UNHCR
The UN Refugee Agency

UNHCR
Innovation
Service

Connecting With Confidence

Managing Digital Risks to Refugee Connectivity

Generously supported by:

LUXEMBOURG AID & DEVELOPMENT

Contents

Executive Summary

Connectivity initiatives, which entail the provision of internet and mobile access, can positively impact the lives of crisis-affected people, especially refugees, who require timely access to critical information, communication channels with family members and close associates, and livelihood opportunities during displacement. The **COVID-19 crisis** has further demonstrated the **value of connectivity access** for those seeking critical—and in some cases life-preserving—information, as well as for remote registration and refugee status determination due to physical distancing requirements.

This research explores how to deliver '**connectivity as aid**' in a dignified way while managing digital risks to refugees. It draws from an extensive literature review and on-the-ground fieldwork in displacement contexts in Uganda and Kenya.

The report, which is targeted at humanitarian organizations interested in providing connectivity as aid as well as public and private sector actors involved in connectivity provision to refugees, identifies a number of **digital risks**—from online censorship to cyber threats, data protection risks, disinformation and privacy harms—which demand increased attention and action as connectivity as aid is mainstreamed as an essential form of humanitarian assistance.

Among the **research findings** were that while connected refugees recognize the importance of security and privacy online, they often feel powerless to do much about online threats and digital risks. Despite this, they still highly value digital connectivity and expect UNHCR to protect their data.

The **impacts** of digital risks on connected refugees vary significantly depending on age, gender and other characteristics. Policy environments around telecommunications access (e.g. SIM registration) may introduce risks to vulnerable users. Refugees are regularly the targets of online fraud and scams involving social media and mobile money. It was also discovered that serious protection incidents in the physical world are increasingly likely to have a digital dimension to them.

Community connectivity centers could make important gains by shoring up local security practices and providing better information on digital risks to the broader community. While the threat models of certain users are relatively sophisticated, there is value in providing additional information about the range of existing online threats. Certain community members are eager to support humanitarian organizations in minimizing digital risk and can play a key role in building the knowledge and skills of their peers.

The report calls on **humanitarian organizations** to:

1. Work with community organizations to develop tailored digital risk awareness and training campaigns based on the local context;
2. Empower early adopters in displacement contexts to support digital risk management;
3. Sponsor information security knowledge exchanges;
4. Better police fraudulent activity targeting persons of concern;
5. Partner with the third and private sectors for increased effectiveness and scale;
6. Engage with government authorities and local security officials on threats facing refugees;
7. Advocate for the inclusion of refugee digital protection into national strategies on trust and security, and;
8. Sponsor further research on relevant topics.

The **private sector** is encouraged to:

1. Engage more closely with community organizations on digital risk identification and mitigation;
2. Build better security into humanitarian technology offerings;
3. Consider extending digital security initiatives to include a refugee focus, and;
4. Amplify humanitarian efforts to shape the digital policy environment.

The report also includes recommendations for future research in this space, building on a number of key insights from the research.

Acknowledgements

A fan cools down the power cabinet at the Community Technology Empowerment Network centre at Rhino Camp Settlement, northern Uganda. © UNHCR/ Michele Sibiloni

The author, Dr. Aaron Martin, is incredibly grateful to the UNHCR Innovation Service for supporting this research. He would like to thank Tina Bouffet both for her authorship of section 2 and for reviewing the full report. Katherine Harris and the GSMA Mobile for Humanitarian Innovation team (Jenny Casswell, Ken Okong'o et al.) also graciously provided peer review. He also would like to thank Damjan Nikolovski, Glenn Ong'uti and the UNHCR teams in Kampala, Arua, Yumbe and Nairobi for facilitating the fieldwork in Uganda and Kenya. Finally, the UNHCR Innovation Service would like to acknowledge the ICRC Data Protection team for their ongoing collaboration and partnership on these critical issues.

Introduction

UNHCR, the UN Refugee Agency, is dedicated to saving lives and protecting the rights of refugees, forcibly displaced communities and stateless people.[1] To this end, the UNHCR Innovation Service—the Refugee Agency's in-house innovation hub—runs a program that aims to enhance the digital inclusion of refugees, break down access barriers and facilitate their participation in humanitarian responses.[2] This program also includes research on how the provision of connectivity as aid intersects with matters of refugee protection. The following report identifies a number of digital risks—from online censorship to cyber threats, data protection risks, disinformation and privacy harms—which demand increased attention and action as 'connectivity as aid' is mainstreamed as an essential form of humanitarian assistance.

Since the start of our research process in 2019, the COVID-19 crisis has further spotlighted the value of connectivity to our societies and economies. The digital risks emerging from humanitarian connectivity interventions have taken on a different complexion during the pandemic, and the potential consequences of these risks are increasingly evident. In June 2020, the UN Secretary General launched the Roadmap for Digital Cooperation, which includes among its eight key action areas "the promotion of trust and security in the digital environment."[3] In this vein, the UNHCR Innovation Service is strongly committed to working with a wide array of stakeholders and partners to address digital risks to refugee connectivity.

While a number of civil society groups and digital rights organizations have raised awareness of digital risks across different settings, their meaning within specific contexts of connectivity use by refugees has not been a central focus, nor have the perspectives and experiences of refugees themselves been a prominent focus. Where research on refugee connectivity has been undertaken, it largely focuses on a limited number of displacement contexts in Europe and North America, leaving a considerable gap in our understanding of connectivity use in other parts of the world where sizeable numbers of refugees reside.

1 While acknowledging the important differences across persons of concern to UNHCR, this report will use the term 'refugee' as a shorthand.
2 For more information on the Digital Access, Inclusion and Participation Program, see: https://www.unhcr.org/innovation/digital-inclusion/
3 Secretary General's Roadmap for Digital Cooperation: https://www.un.org/en/content/digital-cooperation-roadmap/

The current research aims to begin to fill this gap by exploring how to deliver connectivity as aid in a dignified way while managing digital risks to refugees. It draws from an extensive literature review and on-the-ground fieldwork in displacement contexts in Uganda and Kenya. This fieldwork included key informant and focus group interviews with refugees in urban and settlement contexts, observations of connectivity in use, and practical engagement in designing connectivity tools with risk-mitigating measures.

