, one interview was conducted in Amharic by a translator. The interview guideline comprised questions regarding the refugees' general user behavior, their understanding of privacy, the relevance and any occurred breaches of privacy during the flight

situation as well as individual strategies to protect personal information. A translation of the interview guideline can be found in the Appendix B.

The interviewer was a German female who had six years of experience of charitable work with asylum seekers and had been trained by a local Caritas organization in conversational techniques with refugees in this context. Through pre- and post-talks as well as consciously avoiding a frontal interview situation, we aimed to ensure that the interviewees were given enough space to reconstruct their flight experiences without putting them in a situation of stress and creating uncertainty. To this end, the level of detail with which the respondent was prepared to answer a question was also respected. As a consequence, P5 only gave brief answers and did not provide detailed information. During the pre-talks, the questions were shown to the interviewees in advance and the interviewer explained the main topics. Fear of consequences for the asylum procedure was not a major issue, since the independence from administrative institutions was highlighted beforehand. In situations when the focus of the conversation drifted too much towards negative experiences of their flight history, the interviewer tried to refocus on what had been achieved during the flight. Through all these measures any potentially re-traumatizing levels of conversation could be avoided. The authors received approval of the ethics board of the TU Darmstadt.

3.3 Data Analysis

Aiming for an exploratory approach and to make use of the variety of contents within the data material, qualitative content analysis according to Gläser and Laudel [26] was chosen to analyze the obtained data. Thus, we developed a category system in an interrelationship between theory and the collected data [26]. The list of characteristics has been complemented in the process of extraction to ensure that all features were included, even if they did not fit well into the given search grid [26]. The final superordinate categories were *possession of smartphone*, *use case*, *function*, *challenge*, *privacy - concerns*, *privacy - understanding*, *privacy - relevance*, *privacy - behavior because of concerns*. The complete categorical system can be found in the Appendix A. To ease the process of analysis the software *RQDA* (Version 0.2-8) [34] was used.

4 RESULTS

In the following part, we will present the results of our study. First, we will give an overview of the most general findings in Section 4.1. Section 4.2 outlines the prior understanding the respondents had of digital privacy. Subsequently, Section 4.3 describes to what extent privacy is relevant for asylum seekers during their flight. Lastly, in Section 4.4 strategies are described that are used by asylum seekers to protect their digital privacy. In order to protect their identity and avert negative consequences, we will refrain from precisely attributing some of the quotes in the course of the analysis.

4.1 General Findings

In a nutshell, the majority of the participants (P) of our study, 11 out of 14, possessed a smartphone either temporarily or throughout their flight. None of the respondents escaped without the access to a cell phone which includes simple feature phones and also, access through other members within a group. It is striking that smartphones were often used collectively within groups that formed spontaneously during the flight. This means that even people who did not own smartphones had the benefit from useful features like map and GPS applications. Further, costs for prepaid cards or new SIM cards could be shared and batteries could be saved (P11; P14; P2).

In general, it can be summarized that certain smartphone apps were more relevant to the interviewees than others. In the following, this prioritization will be further evaluated. Table 2 illustrates the prioritization of the applications by the asylum seekers. It can be noted that online

Table 2. Prioritization of Smartphone Applications. The relevance was assessed by the interviewer and based on the frequency of mentions by interviewees. Representativeness is not ensured due to small sample size.

Application	Prioritization
On/-Offline maps	very relevant
Calls	relevant
Apps with chat-feature and SMS	relevant
Websites	barely relevant
Camera	barely relevant
Music (apps)	barely relevant
Social media	barely relevant
Apps for refugees (e.g., MigApp)	not relevant

maps were the most frequently used application during the flight. One respondent stated that they had also used an offline map in case of lacking internet access (P6). Generally, the use of mapping applications was strongly related to the autonomy of the asylum seekers. But even though it has been possible for many interviewees to use GPS applications and collective networks to carry out partial sections of the escape route independently of smugglers, this autonomy could not be maintained throughout the route. All interviewees had to rely at least temporarily on the "services" of smugglers in order to cross a certain border undetected. Complete independence from smugglers has not been possible even with the help of smartphones (P6). For interviewees who moved relatively autonomously and largely without smugglers, the search for information was far more relevant. One participant, who fled from a third country during a stay abroad, used ordinary booking and car rental websites. Overall, it can be assumed that the autonomy from the services of the smugglers is causing a stronger dependence on smartphones:

> "*Because all I have done with this smartphone. Without the smartphone most probably, that would be not possible to get out from the country.*"

After using GPS for orientation, calls were the second most frequently mentioned use case, primarily for the asylum seekers to inform friends and relatives about their own well-being and to contact smugglers. Apps with chat functions and sending SMS messages have also been relevant for communication. *WhatsApp* and *Facebook Messenger* were most frequently mentioned here. More rarely also *Telegram* and normal SMS have been used. *Viber*, *Imo* and *Signal* could be classified as barely relevant. However, since the use of apps depends strongly on the respondents' country of origin, no general statements should be made here. Only a few of our participants utilized internet sites and social networks during the flight, these were rather relevant, if at all, before the flight for planning purposes.

4.2 Preconceptions of the Asylum Seekers about Digital Privacy

The four interviewees who fled from Afghanistan had seemingly a very low understanding of the importance of digital privacy. Partly, this might have been due to difficulties to explain the term 'privacy' during the interviews because the specific term for it in Dari, Pashtu or Urdu could not be determined. But all of them have fled from rural areas and had not owned a smartphone in Afghanistan which could also indicate a lack of digital literacy. Because they did not flee from government-related actors, but from the violence of domestic terrorism, and thus, from non-state actors, there was no specific danger to them to be monitored and detained by the Afghan secret service. It can be assumed that they previously had had a low technical understanding and have

learned on the flight that it was better to turn off their smartphones or cell phones, to hide from the (border) police. The same applies to the interviewees from Ghana and Ethiopia, who left their countries for socioeconomic reasons. There seemed to be no particular risk of digital surveillance by the government. Therefore, they had rarely dealt with the issue of privacy before. Furthermore, one of them stated he had been largely unfamiliar with digital technology and described the learning process he went through during the flight:

> "*[...] When I was in Italy, I learned small about technology. [...] Even if you go to Facebook how do you know that you can share this with your friends [...]. Everywhere you go, they want to keep your information for something else.*"

There had been a key experience, when the police presumably observed him and surveilled his mobile phone activities in the context of investigations. Since that experience he developed a critical understanding of technology and uses different strategies to protect his digital privacy.