The report is structured as follows: Section 1 situates the research, providing background on connectivity as aid and digital risks, enumerating the project's objectives and motivating questions, and defining key terms and concepts. Section 2 packages a review of the existing evidence on refugee connectivity and attendant challenges. Section 3 presents the perspectives of users of connectivity in displacement contexts based on fieldwork and interviews in Uganda and Kenya, concluding with 14 key findings across four categories. Section 4 completes the report with recommendations to the humanitarian and private sectors on how to better mitigate digital risks around refugee connectivity. It also issues recommendations to the research community regarding future possible fieldwork in this space.

This report is targeted at humanitarian organizations interested in providing connectivity as aid but for whom discussions on digital risk are still novel. The report also targets public and private sector actors involved in connectivity provision to refugees. These actors may want to better understand their roles and responsibilities with respect to digital risk management in displacement contexts. We also appreciate that this research represents an initial foray into the subject matter and that it will undoubtedly raise more questions for different stakeholders that warrant further study. To that end, the research community will appreciate our suggestions for a future research agenda in the report's final section.

Motivations

In the face of crises that are increasing in number, duration and complexity, humanitarian organizations continue to make important strides in supporting affected communities through the provision of different forms of technology. These innovations include applications of new techniques and technologies for clean water and sanitation, non-polluting lighting, heating and cooking methods, off-grid electricity generation, agriculture, healthcare and shelter to help those in need.

Connectivity initiatives, which entail the provision of Internet and mobile access, can also positively impact the lives of crisis-affected people, especially refugees, who require timely access to critical information, communication channels with family members and close associates, and livelihood opportunities during displacement. The COVID-19 crisis has further demonstrated the value of connectivity access for those seeking critical - and in some cases life-preserving - information, as well as for remote registration and refugee status determination (RSD) due to physical distancing requirements. Connectivity is also increasingly key to humanitarian protection and accountability as it allows aid agencies to communicate, listen and interact more effectively with those in need.

Until recently, decision makers had largely focused on enabling humanitarian organizations with connectivity in the field (i.e. 'connectivity for aid')[4], paying less attention to the extension of modes of connectivity to those affected by crisis as a form of aid in itself. However, this is changing fast as the humanitarian sector comes to appreciate the transformative potential of connectivity for crisis-affected people. This notion of 'connectivity as aid' has emerged in recent years: as Marchant observes, "the Connectivity for Refugees initiative at UNHCR, started in 2016, was designed with precisely this objective, as was (the Emergency Telecommunications Cluster) project known as Services for Communities that prioritizes providing technology solutions, including network connectivity for communities experiencing conflict."[5]

4 ICRC (2020). Handbook on Data Protection in Humanitarian Action (second edition), p. 264: https://www.icrc.org/en/data-protection-humanitarian-action-handbook

5 E. Marchant (2020). Internet Governance in Displacement, p. 6: https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Internet-Governance-in-Displacement_WEB042020.pdf

The emergence of connectivity as aid is a significant step in the evolution of humanitarian assistance. As detailed in the literature review that follows (see section 2), digital connectivity has played a pivotal role in the transformation of the twenty-first century humanitarian response. This has been driven by both opportunity and necessity. Humanitarians and affected communities alike, have seized the opportunities presented by digital technology. Simultaneously, the exigencies of the sector have demanded the pursuit of efficiencies afforded by technology. However, the technologies that underpin connectivity interventions may also exacerbate existing risks or create new risks for users. This may particularly be the case for vulnerable groups who are said to lack 'digital literacy' - that is, "the ability to identify and use (digital) technology confidently, creatively and critically to meet the demands and challenges of living, learning and working in a digital society".[6] Digital literacy also entails an understanding of the potential benefits to be gained through the use of connectivity technologies. But this understanding must also be sensitive to the evolution of online threats.

Humanitarian practitioners and attuned scholars are beginning to appreciate the potential severity of the digital risks associated with access to and use of the Internet and mobile connectivity in crisis and emergency situations,[7] but the underlying dynamics in displacement contexts specifically are highly varied and under researched. Refugees may have particular backgrounds, experiences and constraints that shape their use of connectivity and understanding of digital risks during displacement, as well as particular needs as regards risk mitigation measures.

6 What does it mean to be digitally literate?: https://this.deakin.edu.au/career/what-does-it-mean-to-be-digitally-literate

7 Relevant scholarship in this area includes: 1) a 2018 report on The Humanitarian Metadata Problem - Doing No Harm in the Digital Era jointly authored by the ICRC and Privacy International: https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era; 2) a chapter dedicated to data protection concerns associated with connectivity as aid in the revised (2020) ICRC Handbook on Data Protection in Humanitarian Action: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian action.html; 3) GSMA's 2019 work on The Digital Lives of Refugees https://www.gsma.com mobilefordevelopment/resources/the-digital-lives-of-refugees; 4) research on the weaponization of social media in conflict areas led by The Do No Digital Harm Initiative: https://www.mercycorps.org/research-resources/weaponization-social-media; and 5) 2018 research by Simko et al.: Computer Security and Privacy for Refugees in the United States https://ieeexplore.ieee.org/document/8418616

Describing refugee connectivity use in the United States, Simko et al. note:

"Refugees, by definition, are fleeing from real threats, and hence might have unique perspectives on threats and adversaries. Further, there might be a range of cultural, linguistic, and technological challenges that refugees must overcome in order to sufficiently protect their computer security and privacy." [8]

It was on the basis of this US-centric observation that the UNHCR Innovation Service initiated this specific research. Specifically, it sought to explore connectivity dynamics in more diverse urban and rural settings in Uganda and Kenya.

These contexts have rarely been the focus of any research on this topic, despite the existence of large refugee populations, relatively mature markets for mobile services and fairly advanced digital policy environments in both countries. Moreover, the world in which refugees use digital technology will vary considerably depending on where they are from, where they have sought refuge, their individual backgrounds, etc., so conducting research beyond the European and North American contexts is tremendously valuable. The aim is to better understand how refugees in Uganda and Kenya perceive, assess and mitigate digital risks in their use of the Internet and mobile connectivity. This can in turn assist UNHCR and its partners in protecting connected refugees in the digital sphere. Furthermore, it would affirm digital risk management as a critical dimension to any connectivity as aid intervention undertaken by humanitarian organizations.