Two participants who fled from persecution understood the possibilities of digital surveillance by the government and recognized that they may have been affected by governmental surveillance before fleeing. As a result, they developed some strategies to protect personal information and communicated in a selective way before escaping their countries. The reason for their awareness was probably the fact that they grew up under regimes with authoritarian tendencies. But even though they intuitively perceived the risks of privacy, they relied mainly on the opinions of others and thus did not have a profound preconception.

For some of the Turkish and Syrian interviewees who fled from their country of origin because of political persecution, it is noticeable that all of them have a very profound and detailed understanding of the term "digital privacy". For example, some interviewees fled from government agencies and as a result, their passports were confiscated and they were prosecuted by the police and intelligence agencies, both in their countries of origin and in transit countries. According to one interviewee, the persecutors were able to track people even in foreign countries. Similar concerns were reported by two interviewees, who stated to have actively criticized the policy of their government and operated in an environment in which they were repeatedly confronted with the consequences of digital surveillance. They reported to have seen and heard, either through media reports or within their social network, that people were arrested and killed because of their political activities on the internet.

The interviewees mentioned different types of information that have been considered as sensitive and confidential during their flight. These included political positions, such as criticism of the government's policy, proximity to certain political movements, religious denominations, affiliation with rebel groups and the rejection of radical Islamic ideologies. Furthermore, they mention information on family members and friends and information that might identify them as "illegal immigrants" or that would link them to smugglers.

In summary, it can be said that people, who had already developed a more profound understanding of the meaning of 'digital privacy' beforehand, had often been confronted with the negative consequences of state surveillance and repression in their countries of origin.

4.3 The Relevance of Digital Privacy during the Flight

It can be stated that the protection of their own digital privacy was of importance for people fleeing from their countries for various reasons. Based on open coding of all material, five categories have been identified, which are described below:

4.3.1 Governmental Persecution in Country of Origin. The protection of digital privacy has been identified as most relevant to people who were subjected to a specific political persecution in their country of origin. This applies to interviewees from countries with authoritarian tendencies,

who were afraid of being monitored and detained by police and intelligence agencies. The fear of intelligence surveillance occurred mainly on a digital scale online, while police and soldiers tend to execute a physical form of surveillance, by seizing and searching smartphones.

Interviewees mentioned some apps that they have suspected of being monitored. This included listening to their conversations, monitoring their *WhatsApp* messages or other internet activities on the smartphone and identification by hearing their voice. Some respondents suspected that the governments of their country of origin monitor and kill people because of what they posted on social media or within private networks. Therefore, their privacy concerns are based on the fear of becoming a target of the government as well. This is described by a participant:

> *"A lot has happened. A brother has a girlfriend in [a city] [...]. Our brother has been arrested and killed by beating. His brother in [a city] is alive and the intelligence has arrested his brother."*

Many respondents reported an increasing political pressure in their country of origin: *"I have [a Facebook] account. But since 2015 I did not login."*. Only in the process of developing their plans to escape their countries, privacy became a personally relevant topic. It is striking that in cases of specific governmental prosecution, the relevance of digital privacy of the respondents was directly linked to their personal safety, as stated by an interviewee: *"It is a dead and life case actually."* He became aware of being in danger due to the following key event:

> "*There was some experience. [...] One of our friends [...] was [an employee of a public institution] [...]. And his phone has been monitored. [...] Then he was captured by the intelligence and now he is in prison. So, after this I knew. And I shut down everything.*"

Another participant comes to a similar assessment of the situation:

> "*I think I was in a dangerous situation. In such a situation, I had to use a special application to ensure my safety. That was the point. For safety I would say.*"

4.3.2 Governmental Persecution – Extended to Family Members. In some of the interviews, it could be observed that this fear of state surveillance continued as the asylum seekers had reached countries with rule of law structures. The reason for this was the concern for their family members. Some refugees feared that their family members' communication could be monitored by the government and that their political statements could bring their family members into trouble:

> "*When I speak with German or Arab people or write or something, I just write without being afraid. But if I send something to my home, to my mother, I do not speak against [the leader of the country of origin].*"

Thus, their own privacy and security is directly related to that of their family members: "*So, this to me is privacy. My life privacy. My family privacy. I have to protect them*". Moreover, one participant described that the protection against physical access to smartphones is of great relevance, as police officers and soldiers can access personal information about their family members.

4.3.3 Persecution by Non-State Actors. A further threat identified has been the persecution by non-state actors, as the IS or Taliban. This form of monitoring occurred only on a physical level. Different respondents from Syria state that cell phones and smartphones were confiscated and searched by members of non-state groups. For example, one reported on how his smartphone was searched by followers of the IS when they did not have an ID card to identify themselves:

> *"Previously [name], me and my cousin were riding a motorcycle and the IS arrested us. 'Where are your IDs?' 'Unfortunately at home.' They checked our cell phones."*

4.3.4 Privacy Related Cooperation with People Smugglers. Being discovered by law enforcement agencies posed a risk not only to the asylum seekers, but also to the smugglers. Due to the shared

risks, asylum seekers and smugglers pursued similar interests. Many interviewees said that they were told by the smugglers to sell their cell phone or to leave the device switched off (P1; P4; P9). Privacy concerns, interests and fears of the smugglers were thus transferred to the refugees and partly addressed by them:

> "*Because the smugglers are scared to be detected by police. So, they may tell the people they are helping to cross the border to turn off their smartphone.*" (P6)

This aspect will be further discussed in the following section. Because of the shared danger, a kind of alliance arose during the flight, which one of the interviewees describes as follows:

> *"[...] I always had the number of a smuggler who called me to find out where we were. And he always said that if we are in Germany [...]. They [the smugglers] cannot be caught. [...] They helped us, why should we tell the police: 'Hey, they are smugglers.' [...] And the smuggler says to you: 'If you don't delete the number, then you have a big problem."* (P13)

This is related to the prevention of border crossing in general. Without privacy, respondents cannot carry out their flight plan and cross the border without being detected by police (P2; P4; P9; P11). One Turkish participant describes this risk as follows:

> "*I had a plan for coming to Germany. I had to manage everything. Everything should be in the secure mode. So, if somebody else could know my plan. So, my plan could not be achieved.*"

Another mentioned privacy related threat in the context of smugglers, was the extortion of family members. Two interviewees were afraid that smugglers could try to find out the phone numbers of their relatives, and then blackmail them with money demands (P2; P8).