This field research endeavored to create a more robust evidence base to inform possible interventions. In the absence of such an evidence base, it would be unwise to set out to develop data protection awareness campaigns targeted at refugees (be it to help them safely connect to the Internet or use digital security tools such as secure messaging apps or privacy-enhancing technologies). Indeed, we must first understand the world in which refugees use digital technology, what they seek from connectivity, what concerns they hold—if any—about their safety and security online, and whether those concerns are informed by an adequate risk calculus. As connectivity usage does not take place in a vacuum, we must also account for the role that host countries and communities play in shaping these dynamics for refugees. As Payal Arora remarks in the closing of her 2019 book on the 'next billion users', "It is time to discover, in detailed research, how surveillance, security, and privacy play out in these much-neglected contexts."[9]

8 Simko et al. (2018), p. 410

9 Payal Arora (2019). The Next Billion Users: Digital Life Beyond the West, pp. 210-211

Research Objectives

This research builds on an extensive review of the existing literature on refugee connectivity,[10] as well as interviews and focus groups with connected refugees, and on-the-ground observations on connectivity sites in Uganda and Kenya in October 2019. It seeks to form a deeper understanding of the digital risks emerging from refugee connectivity and to inform appropriate mitigation measures. This understanding has been further shaped by the UNHCR Innovation Service's own experiences with delivering connectivity-as-aid solutions during the COVID-19 pandemic.[11]

The purpose of the research is to suggest pathways for action to improve the way that UNHCR secures the protection of refugees when accessing connectivity, as well as for addressing concomitant digital risks around connectivity (e.g. social media-related harms or mobile money fraud). We do not presuppose that refugees should use technology to connect, or, if they do, that the 'best practices' for most users are the optimal practices for refugees. This perspective—both valuing digital risk management, but not wanting to assume that established ways of conceiving and mitigating risk will match those of refugees—guided the formulation of the following research objectives:

- To develop a more nuanced understanding of how issues relating to digital risks (both real and perceived) manifest practically in the use of connectivity by refugees;
- To ascertain what role, if any, UNHCR and other stakeholders should play in helping support the protection of refugees in the digital environment; and
- Accordingly, determine suitable pathways for interventions to be undertaken by UNHCR and others to mitigate digital risks and ensure refugee protection online.

10 This literature review, undertaken by Tina Bouffet, is presented in the next section. It has also been published in its entirety as a stand-alone report (Connecting with Confidence: Literature Review): https://www.unhcr.org/innovation/wp-content/uploads/2020/03/Connecting-with-confidence-LitRev-Web.pdf

11 John Warnes (2020). Meeting communities where they are — the increasing preference of messaging apps: https://medium.com/unhcr-innovation-service/meeting-communities-where-they-are-the-increasing-preference-of-messaging-apps-3338ee9ee957

SECTION 1: MOTIVATIONS / RESEARCH OBJECTIVES

We initiated this research with the following exploratory research questions:

1. How do refugees use connectivity during displacement?
2. What barriers inhibit refugees from accessing connectivity?
3. What do refugees perceive as digital risks in their use of connectivity?
4. What vulnerabilities do refugees face unique to their circumstances in using connectivity?
5. What techniques do refugees practice to manage digital risks in their use of connectivity?
6. How do refugees learn about digital risks during their journeys and/or in their host environments?
7. What can humanitarian organizations do to help refugees mitigate digital risk in their use of connectivity?

A mobile phone mast near Rhino Camp Settlement in northern Uganda. © UNHCR/Michele Sibiloni

Key Definitions

As this report engages a number of technical concepts, some upfront definitional work is helpful:

Cyber Risk The risk of financial loss, disruption or damage resulting from the failure of digital technology (in the current context, internet and mobile connectivity technologies). These failures may materialize through deliberate and unauthorized breaches of security as well as unintentional or accidental breaches.[12]

Cyber Threats In the context of this research, cyber threats are circumstances or events with the potential to adversely impact people's use of Internet and mobile connectivity via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[13]

Cybersecurity Likewise, cybersecurity refers to measures taken to protect internet and mobile connectivity against unauthorized access or attack.

Data Protection Practices, safeguards and rules put in place to protect personal data.[14]

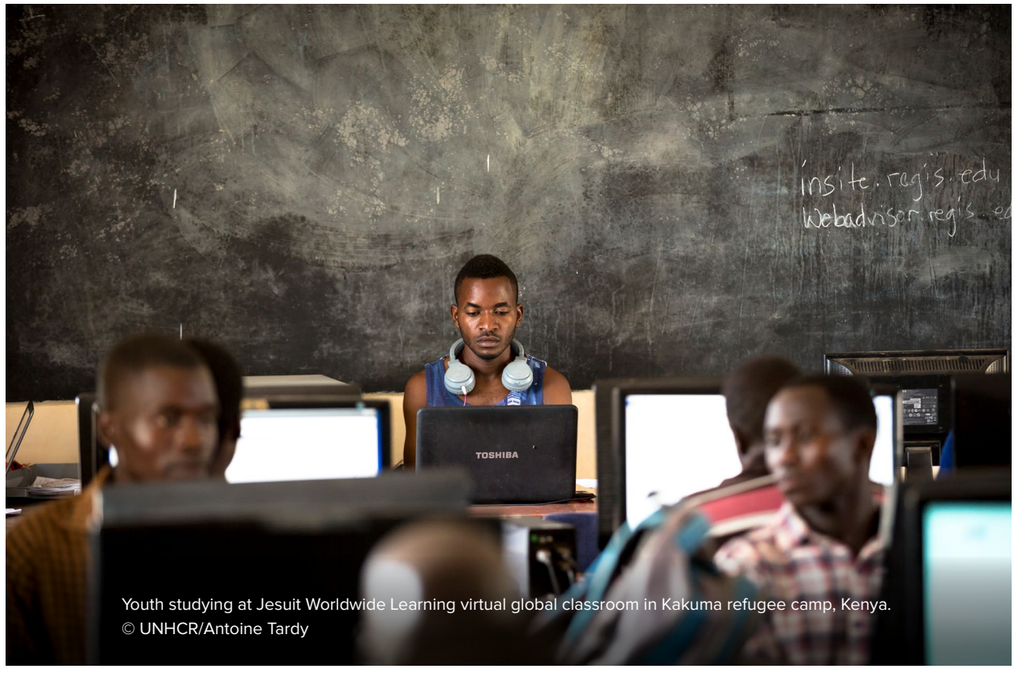
Digital Risks Unwanted - and often unexpected - outcomes stemming from the adoption of internet and mobile connectivity.[15] In the current context, digital risks include unwarranted communications surveillance, monitoring and intrusion, misinformation/disinformation over digital channels and cyber risks[16] emerging from connectivity.