4.3.5 Negative Consequences for Residence Status in the Country of Destination or on Re-entry Country of Origin / Transit Country. The fear of negative consequences for the asylum seekers' residence status in the country of destination has been rarely expressed. This can be attributed to the fact that the inclusion of smartphones in the asylum procedure represents a new development, and the interviewees were therefore not yet confronted with this issue. In addition, it might be assumed that these concerns were overshadowed by more relevant threats, such as persecution by their countries of origin and the difficult and sometimes life-threatening flight conditions themselves. An interviewee from Syria feared that he might be denied re-entering into Lebanon if he criticizes their government policy on his smartphone. Moreover, one of the interviewees has feared negative consequences on his residence rights as well, since he is staying in Germany without a residence status. The interviews revealed that asylum seekers found themselves in the dilemma of having to deal with smugglers in order to reach their country of destination (P6). On the other hand, however, they had to fear that they would be regarded by the police themselves as human traffickers and thus as part of a criminal network. They feared that the police could uncover this connection to smuggling networks by using the data and numbers stored in their phones (P2; P3; P11).

The interviews also showed that the understanding of digital privacy for respondents changed depending on the context they found themselves in. Many respondents stated that protecting their privacy was more relevant in their countries of origin and during their flight than in Germany. This was mainly due to the perception of a lack of rule of law in their home countries and challenges during transit procedures. They seemed to be less concerned about a reasoned release of their data based on the rule of law:

> "*If there is freedom, then you do everything. I learned that way. When I was at job center. Send my data, age, CV to another company. I did not care.*" (P9)

Some interviewees justified this new openness concerning the disclosure of personal information because of the fundamental right of free expression in Germany (P6; P11; P12). Information that

was previously considered as sensitive and confidential was no longer associated with the concept of privacy in Germany:

> "*Now I have an opinion. I can say everything. I can say 'Oh, Germany, a little bit treated with me not good.' I can say.*" (P9)

Nevertheless, it is quite important not to make a generalizing statement here. There is no simple link between an increase in the rule of law and a decrease in the relevance of privacy. P7 from Turkey made an ambivalent statement here. On the one hand, he was stressed out since he did not possess any private information as long as people could use this information against him. On the other hand, he remained skeptical and pointed out that one cannot really be sure of this in any context:

> "*You can know everything about me. It's not [opaque] to me. But unless someone is mis-use it. And I can't make sure either people do misuse it or not. Nobody can know this.*"

For the release of personal information, therefore, a secure basis of trust and a limitation of the released data is required. To protect himself from the secret service, one participant revealed his location data towards a friend, so that he is informed in case of being kidnapped back to his country of origin: "*There was one application. It's like, wherever you are in this app, your friend, they can see where you are [...] and what I'm doing*".

For P6 from Turkey, privacy is relevant in every context and is considered as a human right:

> "*I can say that privacy is necessary for everyone. Even for such kind of people like me or for you or for somebody else [...] That does not mean we are doing some illegal things. [...] Its normal privacy need. Because we are human beings.*"

He further made a statement against the assumption that people who take their digital privacy seriously often tend to be criminals.

4.4 Strategies of the Asylum Seekers to Protect their Digital Privacy

Some respondents have developed strategies to protect their personal privacy during the flight. This applies especially to people who have already been exposed to pressure from state or non-state persecution in their countries of origin. The strategies seemed to serve different purposes, such as preventing a personal identification and localization or protecting personal information from access by government agencies, police, soldiers or non-state actors. The superior objective was always to ensure their own safety as well as the safety of their family members. This is described by a respondent, who fled from political persecution, as follows:

> "*I think that I was in dangerous situation. In such a situation I had to use a special application for my security. That was the point. For safety I would say.*"

The individual strategies are summarized in figure 3 and presented below. It can be distinguished between strategies that relate to the digital level and strategies that aim to prevent physical access to smartphones:

4.4.1 Strategy 1: Anonymity of the Cell Phone (Number) and Online. Some respondents had decided to purchase an anonymous cell phone number online that cannot be linked with their identity. This is very useful when using *WhatsApp* or *Telegram*, which cannot be used without a phone number (P6; P10). Another strategy with the same objective was to purchase a used smartphone, which could not be associated with their own identity. Then, this has often been used as a second cell phone to contact smugglers (P6; P7; P9). Hotel bookings or the creation of *Facebook* accounts were also carried out using pseudonyms (P6; P7; P10). Another strategy mentioned for anonymity online was the additional activation of a Virtual Private Network (VPN) connection (P4; P6; P7).

4.4.2 Strategy 2: Adaptation of Communication. A further strategy was the adaptation of communication. This includes withholding sensitive information, such as details of the flight plan or the discussion of political issues (P7; P10). This goes hand in hand with a selective form of communication which means not to talk about certain topics (P9; P11), or by using a code language to speak about politically sensitive topics and to express criticism (P1; P9; P13).

4.4.3 Strategy 3: Adaptation of User Behavior. Further strategies can be listed under the category "Adaption of User Behavior". Many respondents said that they preferred certain apps over others, which was reflected in a selective use. It is striking that the mentioned apps and strategies of the interviewees are very different and sometimes even contradictory. For example, some respondents reported to avoid commercial and popular apps, such as *WhatsApp*, or to renounce *Microsoft* apps (P4, P6). They argued that secret services were particularly active in those apps and that *WhatsApp* would be very unsafe and "open". As a consequence some interviewees preferred to use “rather unknown, smaller” apps such as *Signal*, *Viber* and *Skype* or tend to diversify the use of information and communication channels (P4). However, P6 noted that it would be easier to monitor rather unknown and only rarely used apps, whereas the high amount of information exchanged via *WhatsApp* would make filtering and monitoring much more difficult, time-consuming and expensive. *Facebook* and GPS signals were also considered unsafe, whereas entering online banking data was considered as safe (P7; P9).

Also, selective use did not only refer to the apps themselves, but also to the selection of a specific cell phone type and / or manufacturer. For example, P9 from Syria preferred using simple cell phones over smartphones, others chose *Blackberry* and *Nokia* over *Samsung*. The last adaptation of user behavior described was the deletion of personal data, as well as of message histories and call lists on the phone (P2; P4; P8; P9). Alternatively, some interviewees also stated they had transferred their personal information to external data storage media and had been hiding these in their clothing (P8; P13).

4.4.4 Strategy 4: Renouncement. Many interviewees stated that they had temporarily or completely stopped to use their smartphone during the flight and took recourse to non-technical solutions. These include, for example, renunciation of digital communication channels and the preference for face-to-face communication or memorizing one’s escape plan as well as memorizing cell phone numbers to avoid leaving digital traces (P4; P7). In this context, two interviewees mentioned that they threw their smartphones away as soon as they were discovered by the police (P8; P11). One reason for this seemed to be the fear of being associated with criminal networks (P3; P6; P7). Another strategy was to turn off the smartphone or to remove the SIM card (P6; P10). To protect their smartphones from physical access by smugglers or police, many respondents hid them (P2; P9; P11; P14).

However, some of the interviewees questioned the effectiveness of their strategies and assumed that they could protect them only for a limited period. In general, it is remarkable that there is a great deal of perceived uncertainty and that the boundaries between the actual risks of surveillance and speculation are fluid. Some respondents pointed out that effective privacy protection is not possible when using smartphones (P4; P10). P6 from Turkey expressed this as follows:

> "*As I said before there is no 100% privacy. I do not think even for the future, you can get 100% privacy online.*"

In the description of the category 4 "Privacy Related Cooperation with People Smugglers" within the previous section (4.3.4), it was pointed out that some of the mentioned privacy aspects are relevant for the smugglers as well. It is therefore understandable that the strategies for protecting privacy are similar. These include the use of a code language (see strategy 2), the selective use of

Table 3. Identified strategies of asylum seekers to protect their digital privacy. These strategies are characterized by specific protection behaviors that could be identified within the interviews.

(1) Anonymity efforts	(2) Adaption of communication	(3) Adaption of user behavior	(4) Renouncement
• anonymous purchase of a SIM card • anonymous purchase of a smartphone • use of pseudonyms • VPN connection	• minimization of communication • selective communication • code-language	• selective usage • variety of apps • delete data • use of external storage media	• disposal of smartphone or SIM card • hiding the smartphone • use of non-technical solutions (e.g. face-to-face communication)

cell phones (P9), and the disposal of cell phones in case of police controls (P3; P9). In addition, it can be stated that it is in the smugglers' interest to inform refugees about the risks of smartphone use during flight and to make sure they adapt their strategies or do not to carry smartphones with them at all (P1; P3; P4; P8; P9).

5 DISCUSSION

Our study explored the smartphone use of asylum seekers during their journey, especially raising the questions of how relevant the protection of digital privacy is for asylum seekers and to what extent and how this is reflected in their user behaviour. In the following, we will situate our findings in the existing literature and highlight contradictions and confirmations to previous findings. Furthermore, we discuss influences that were not fully uncovered by our study. Further we will reflect on the results from a theoretical perspective of HCI and CSCW and work out design implications based on our findings.

5.1 Reflections on the Results

The general user behavior reported within the interview was mostly in line with previous research. Most asylum seekers interviewed (11 out of 14) owned a smartphone at least temporarily. Respondents without a smartphone stated that they possessed at least a simple mobile phone. This is consistent with the results of Emmer et al. [15]. However, it is noticeable that the possession of smartphones was by no means continuous for all interviewees. During the flight, some of the smartphones were confiscated by smugglers or police officers or phones were disposed to avoid someone checking up on them. The primary use cases, (1) GPS applications and (2) communication with relatives, friends, other asylum seekers or smugglers, are consistent with previous research [13, 15]. Our results showed that online maps were the most frequently used application during the escape. Offline maps were also relevant when internet access was not given. It became clear that relying on map applications contributed significantly to asylum seekers' autonomy. Here, our findings confirm those of Zijlstra and van Liempt [67]. They found that mapping applications increase refugees' mobility, especially when crossing borders. Moreover, they too found that the use of such services reduced dependence on smugglers. Dekker et al. [13], Gillespie et al. [23] and Alencar [6] also emphasize the critical importance of smartphones for, among other things, planning routes and orientation.

Furthermore, Gillespie et al. [23] find that refugees, depending on borders and actors, make a shift in their digital practices, creating the need for "online (in)visibility" to avoid being discovered, apprehended, or deported. This is partly consistent with our findings showing that the threat from border controls can have an impact on the use of smartphones and their applications. In

addition, we found indications that digital privacy practices also depend on origin and reason for fleeing. Thus, our analysis has shown that especially asylum seekers confronted with negative consequences of state surveillance and persecution in their countries of origin developed a comprehensive understanding of the meaning of "digital privacy". Since the threat of being monitored and imprisoned by intelligence agencies because of critical opinions or actions is ubiquitous, the protection of their digital privacy is, as expressed by an interviewee, directly related with their own and families security interest. This result is also consistent with the findings of the International Rescue Committee [36] and the study conducted by Latonero and Kift [41]. While Coles-Kemp and Jensen [11] found that under the precarity of adapting to a new country, for refugees and asylum seekers the primary concern is to leverage the benefits of digital services rather than to control access to data, we found that under severe precarity, where data privacy is directly connected to the imminent danger of imprisonment or potentially even life-threatening consequences, the adaption of user behavior can be drastic and lead to renunciation. Many of our interviewees had a steep learning curve, sometimes triggered by a key event. Still, preconceptions and technological literacy might be a strong factor for empowering asylum seekers to make safely use of ICT.

5.2 Considering Cultural and Contextual Influences

In our sample, the interviewees had a variety of countries of origin. While this might have added to the spectrum of reported user behaviours, the cultural background and contextual factors might have strong influences on the user behaviours. Additionally, the specific ICT functionalities required are likely to be dependent on situational factors, such as the route chosen for the journey. Unfortunately, these factors are not to differentiate reliably, since they tend to co-occur. While we had interviewees fleeing from certain countries for political rather than economical reasons, these factors seemed to coincide with higher education and preconceptions of privacy. Also, cultural factors might be interrelated with these findings, but considering the size of our sample, any generalizations would be speculative. Nevertheless, it should be noted, that user practices might differ in the Global South, as it has been noted by Ahmed et al. [5] especially regarding device sharing. These cultural differences might be an influencing factor for the strategies we found. Researching the interplay of these factors could be a subject for further studies using a representative, quantitative approach.

5.3 Privacy Strategies from an HCI and CSCW Perspective

Considering the identified strategies and the user behaviours, it is notable that these are often in conflict with "typical" functionalities, which are often rather designed for end users from the Global North. This problem is mentioned by Ahmed et al. [5], who find a mismatch between cultural practices from the Global South and the design of cell phones. Due to the very specific circumstances of asylum seekers on their journey, we found this mismatch to be even larger. While modern smartphones often link the device to a user-accounts relating to eco-system of the operating system for the sake of usability, this concept seems to be highly unsuitable for multiple users sharing a device. This is also true for *WhatsApp*, which is linked to only one phone number once it is installed. *WhatsApp* even states that an account might be blocked from the verification process, if one should attempt to switch devices or numbers frequently [64]. Considering that we found that sim cards and hence, phone numbers often are swapped during the journey and considering that devices are shared, the use of the app seems to be rather inconvenient. Moreover, *Facebook* is supposed to be used with real names, prohibiting the use of pseudonyms and fake identities. As a consequence, the account can be locked, needing to be reactivated by providing an explanation of special circumstances [43]. However, considering the vulnerability resulting from for example political persecution, providing an explanation might be inappropriate. Even though these aspects might be complicating the use of these technologies, we found they still are most likely to be used

by asylum seekers anyway, often ignoring the terms of use. This can be seen as a case of *repurposive appropriation* of technology. Salovaara [54] describes repurposive appropritation as the process of users finding new purposes of technology other than the ones intended by the designer. This happens by the user mapping situational features of the context together [54]. Since the situational features of the asylum seekers' journeys are very distinct and differ strongly from the intended (typically western) user context, the privacy strategies we identified can be seen as appropriative acts.