12 U.S. National Institute of Technology and Standards: https://csrc.nist.gov/glossary/term/cyber_risk
13 U.S. National Institute of Technology and Standards: https://csrc.nist.gov/glossary/term/threat
14 See UNHCR's 2015 Policy on the Protection of Personal Data of Persons of Concern to UNHCR for further information: https://www.refworld.org/docid/55643c1d4.html
15 RSA (2020). Managing Digital Risk, p. 3: https://www.rsa.com/content/dam/en/e-book/how-to-manage-eight-types-of-digital-risk.pdf
16 See the 2018 symposium report on Digital Risks in Situations of Armed Conflict: https://reliefweb.int/report/world/digital-risks-situations-armed-conflict-symposium-report-codenode-london-uk-11-12-dec

SECTION 1: MOTIVATIONS / KEY DEFINITIONS

Disinformation Information that is false and deliberately created to harm a person, social group, organization or country. It differs from **misinformation**, which is information that is false but not created with the intention of causing harm.[17]

Privacy Usually defined as a person's right to control and selectively express information about themself, it is a fundamental human right that is recognized in the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), and other international and regional human rights conventions.



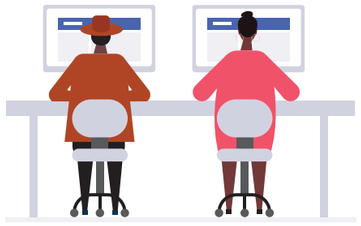
Youth studying at Jesuit Worldwide Learning virtual global classroom in Kakuma refugee camp, Kenya.
© UNHCR/Antoine Tardy

17 UNESCO: https://en.unesco.org/fightfakenews

Models of Connectivity as Aid

It is also important to distinguish between two basic models of connectivity that are relevant in displacement contexts and to an analysis of digital risks therein:

1. Community Connectivity Centers and;
2. Mobile-Centered Connectivity.[18]



Community Connectivity Centers[19] are communal spaces, generally financially supported by humanitarian organizations, in which refugees and others are able to access the Internet via workstations. These centers may also offer access to wireless connections for users to connect to the Internet via their own devices. This model of connectivity as aid is more centralized and generally easier for humanitarian organizations to control than mobile-centered connectivity, including from a security perspective. That said, the financial sustainability of community connectivity centers is a recurring concern.

Mobile-centered connectivity involves the direct provision of connections via cellular networks and does not require users to visit specific locations for regular access (though depending on the locale, signal strength may be poor). In this model of connectivity, the humanitarian actor may be involved in the initial provision of a mobile device, SIM card or airtime, but has little control over the service and how it is used once it is established. This is significant for how digital risks are identified and mitigated, and by whom.

Having laid the groundwork for the research, the next section delves into the extant literature on refugee connectivity and attendant challenges. This review of the existing evidence will help situate the empirical work undertaken by the Innovation Service, which is presented in section 3.

18 This distinction is addressed in further detail in the revised ICRC Handbook on Data Protection in Humanitarian Action, chapter 15

19 Giulia Balestra (2019). When innovation is yet another Connected Community Centre: Connectivity at the margins of innovation: https://medium.com/unhcr-innovation-service/when-innovation-is-yet-another-connected-community-centre-connectivity-at-the-margins-6bcb4227fc54

Literature Review[20]

Different authors pinpoint the mainstreaming of conversations on the role of technology and connectivity in humanitarian contexts to the watershed moment that was the response to the 2010 Haiti earthquake.[21] Volunteers used SMS and social media to crowd-map the response, monitor the situation, and share potentially life-saving information with affected people.[22]

Since then, different actors have commented on key trends and developments in the use of connectivity in humanitarian contexts. This includes the use of connectivity by both humanitarian practitioners and affected people, with each other and among themselves, as part of or independently from the humanitarian response. This review will focus on connectivity as aid, i.e. aid that supports affected people's ability to access digital technology and connect to the Internet.

Specifically, the review focuses on the means, barriers and associated digital risks that refugees face around connectivity, with special attention paid to refugees' perspectives on and experiences with connectivity. This includes, but is not limited to, mobile connectivity and social media, particularly in displacement contexts. This literature review is divided into different sub-themes:

1. Means to Connect;
2. Connectivity Divides;
3. Regulatory Barriers;
4. Other Influences on Usage Dynamics;
5. The Role of Connectivity in Refugee Lives;
6. Connectivity as a Form of Aid, and;
7. Digital Risks.

20 Tina Bouffet (2020). Connecting with Confidence: Literature Review: https://www.unhcr.org/innovation/wp-content/uploads/2020/03/Connecting-with-confidence-LitRev-Web.pdf

21 Barnaby Willitts-King et al. (2019). The Humanitarian Digital Divide: https://www.odi.org/publications/16502-humanitarian-digital-divide; Róisín Read et al. (2016). Data hubris? Humanitarian information systems and the mirage of technology: http://www.tandfonline.com/doi/abs/10.1080/01436597.2015.1136208; Patrick Meier (2015). Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response: https://link.springer.com/article/10.1007/s11673-017-9807-8