When considering the specific user behavior of asylum seekers, the notion of affordances often is used in research [6, 13, 23]. Roughly speaking, in HCI affordances refer to the the different possibilities for action a technology has to offer to its user [52]. Due to varying contexts and subjective perceptions, the saliency of different affordances may vary for different user groups. Dekker et al. [13] state that ICT affordances give refugees the possibility to develop "smart strategies". The privacy strategies we identified are part of these strategies, as they enable asylum seekers to leverage ICT while protecting private information, and thus, personal safety. When considering the design process, the functional mismatch we noticed can be attributed to the device or software designers' efforts to identify important affordances and to optimize usability or ergonomics for them. Since the intended user group of ICT usually is rather western, and since different affordances might be salient in this context, the optimization of the interaction design for this context might end in incompatibilities for other contexts.

5.4 Implications for Design and Information Strategies

Our findings have several general implications for the design of online platforms and digital tools for asylum seekers. As outlined earlier, the development of apps aiming to help refugees is facing the challenge of being used mostly by volunteers and humanitarian organizations, rather than by the target group itself [60]. Asylum seekers are not everyday consumers but rather a vulnerable population that has specific characteristics and needs that require to be addressed when developing in designing applications [41].

Many of our interviewees reported to have changed their phone multiple times. Also, they reported having limited internet access. Especially asylum seekers fleeing from political persecution were afraid of surveillance and feared their phones and social media accounts to be checked. Hence, we draw the conclusion that online platforms, that can be accessed within a browser from changing devices and that can be wiped from the browsing history, could lead to more acceptance compared to assistance or information apps, that would need to be downloaded to the device. Further, since the interviewees expressed a great need for anonymity and many reported using fake identities on social media, any effective assistance or information tool would need to allow for this level of anonymity. Hence, ideally platforms and services should allow for pseudonyms and not be linked to phone numbers. The assumption, that asylum seekers would rather remain in control of their data, is also consistent with findings reached by Hayes [30], where he found that standardized approaches to data collection by aid organizations are not willingly adopted by refugees and digital data are not happily provided by them due to the fear of surveillance. Shoemaker et al. [56] report privacy concerns of refugees and a lack of transparency within the context of humanitarian aid as well. Consequently, future efforts for digitalization within the context of humanitarian aid should carefully consider this need for digital privacy to support acceptance. Also, it should be considered that sharing devices is a common practice to save battery and data volume during the journey. This should be considered and any log-in based platform would need to make it easy to log-out, so privacy can be maintained also towards the co-users of a device.

Nevertheless, we want to emphasize again, that none of our interviewees stated to have used any assistance apps. Dekker et al. [13] suggests the reason for this might be unawareness about

the existence of these sites and apps. Instead, we found a preference for apps and platforms like *WhatsApp* or *Facebook*, which the interviewees were familiar with. Consequently, offerings for assistance and information might be more visible on already adopted platforms. This could also be a way to address false expectations about their target destinations that Emmer et al. [15] found to be very common among refugees from Iraq and Syria.

Last but not least, in their work about undocumented migrants Guberek et al. [29] point out that there should be an effort to facilitate information hiding on demand and plausible deniability. With respect to our results, showing that, besides digital surveillance, the seizure of smartphones and forced access is a major issue for asylum seekers, we agree with the authors' conclusion. There have been efforts to provide hidden storage volumes for smartphones [32, 58] or an app-based lockdown mode hiding critical information, which can be triggered by a specific unlocking pattern [27]. We would greatly encourage future research endeavours to improve such technologies and to make them more accessible.

5.5 Limitations

While we could provide valuable findings to the research field on on digital privacy perceptions of asylum seekers during flight, our work comes with some limitations due to the sampling method and the qualitative approach.

First, there is a limited representativeness: As mentioned in Section 3.1, we wanted to create a certain representation in the group of male asylum seekers aged 16-35 years within the study. However, this selection does not fully cover the demographic distribution of arriving asylum seekers, which leads to a limitation in the heterogeneity of the results and means that representativeness of the results is limited by case selection. Also, the study was conceptualized for an explorative, hypothesis-generating purpose. Due to the qualitative research approach, sensitive data could be recorded, and the results show a high degree of content detail compared to a quantitative approach. Nevertheless, regarding the limited scope of the interviews the gained insights should not be generalised, because no reliable quantitative conclusions can be drawn from it.

Lastly, we also want to point out limitations resulting from the interview languages. While the interviews were conducted in German and English, there were still comprehension problems, especially concerning the introduction of the term "digital privacy". This problem arose not only due to a lack of conception but also due to the language. While this problem could mostly be addressed by repeated explanations and rephrasing questions, it would have been advantageous to work with a translator in all the interviews for even more precise statements.

6 CONCLUSION

Asylum seekers are increasingly reliant on smartphones and ICT during their flight. Since they must be considered as a vulnerable user group, we conducted interviews with asylum seekers to gain knowledge about their privacy perceptions, their user behavior, the accessibility and the specific use cases during the flight. Generally, we found that the gains in autonomy by using smartphones lead to more independence from the services of people smugglers, and thus contributed to a protection from criminal exploitation. Regarding the digital privacy preconceptions, we found that there was a better understanding and sensibility in interviewees who feared governmental persecution or surveillance in their country of origin in contrast to the refugees that fled from the violence of non-state actors or migrated for socioeconomic reasons. The interviewees rarely expressed concerns that privacy breaches could result in negative consequences in their country of destination, e.g. for the asylum application. Rather they feared that their data could be used for blackmail or persecution, also of their families, or link them to illegal smuggling networks. People smugglers were reported to brief asylum seekers regarding privacy strategies, because it is in their interest to remain unknown

to police and border patrols. We could identify several privacy protection behaviors in our sample that we could ascribe to four classes of protection strategies, primarily aiming at the protection of their identity and location from access by (border) police, smugglers or non-state organizations.

Although the study has methodological limitations (see Section 5.5), the exploratory results give essential impulses for further research on privacy perceptions of asylum seekers during flight. Smartphones are increasingly important for them to strengthen their autonomy from criminal smuggling networks as well as for communication, information and collaboration. Because privacy concerns can be a hindrance for technology adoption and can lead to renouncement or self-restriction, the findings provide useful insights that could benefit the development of privacy-enhancing technologies for asylum seekers or assistance and collaboration platforms in the context of CSCW.

ACKNOWLEDGMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050 (https://gepris.dfg.de/gepris/projekt/251805230?language=en) and by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. We would like to thank Larissa Aldehoff for her valuable advice during the empirical study and the anonymous reviewers for their helpful suggestions.

REFERENCES

[1] Safa'a AbuJarour. 2019. Smartphone App Adoption at Home and on the Move: The Case of Syrians. In *3rd AFU International Conference: Towards Advanced Scientific Knowledge (TASK2019) in Business Sciences*. Al Falah University, Al Garhoud, Dubai.

[2] Safa'a AbuJarour, Haya Ajjan, Jane Fedorowicz, and Antonia Köster. 2021. ICT Support for Refugees and Undocumented Immigrants. *Communications of the Association for Information Systems* 48 (2021), 1–20. https://doi.org/10.17705/1CAIS.04840

[3] Safa'a AbuJarour and Hanna Krasnova. 2017. Understanding the role of ICTs in promoting social inclusion: The case of syrian refugees in Germany. In *Proceedings of the 25th European Conference on Information Systems (ECIS)* (Guimaraes, Portugal). Association for Information Systems, Atlanta, GA, USA, 1792–1806. http://aisel.aisnet.org/ecis2017_rp/115

[4] Safa'a AbuJarour, Hanna Krasnova, Helena Wenninger, Jane Fedorowicz, Sebastian Olbrich, Chee-Wee Tan, Viswanath Venkatesh, and Cathy Urquhart. 2016. No Leveraging Technology for Refugee Integration: How Can We Help?. In *Proceedings of the 37th International Conference on Information Systems (ICIS)* (Dublin). Association for Information Systems, Atlanta, GA, USA, 1–16.

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW, Article 17 (2017), 20 pages. https://doi.org/10.1145/3134652

[6] Amanda Alencar. 2020. Mobile communication and refugees: An analytical review of academic literature. *Sociology Compass* 14, 8, Article e12802 (2020), 13 pages. https://doi.org/10.1111/soc4.12802

[7] Asam Almohamed and Dhaval Vyas. 2016. Designing for the Marginalized: A Step Towards Understanding the Lives of Refugees and Asylum Seekers. In *Companion Proceedings of the 2016 ACM Conference Companion Publication on Designing Interactive Systems* (Brisbane, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 165–168. https://doi.org/10.1145/2908805.2909415

[8] Rocco Bellanova, Maria Gabrielsen Jumpert, and Raphael Gellert. 2016. *Give Us Your Phone and We May Grant You Asylum*. PRIO Blogs. https://blogs.prio.org/2016/10/give-us-your-phone-and-we-may-grant-you-asylum/

[9] G.W. Blarkom, John J. Borking, and J.G. Eddy Olk. 2003. Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents. In *PISA Consortium*. CBP (Dutch Data Protection Authority), The Hague.

[10] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, USA, 129–142. https://www.usenix.org/conference/soups2014/proceedings/presentation/chen

[11] Lizzie Coles-Kemp and Rikke Bjerg Jensen. 2019. Accessing a New Land: Designing for a Social Conceptualisation of Access. In *CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300411

[12] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. 2018. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174158

[13] Rianne Dekker, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk. 2018. Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making. *Social Media + Society* 4, 1 (Jan. 2018), 1–11. https://doi.org/10.1177/2056305118764439

[14] Adrian Edwards. 2015. *UNHCR viewpoint: 'Refugee' or 'migrant' – Which is right?* UNHCR, Geneva, Switzerland. https://www.unhcr.org/news/latest/2016/7/55df0e556/unhcr-viewpoint-refugee-migrant-right.html

[15] Martin Emmer, Carola Richter, and Marlene Kunst. 2016. *Flucht 2.0: Mediennutzung durch Flüchtlinge vor, während und nach der Flucht.* Freie Universität Berlin, Berlin, Germany. https://www.polsoz.fu-berlin.de/kommwiss/arbeitsstellen/internationale_kommunikation/Media/Flucht-2_0.pdf

[16] European Commission. 2020. economic migrant | Migration and Home Affairs. https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/economic-migrant_en

[17] European Statistics Office. 2016. *Record number of over 1.2 million first time asylum seekers registered in 2015.* Technical Report. European Statistics Office. https://ec.europa.eu/eurostat/documents/2995521/7203832/3-04032016-AP-EN.pdf

[18] Achraf Farraj. 2011. Refugees and the Biometric Future: the Impact of Biometrics on Refugees and Asylum Seekers. *Columbia Human Rights Law Review* 42, 3 (2011), 891–942.

[19] Federal Office for Migration and Refugees. 2018. *Safe countries of origin.* Federal Office for Migration and Refugees. https://www.bamf.de/EN/Themen/AsylFluechtlingsschutz/Sonderverfahren/SichereHerkunftsstaaten/sichereherkunftsstaaten-node.html

[20] Uwe Flick. 2014. *The SAGE Handbook of Qualitative Data Analysis.* SAGE Publications Ltd, London. https://doi.org/10.4135/9781446282243

[21] Federal Ministry for Economic Cooperation and Development. 2020. *Flüchtlinge und Asylsuchende.* Federal Ministry for Economic Cooperation and Development. https://www.bmz.de/de/themen/Sonderinitiative-Fluchtursachen-bekaempfen-Fluechtlinge-reintegrieren/hintergrund/definition_fluechtling/index.jsp

[22] Marie Gillespie, Lawrence Ampofo, Margaret Cheesman, Becky Faith, Evgenia Iliadou, Ali Issa, Souad Osseiran, and Dimitris Skleparis. 2016. *Mapping refugee media journeys: Smartphones and social media networks.* The Open University/France Médias Monde. https://doi.org/10.13140/RG.2.2.15633.22888

[23] Marie Gillespie, Souad Osseiran, and Margie Cheesman. 2018. Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances. *Social Media + Society* 4, 1 (2018), 1–12. https://doi.org/10.1177/2056305118764440

[24] Janine di Giovann, Marianne Nari Fisher, Ali Shajrawi, Kinan Madi, Abodi Nova, and Aleksi Tzatzev. 2013. *Lost. Syrian Refugees and the Information Gap.* Internews. https://www.internews.org/sites/default/files/resources/Internews_Lost_SyriaReport_Nov2013_web.pdf

[25] Barney G. Glaser and Anselm L. Strauss. 1969. The Discovery of Grounded Theory: Strategies for Qualitative Research. *The British Journal of Sociology* 20, 2 (1969), 227. https://doi.org/10.2307/588533

[26] Jochen Gläser and Grit Laudel. 2010. *The Expert Interview and Content Analysis.* VS Verlag für Sozialwissenschaften, Wiesbaden, Germany. https://doi.org/10.17169/fqs-6.2.476

[27] Bernhard Gründling. 2020. *App-based (Im) plausible Deniability for Android.* Ph.D. Dissertation. Johannes Kepler University Linz.