22 Meier (2015)

Means to Connect

The means that refugees use to connect have mostly been analyzed by service providers operating in displacement contexts, or trade bodies of which they are a part (namely, the GSM Association (GSMA)). Globally, mobile adoption continues to be on the rise, including in countries that contribute to outflows of refugees, transit countries and destination countries.[23] In 2011, a needs assessment in Kenya's Dadaab refugee camp found that "new Information and Communications Technologies (ICTs), including mobile phones are on the rise registering below 20% among long-term residents and around 10% for new arrivals".[24] Less than a decade later, in 2019, the GSMA's report on the digital lives of refugees found that over two-thirds of refugees in the selected research locations (i.e. in Jordan (Amman, Irbid and Zarqa), Rwanda (Kiziba camp), and Uganda (Bidibidi settlement)) were active mobile phone users. Active mobile internet users accounted for a third of all respondents, with many more aware of these services but unable to access them.[25]

Case studies indicate that these usage rates may vary across displacement contexts and among respondent groups. In a refugee camp in Greece, Latonero et al. found that 94% of men and 67% of women owned a mobile phone and 94% of all mobile phone users used WhatsApp, implying that they were able to access mobile data or a public Internet connection.[26] Even in contexts where mobile penetration rates are lower or more tightly regulated, refugees have found creative ways to access mobile services. These include sharing or borrowing handsets, or owning multiple SIM cards.[27] For instance, a case study of Nakivale refugee settlement in Uganda found that while 81% of respondents owned their own mobile phone, 12% were sharing a device with someone else.[28]

23 GSMA (2019). The State of Mobile Internet Connectivity Report 2019: https://www.gsma.com/mobilefordevelopment/resources/the-state-of-mobile-internetconnectivity-report-2019
24 Internews (2011). Dadaab, Kenya - Humanitarian Communications and Information Needs Assessment among Refugees in the Camps: Findings, Analysis and Recommendations, p. 19: https://internews.org/sites/default/files/resources/Dadaab2011-09-14.pdf
25 GSMA (2019). The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in The Way: https://www.gsma.com/mobilefordevelopment/resources/the-digital-lives-of-refugees
26 Mark Latonero et al. (2018). Refugee Connectivity: A Survey of Mobile Phones, Mental Health and Privacy at a Syrian Refugee Camp in Greece, p. 5: https://hhi.harvard.edu/publications/refugee-connectivity-survey-mobile-phonesmental-health-and-privacy-syrian-refugee-camp
27 GSMA (2019). The State of Mobile Internet Connectivity Report 2019: https://www.gsma.com/mobilefordevelopment/resources/the-state-of-mobile-internetconnectivity-report-2019
28 Samuel Hall (2018). Opportunities and Barriers to Using Mobile Technology and the Internet in Kakuma Refugee Camp and Nakivale Refugee Settlement: https://www.elrha.org/researchdatabase/opportunities-barrier-using-mobile-technology-internet-kakuma-refugee-camp-nakivale-refugee-settlement/

SECTION 2: LITERATURE REVIEW / MEANS TO CONNECT

The breakdown of the type of device owned also varies across contexts, and has significant implications in terms of access to app-sustained services as well as mobile security. In Nakivale refugee settlement, 27% of respondents owned a smartphone, 22% owned a feature phone, and 46% owned a basic phone. In Kakuma refugee camp, these numbers changed to 44%, 15%, and 39%, respectively.[29] These smartphone ownership rates contrast heavily with those found by Latonero et al. in Greece, where the overwhelming majority of mobile users had a phone that supported messaging apps and Internet applications.[30] This contrast has implications for the broader validity of research on refugee connectivity. Indeed, much of the research cited in this review focuses on European refugee contexts, which primarily host Syrian refugees. However, their ICT access and practices differ significantly from those of refugees in sub-Saharan Africa, and for whom information is more limited.

Moreover, even where refugees are able to obtain smartphones, these are likely to be older-generation devices.[31] This has implications for the level of security these devices can provide: software may no longer be supported and security patches may be unavailable,[32] not to mention the practical disadvantages such as relatively poor battery capacity, less efficient hardware, limited features, etc. The means that refugees use to connect is also subject to barriers like their ability to charge their phones, particularly in contexts with limited or cost-significant power supply.[33] It can also be conditioned by their ability to meet or circumvent legal barriers conditioning mobile access.

Finally, connectivity can also be accessed in specific communal locations, such as Internet cafés, community centers, etc. Not only in refugee camps and settlements, but also in urban areas, humanitarian organizations have invested in communal facilities, which are increasingly commonplace across a diversity of contexts. However, the affordability and accessibility of these locations varies across contexts, with access rates ranging from much cheaper to far more expensive than mobile data.[34] Moreover, individuals accessing connectivity in these locations may face other constraints, such as lack of anonymity, time constraints (in terms of duration but also access hours), etc.[35]

29 Ibid, p. 14
30 Mark Latonero et al. (2018), p. 5
31 ICRC and Privacy International (2018). The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era, p. 14: https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era
32 Ibid
33 GSMA. (2019). The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in The Way: https://www.gsma.com/mobilefordevelopment/resources/the-digital-lives-of-refugees
34 Samuel Hall (2018), p. 23
35 Ibid

Connectivity Divides

At first, connectivity was seen as a phenomenon with the power to act as a "potential equalizer" in society.[36] However, this optimism has been quickly and repeatedly called into question as technology was shown to be a replicator - if not amplifier - of social inequalities.[37] This includes areas affected by crisis. Writing on the response to Typhoon Haiyan, Madianou describes "sharp digital inequalities" which led to a "second-order disaster" among affected people who were left behind by the humanitarian sector's digital response. Countering this inequality with the design of inclusive responses has proven difficult,[38] with some even alleging that despite these efforts, the coverage of needs by the humanitarian sector was deteriorating.[39]

Connectivity divides predominantly align with gender lines, socioeconomic divides, differentiated access to education, disability or a combination of these.[40] They can also be exacerbated by factors such as geographic location and age,[41] biases built into technologies themselves - for instance, the difficulties that facial recognition software might have recognizing diverse datasets of faces[42] - or the trouble that automated mapping technologies have recognizing houses in crisis-affected areas.[43]

Among refugee populations, connectivity divides have impacted everything from the ability to travel safely,[44] to accessing mobile money,[45] connecting with family and friends, or safeguarding mental health.[46]