[28] GSMA. 2017. *Refugees and Identity: Considerations for mobile-enabled registration and aid delivery.* Technical Report. GSMA Intelligence, London, United Kingdom. https://www.gsma.com/mobilefordevelopment/resources/refugees-and-identity/

[29] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal, QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3173574.3173688

[30] Ben Hayes. 2017. Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data". *International Review of the Red Cross* 99 (2017), 179–209. https://doi.org/10.1017/S1816383117000637

[31] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. 2021. Who Should Get My Private Data in Which Case? Evidence in the Wild. In *Mensch und Computer 2021.* ACM, Ingolstadt.

[32] S. Hong, C. Liu, B. Cheng, B. Ren, and J. Chen. 2017. MobiGemini: sensitive-based data and resource protection framework for mobile device. *China Communications* 14, 7 (2017), 1–11. https://doi.org/10.1109/CC.2017.8010979

[33] Joey Chiao-Yin Hsiao and Tawanna R. Dillahunt. 2018. Technology to Support Immigrant Access to Social Capital and Adaptation to a New Country. In *Proceedings of the ACM on Human-Computer Interaction (CSCW, Vol. 2).* Association for Computing Machinery, New York, NY, USA, Article 70, 21 pages. https://doi.org/10.1145/3274339

[34] Ronggui Huang. 2014. RQDA: R-based qualitative data analysis. http://rqda.r-forge.r-project.org/
[35] International Organization for Migration. 2017. MigApp. https://www.iom.int/migapp
[36] International Rescue Commitee. 2017. Using ICT to Facilitate Access to Information and Accountability to Affected Populations in Urban Areas: A review of the ServiceInfo and Refugee.Info Platforms. https://www.rescue.org/sites/default/files/document/1713/usingicttofacilitateweb.pdf
[37] Rikke Bjerg Jensen, Lizzie Coles-Kemp, and Reem Talhouk. 2020. When the Civic Turn Turns Digital: Designing Safe and Secure Refugee Resettlement. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376245
[38] Dragana Kaurin. 2019. *Data Protection and Digital Agency for Refugees*. Centre of International Governance Innovation, Waterloo, ON, Canada. https://www.cigionline.org/sites/default/files/documents/WRC%20Research%20Paper%20no.12.pdf
[39] Patrick Kingsley. 2015. *People smugglers using Facebook to lure migrants into 'Italy trips'*. The Guardian. https://www.theguardian.com/world/2015/may/08/people-smugglers-using-facebook-to-lure-migrants-into-italy-trips
[40] Chris Köver and Vasilis Tsianos. 2015. *Smartphones sind für Flüchtlinge überlebenswichtig*. WIRED. https://www.wired.de/collection/latest/ohne-smartphones-hatten-fluchtlinge-kaum-eine-chance-sagt-der-migrationsforscher
[41] Mark Latonero and Paula Kift. 2018. On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control. *Social Media + Society* 4, 1 (Jan. 2018), 1–11. https://doi.org/10.1177/2056305118764432
[42] Mark Latonero, Danielle Poole, and Jos Berens. 2017. *Refugee Connectivity: A Survey of Mobile Phones, Mental Health, and Privacy at a Syrian Refugee Camp in Greece*. Harvard Humanitarian Initiative, Cambridge, MA, USA. http://hhi.harvard.edu/publications/refugee-connectivity-survey-mobile-phones-mental-health-and-privacy-syrian-refugee-camp
[43] Dave Lee. 2015. *Facebook amends 'real name' policy after protests*. BBC News. https://www.bbc.com/news/technology-35109045
[44] Jessica Lingel, Mor Naaman, and Danah M. Boyd. 2014. City, Self, Network: Transnational Migrants and Online Identity Work. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 1502–1510. https://doi.org/10.1145/2531602.2531693
[45] Sebastian Linsner, Franz Kuntke, Enno Steinbrink, Jonas Franken, and Christian Reuter. 2021. The Role of Privacy in Digitalization – Analysing the German Farmers' Perspective. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2021, 3 (2021), 334–350. https://www.petsymposium.org/2021/files/papers/issue3/popets-2021-0050.pdf
[46] Jingjing Liu, Alexander Boden, David William Randall, and Volker Wulf. 2014. Enriching the Distressing Reality: Social Media Use by Chinese Migrant Workers. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 710–721. https://doi.org/10.1145/2531602.2531632
[47] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375174
[48] Ministry of Security and Justice. 2016. *2016 ANNUAL REPORT Migration and Asylum in the Netherlands*. Technical Report. Ministry of Security and Justice.
[49] Bryce Clayton Newell, Ricardo Gomez, and Verónica E. Guajardo. 2016. Information seeking, technology use, and vulnerability among migrants at the United States–Mexico border. *The Information Society* 32, 3 (2016), 176–191. https://doi.org/10.1080/01972243.2016.1153013
[50] David Pannocchia, Petra Saskia Bayerl, and Karen Latricia Hough. 2020. The digital mediation of migration: A qualitative thematic synthesis. In *Proceedings of the 13 th IADIS International Conference Information Systems 2020*. IADIS Press, Sofia, Bulgaria, 145–150. https://doi.org/10.33965/is2020_202006c018
[51] Ashwed Patil. 2019. The Role of ICTs in Refugee Lives. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development* (Ahmedabad, India) *(ICTD '19)*. Association for Computing Machinery, New York, NY, USA, Article 48, 6 pages. https://doi.org/10.1145/3287098.3287144
[52] Giulia Pozzi, Federico Pigni, and Claudio Vitari. 2014. Affordance theory in the IS discipline: A review and synthesis of the literature. In *AMCIS 2014 Proceedings*. Association for Information Systems, Savannah, United States, 1–12. https://halshs.archives-ouvertes.fr/halshs-01923663/file/Pozzi%202014AMCIS%20Affordance_aisel.pdf
[53] Markus Rohde, Konstantin Aal, Kaoru Misaki, Dave Randall, Anne Weibert, and Volker Wulf. 2016. Out of Syria: Mobile Media in Use at the Time of Civil War. *International Journal of Human-Computer Interaction* 32, 7 (July 2016), 515–531. https://doi.org/10.1080/10447318.2016.1177300
[54] Antti Salovaara. 2012. *Repurposive appropriation and creative technology use in human–computer interaction*. Ph.D. Dissertation. University of Helsinki, Helsinki, Finland. http://hdl.handle.net/10138/37289