36 Benjamin Compaine (2001). Information Gaps, pp. 105–118: https://direct.mit.edu/books/book/2847/The-Digital-DivideFacing-a-Crisis-or-Creating-a

37 Eszter Hargittai (2003). The Digital Divide and What To Do About It: http://www.eszter.com/research/pubs/hargittai-digitaldivide.pdf; Eszter Hargittai (2008). The Digital Reproduction of Inequality: https://www.taylorfrancis.com/books/e/9780429494468/chapters/10.4324/9780429494468-69; Jen Schradie (2013). The Trend of Class, Races and Ethnicity in Social Media Inequality: https://doi.org/10.1080/1369118X.2012.665939

38 Willitts-King et al. (2019)

39 ALNAP (2018). The State of the Humanitarian System: https://www.alnap.org/help-library/the-state-of-the-humanitarian-system-2018-full-report

40 Willitts-King et al. (2019)

41 Willitts-King et al. (2019); Samuel Hall (2018)

42 ICRC and Privacy International (2018)

43 Willitts-King et al. (2019)

44 Samuel Hall (2018)

45 GSMA (2019). The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in The Way: https://www.gsma.com/mobilefordevelopment/resources/the-digital-lives-of-refugees

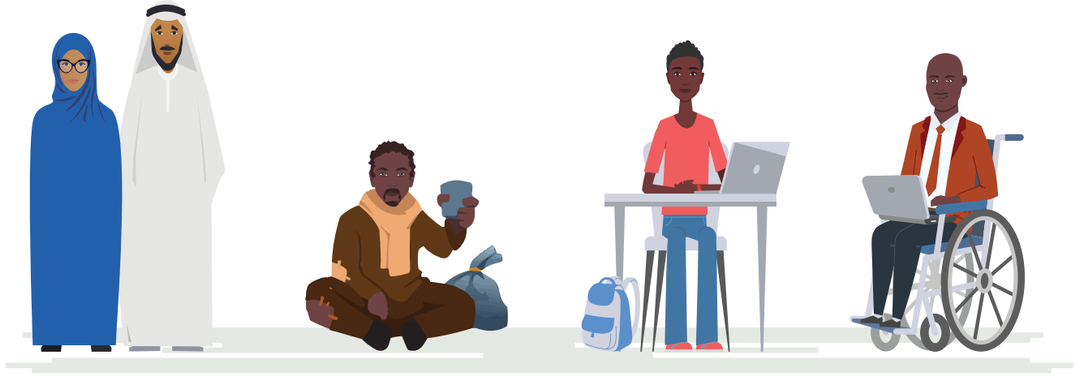
46 Latonero et al. (2018)

SECTION 2: LITERATURE REVIEW / CONNECTIVITY DIVIDES

Moreover, intersecting barriers relating to language and technical skills can compromise a refugee's ability to navigate connected devices and platforms securely, detect, avoid or seek redress for scams, and retain control and consent around the use of their data.[47] Finally, previous research by UNHCR has also documented how inequalities in mobile access can place certain individuals - for instance, single women with children and no income - at a greater risk of analog exploitation and abuse in order to be connected.[48]

In certain contexts, connectivity can also be subject to certain regulatory barriers or restrictions. A number of these are related to the ability to prove one's identity, a feat that can be particularly difficult for the UNHCR's populations of concern. Moreover, certain countries choose to deliberately restrict access to certain platforms and websites, or restrict the coverage available to areas known to host refugees. Documentation and research on these various types of barriers is further explored below.

Connectivity divides predominantly align with:



47 Khorshed Alam and Sophia Imran (2015). The Digital Divide and Social Inclusion among Refugee Migrants: https://www.emerald.com/insight/content/doi/10.1108/ITP-04-2014-0083/full/html; Kristy Crabtree and Petronille Geara (2018). Safety planning for technology: displaced women and girls' interactions with information and communication technology in Lebanon and harm reduction considerations for humanitarian settings: https://link.springer.com/article/10.1186/s41018-018-0031-x

48 UNHCR (2016). Connected Refugees: https://www.unhcr.org/5770d43c4.pdf

Regulatory Barriers

Over the past decade, a growing number of governments have conditioned mobile and internet connectivity to registration and proof-of-identity processes.[49] According to GSMA research, as of January 2020 governments of 155 countries had mandated SIM registration.[50] These policies place an estimated 1.1 billion people who lack recognized proofs of identification at risk of digital, social and financial exclusion. Among them are a number of refugees whose access to mobile enabled services - such as mobile money, pay-as-you-go utility services, navigation services, but also information and the ability to connect with family and friends - is compromised.[51]

1.1 Billion People

lack recognized proofs of identification

They are at risk of digital, social and financial exclusion

Mandatory SIM registration policies affect the majority of Latin America, Africa and Eurasia, with some states even linking this registration to biometrics (e.g. Nigeria, Syria or Bangladesh.)[52] However, these policies are not always enforced in a consistent manner. Countries like Somalia, Libya or Zimbabwe have a higher number of mobile subscribers than persons with official proof-of identity. This may be because acceptable identity credentials extend to non-official documents, but also because individuals rely on a peer to procure a SIM card for them or have procured one in derogation of the regulation. However, while the enforcement of SIM registration rules may have been lax at first, operators have started to apply it more stringently after fines and crackdowns were reported in countries like Nigeria and Kenya.[53] This puts a number of individuals at risk of seeing their mobile services - and the support network that comes with it - disconnected.

49 GSMA (2018). Access to Mobile Services and Proof of Identity: Global Policy Trends,Dependencies and Risks: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

50 GSMA (2020). Access to Mobile Services and Proof of Identity: https://www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks/

51 GSMA (2018). Access to Mobile Services and Proof of Identity: Global Policy Trends,Dependencies and Risks: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf; UNHCR (2019): Displaced and Disconnected: https://www.unhcr.org/innovation/wp-content/uploads/2019/04/DisplacedDisconnected-WEB.pdf

52 Ibid, p. 14

53 UNHCR (2016)

SECTION 2: LITERATURE REVIEW / REGULATORY BARRIERS

Moreover, a growing number of these registration processes involve the real-time verification of identity information in a government database, in contrast to simply holding photocopies or local digital scans of a person's credentials.[54] This complex and evolving shift can have real repercussions for refugees as the documentation they hold - if any - may not be sufficient to register for connectivity services. This was the case in Uganda, where only refugee ID cards were accepted as a form of identification to access SIM cards.[55] Fortunately, new guidance was issued in 2019, widening accepted forms of identification to other registration documents or attestation letters.[56] Here, humanitarian organizations can play a pivotal role achieving more inclusive and accessible registration processes.

A South Sudanese refugee buys airtime from a mobile phone vendor in the Imvepi settlement, northern Uganda
© UNHCR/Catherine Robinson

54 GSMA (2018). Access to Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

55 GSMA (2020): Proportionate Regulation in Uganda - A gateway for refugees accessing services in their own name: https://www.gsma.com/mobilefordevelopment/resources/proportionate-regulation-in-uganda-a-gateway-for-refugees-accessing-mobile-services-in-their-own-name/

56 UNHCR (2019). UNHCR welcomes Uganda Communications Commission directive to improve refugees' access to SIM cards: https://www.unhcr.org/afr/news/press/2019/8/5d5ba4274/unhcr-welcomes-uganda-communications-commission-directive-to-improve-refugees.html

Proof-of-identity requirements may be even more demanding when refugees interact with financial services and particularly mobile money (within or outside of the context of a humanitarian cash transfer program). Financial service providers must comply with Know Your Customer (KYC) requirements, even where there is a humanitarian organization acting as an intermediary.[57] These requirements, grounded in efforts to combat money laundering or the financing of criminal activity, are more stringent, and risk excluding a greater segment of the refugee population. Notably, the intergovernmental body responsible for setting standards in this space - the Financial Action Task Force - published guidance in 2020 on digital identification that includes an extended consideration of the realities and needs of refugees, warning of the risks of exclusion.[58] Civil society actors warn that the sharing of KYC data across different actors in the financial sector can also potentially lead to the financial exclusion or discrimination of individuals who have received humanitarian aid.[59]

Museveni Eric Rugambwa(R), 29, a refugee from D.R. Congo takes a selfie using a phone with his best friend, Kenyan national, Peter Mulu,30 at a field at Mwiki estate in Nairobi's Kasarani area where they reside. © UNHCR/Anthony Karumba

Finally, there are cases of host countries deliberately restricting refugees' access to mobile connectivity. A notable recent case would be that of Rohingya refugees in Bangladesh, whose mobile access was restricted to 2G voice service - i.e. no access to mobile data[60] - though these restrictions were lifted in August 2020 in light of the COVID-19 crisis.[61]

57 GSMA (2018). Access to Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

58 FATF (2020). Guidance on Digital ID: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

59 ICRC and Privacy international (2018)

60 Karen McVeigh (2019). Bangladesh imposes mobile phone blackout in Rohingya refugee camps: https://www.theguardian.com/global-development/2019/sep/05/bangladesh-imposes-mobile-phone-blackout-in-rohingya-refugee-camps; Aaron Martin and Linnet Taylor (2020). Exclusion and inclusion in identification: regulation, displacement and data justice: https://doi.org/10.1080/02681102.2020.1811943

61 Daily Star (2020). 3G and 4G mobile services restored at Rohingya camps: https://www.thedailystar.net/country/news/3g-and-4g-mobile-services-restored-rohingya-camps-coxs-bazar-1952373

Other Influences on Usage Dynamics

In their case study on how Syrian asylum seekers use social media to inform their migration decisions, Dekker et al found that social media restrictions and fear of digital surveillance from home governments constituted additional obstacles for migrants on the move.[62] Indeed, while a number of authors have confirmed refugees' awareness of digital surveillance and digital border control,[63] Dekker et al additionally mention strategies that refugees had developed to circumvent surveillance - namely, deactivating the WiFi signal or turning off their smartphone.[64] As such, fear of surveillance or lack of security may influence certain individuals' Internet or mobile use, leading for instance to added self-censorship.

Some refugees use virtual private networks (VPNs) to avoid monitoring or to circumvent local restrictions on certain websites or social media platforms.[65] However, the use of a VPN can drain the phone battery, may incur additional data charges, and significantly slow down navigation - particularly in older generation phones with limited processing power.[66]

Finally, connectivity taxes might also influence usage dynamics. In July 2019, the Ugandan government introduced a daily levy on over 60 online platforms, including Facebook, WhatsApp, and Twitter. As a result, millions of Ugandans were reported as having abandoned these Internet services.[67] This move could also adversely impact connectivity among refugees because of the financial cost incurred, but also, the reasoning behind it. Ugandan president Yoweri Museveni claimed the "Over the Top" (OTT) tax sought to prevent online gossip.[68] This could stoke fears of surveillance among refugee communities, and impact the freedom and agency with which they make use of mobile and Internet services.

62 Rianne Dekker et al. (2018). Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making: https://doi.org/10.1177/2056305118764439

63 From Huub Dijstelbloem and Albert Meijer (2009). De migratiemachine: de rol van technologie in het migratiebeleid: https://dare.uva.nl/search?identifier=f72527ba-a5d7-4413-9fc1-f627b5b4a2b6 to Melissa Wall et al. (2017). Syrian Refugees and Information Precarity: http://journals.sagepub.com/doi/10.1177/1461444815591967

64 However, turning off a smartphone does not necessarily mean that all forms of geolocalization are deactivated, as the phone may continue to ping nearby cell towers. The only way to prevent this is by removing the battery, a procedure that is unavailable in a growing number of smartphones (ICRC and Privacy International, 2018).