[55] Marina Sharpe. 2018. Mixed Up: International Law and the Meaning(s) of "Mixed Migration". *Refugee Survey Quarterly* 37, 1 (01 2018), 116–138. https://doi.org/10.1093/rsq/hdx021

[56] Emrys Shoemaker, Gudrun Svava Kristinsdottir, Tanuj Ahuja, Dina Baslan, Bryan Pon, Paul Currion, Pius Gumisizira, and Nicola Dell. 2019. Identity at the Margins: Examining Refugee Experiences with Digital Identity Systems in Lebanon, Jordan, and Uganda. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies* (Accra, Ghana) *(COMPASS '19)*. Association for Computing Machinery, New York, NY, USA, 206–217. https://doi.org/10.1145/3314344.3332486

[57] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. Institute of Electrical and Electronics Engineers Inc., Danvers, MA, USA, 409–423. https://doi.org/10.1109/SP.2018.00023

[58] Adam Skillen and Mohammad Mannan. 2013. Mobiflage: Deniable storage encryptionfor mobile devices. *IEEE Transactions on Dependable and Secure Computing* 11, 3 (2013), 224–237.

[59] Reem Talhouk, Konstantin Aal, Anne Weibert, Max Krüger, Volker Wulf, Karen Fisher, Franziska Tachtler, Suleman Shahid, Syed Ishtiaque Ahmed, and Anna Maria Bustamante Duarte. 2019. Refugees & HCI SiG: Situating HCI within humanitarian research. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, United Kingdom) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3290607.3311754

[60] Reem Talhouk, Ana Bustamante, Konstantin Aal, Anne Weibert, Koula Charitonos, and Vasilis Vlachokyriakos. 2018. HCI and Refugees: Experiences and Reflections. *Interactions* 25, 4 (June 2018), 46–51. https://doi.org/10.1145/3215846

[61] Maria Ullrich. 2017. Media Use During Escape: A Contribution to Refugees' Collective Agency. *spheres Journal for Digital Cultures* 4 (2017), 1–11.

[62] Melissa Wall, Madeline Otis Campbell, and Dana Janbek. 2017. Syrian refugees and information precarity. *New Media & Society* 19, 2 (2017), 240–254. https://doi.org/10.1177/1461444815591967

[63] Alan F. Westin. 1967. *Privacy and Freedom.* Athenum, New York, NY, USA.

[64] WhatsApp LLC. 2021. *Using one WhatsApp account on multiple phones, or with multiple phone numbers.* WhatsApp LLC. https://faq.whatsapp.com/general/verification/using-one-whatsapp-account-on-multiple-phones-or-with-multiple-phone-numbers/?lang=en

[65] Susan Wyche, Sarita Schoenebeck, and Andrea Forte. 2013. 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 (CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 33–44. https://doi.org/10.1145/2441776.2441783

[66] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1676–1690. https://doi.org/10.1145/2818048.2820073

[67] Judith Zijlstra and Ilse van Liempt. 2017. Smart (phone) travelling: Understanding the use and impact of mobile technology on irregular migration journeys. *International Journal of Migration and Border Studies* 3 (2017), 174–191. https://doi.org/10.1504/ijmbs.2017.083245

A CATEGORIES FOR QUALITATIVE CONTENT ANALYSIS

Table 4. Categorical system for content classification. "Category" describes the general content category, "Differentiation" specifies the contents regarding the respective category. The column "Evidence" provides examples for manifestations that implied an assignment to a (sub)category

Category	Differentiation	Evidence
Possession smartphone	– Yes / no – Temporary	
Use case	– Chat – Platform – Voice/video call – Voice message – On-/offline maps – Website	
Function	– Communication	Warnings, information procurement, contact of family members, emotional support, emergency calls at sea
	– Information	Topicality, orientation, self-organization, decision-making, safety
	– Networking	Information exchange, solidarity, self-organization
Challenge	– Information precarity	Misinformation, safety, standard of living in target country, prospect of staying, offers of smugglers
	– Traffickers, smugglers recruitment	
	– Infrastructure	Costs, network coverage, access to internet, energy, battery charging, sim cards
Privacy - concerns	– Origin country: stately prosecution	Repression, surveillance, torture, incarceration
	– Extortion by traffickers	
	– Prevention of border crossings	Push back, repatriation, expulsion, detention, internment
	– Country of destination: negative consequences for legal status	Repatriation, expulsion, asylum procedure
Privacy - understanding	– Access control, protection of private data from access by 3rd parties	Physically (theft by smugglers, safety checks), digitally (stately persecution, surveillance)
	– Personal information	Physical, social, financial or behavioral data, e.g. country of origin, name, age, phone number, date of birth, location, contact data, family, list of calls, message history
	– Safety	Depotism or persection from country of origin or transit countries, unresolved legal status in target country, extended safety of family members
	– Localisation	
	– Identification, anonymity	
Privacy - relevance	– Very important / not important at all (rated in categories from 1-4)	
Privacy - behavior because of concerns	– Renouncement	Deliberate renunciation of smartphone, turn off smartphone, renunciation of certain applications
	– Selective Use	Abandonment of specific applications, use of alternative applications because of concerns
	– Prevent identification	Use of pseudonyms and avatars in social media
	– Prevent localisation	Physical dimension (lights), digital dimension, turn off smartphone, turn off GPS, VPN

B INTERVIEW GUIDELINES

- Introduction
- Note: Anonymization of data, independence, assurance that the information will have no effect on the asylum procedure in any way
- Statement of agreement
- Questions:
  - *Did you use a smartphone during the flight? For what? For what did it help you? Were there any difficulties during the flight to use a smartphone?*
  - *What does privacy mean for you? How important is privacy for you? What would violate your privacy personally?*
  - *Consistent explanation of the term privacy in everyday language, use of synonyms like data security and information protection, refer to access control and utilization of data, if necessary translation of term to first language*
  - *Was privacy relevant during the flight? Do you think about it, when you share personal information in apps on your smartphone?*
  - *Did you share data that you would rather have kept to yourself? What risk to you see in sharing personal data?*
  - *Did you have concerns to be subjected to surveillance or to be discovered? Who by and why?*
  - *Was your smartphone ever confiscated or your account checked?*
  - *What would have to happen so that your right to privacy is better protected? What would have to be improved in smartphone apps?*
  - *Is there anything else you want to say?*
  - *What did friends and acquaintances experience who were in a similar situation? Do you know further refugees that would agree to give an interview?*
- Ask again when aspects remained unclear or language problems occurred
- As the circumstances require adaption of the interview guidelines after the first interviews
- Transparency: Provision of the finished work

Received October 2020 ; revised April 2021 ; accepted July 2021