65 Andrienne Yandell (2016). "All refugees have smartphones…" and here's what we can do about it.: https://medium.com/@ayandell/all-refugees-have-smartphones-and-heres-what-we-can-do-about-it-511b5bf848b0

66 Duncan Kinuthia (2020). Exploring data anonymisation and VPN adaptation in East Africa: https://researchictafrica.net/2020/10/07/exploring-data-anonymisation-and-vpn-adaptation-in-east-africa/

67 Rebecca Ratcliffe and Samuel Okiror (2019). Millions of Ugandans quit internet services as social media tax takes effect: https://www.theguardian.com/global-development/2019/feb/27/millions-of-ugandans-quit-internet-after-introduction-of-social-media-tax-free-speech

68 Ibid

Role of Connectivity in Refugee Lives

People on the move have always sought ways to maintain networks and relationships across borders - be it by exchanging letters and audio cassettes, launching diaspora newspapers, running transnational radio stations or satellite channels, sending remittances, and over the past decade, making use of Internet and mobile connectivity.[69] The essential role that connectivity plays in refugee lives was famously spotlighted during the so-called '2015 European refugee crisis', which saw a wide circulation of photographs of Syrian refugees bearing smartphones and taking selfies.[70]

That being said, previous research had already investigated the role of Internet connectivity in identity development and integration among resettled migrants and refugees. In 2009, Elias and Lemish interviewed seventy teenage immigrants from the former Soviet Union to Israel, and found that the Internet had provided them with valuable resources for personal growth and empowerment.[71] More recently, drawing from interviews with more than fifty resettled refugees on their use of ICTs in host countries, Andrade and Doolin highlighted five key capabilities that connectivity offered in favor of their social inclusion: participation in an information society, effective communication, an understanding of the new society, social connection and cultural expression.[72] However, this was recently challenged by Marlowe, whose research found that connectivity, and namely the access to social media that it enabled, could hinder social integration.[73] Connectivity has also been credited for refugees' ability to maintain transnational connections and identities, ward off isolation or share the difficulties and challenges they face in their resettlement.[74]

69 Koen Leurs and Kevin Smets (2018). Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe: https://doi.org/10.1177/2056305118764425

70 Ibid

71 Nelly Elias and Dafna Lemish (2009). Spinning the web of identity: the roles of the internet in the lives of immigrant adolescents: https://journals.sagepub.com/doi/abs/10.1177/1461444809102959

72 Antonio Diaz Andrade and Bill Doolin (2016). Information and Communication Technology and the Social Inclusion of Refugees: https://doi.org/10.25300/MISQ/2016/40.2.06

73 Jay Marlowe (2019). Refugee Resettlement, Social Media and the Social Organization of Difference: https://onlinelibrary.wiley.com/doi/pdf/10.1111/glob.12233

74 Suzanna Brown et al. (2019). Refugees and ICTs: Identifying the Key Trends and Gaps in Peer-Reviewed Scholarship: https://www.springerprofessional.de/en/refugees-and-icts-identifying-the-key-trends-and-gaps-in-peer-re/16677744; SINGA France (2014). Refugees & ICT: https://marcopolis.org/wp-content/uploads/2017/04/SINGA-International-Study-2014-Refugees-and-ICTs.pdf; Simko et al. (2018)

SECTION 2: LITERATURE REVIEW / ROLE OF CONNECTIVITY IN REFUGEE LIVES

Andrade and Doolin's five key capabilities that connectivity offers in favor of social inclusion:

Connectivity also plays a key role for refugees during their flight. In 2018, Alencar et al. defined the 'refugee smartphone' as a companion, an organizational hub, a lifeline and a diversion.[75] Mobile services enabled people on the move to connect with family, friends, and other migrant communities, navigate through migration networks, store personal information and ensure a sense of security and preserve memories of their journey.[76] Mobile connectivity also means access to mobile-enabled utilities, namely mobile money - including person-to-person transfers, airtime top-up and international remittances.[77] As essential as connectivity has become during the flight stage, studies have also shown that refugees 'triage' information gleaned on social media based on existing social ties and personal connections.[78] In other words, to validate the information they find online, refugees use various strategies with links to the analog world.

75 Amanda Alencar et al. (2018). The smartphone as a lifeline: an exploration of refugees' use of mobile communication technologies during their flight: https://doi.org/10.1177/0163443718813486

76 Alencar et al. (2018); GSMA (2019). The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in The Way: https://www.gsma.com/mobilefordevelopment/resources/the-digital-lives-of-refugees

77 Ibid

78 Dekker et al. (2018); Annemaree Lloyd et al. (2013). Connecting with new information landscapes: information literacy practices of refugees: https://www.emerald.com/insight/content/doi/10.1108/00220411311295351/full/html

Connectivity as a Form of Aid

Connectivity has also been used as a means to provide services to support refugees in a variety of ways. Alongside humanitarian organizations, a rising number of tech entrepreneurs have taken part in 'digital humanitarianism' by creating platforms and apps that help refugees navigate local services, find work or training, access education or social services and more.[79] While these are not part of connectivity per se (concerning apps and content over access), connectivity plays a key role in the ability for these initiatives to reach their target audience - so much so that connectivity service providers have also launched similar initiatives. For instance, Ustad Mobile provides educational content in refugee camps in Bangladesh and Jordan,[80] and Vodafone-supported mPower Youth's uses mobile technology to advance children's rights by providing power, internet and IT equipment to refugee camps.[81] However, assessments of these new programs and tools have been mixed, partly due to their extensive duplication, their limited understanding of refugees' needs, or their funding and organizational limitations.[82]

Meanwhile, humanitarian organizations have used connectivity to alter the way they provide or expand their coverage for certain services. Livelihood programs are increasingly turned into digital voucher or cash transfer programs, medical assistance is provided through telemedicine or phone-based healthcare applications and community engagement and accountability are enhanced through the use of messaging apps and other platforms to conduct surveys, enable inclusive participation and feedback, disseminate info-as-aid or even flag protection concerns.[83]

79 Meghan Benton and Alex Glennie (2016). Digital Humanitarianism: How Tech Entrepreneurs Are Supporting Refugee Integration: https://www.migrationpolicy.org/research/digital-humanitarianism-how-tech-entrepreneurs-are-supporting-refugee-integration; Brown et al. (2019)

80 Fareed Rahman (2019). Generation Start-up: Ustad Mobile helps those living remotely access digital learning: https://www.thenationalnews.com/business/generation-start-up-ustad-mobile-helps-those-living-remotely-access-digital-learning-1.944740

81 Sara Okuoro (2019). Mpower: Enabling Refugee Children In Kenya To Learn: https://www.standardmedia.co.ke/article/2001349988/mpower-enabling-refugee-children-in-kenya-to-learn

82 Benton and Glennie (2016); Brown et al. (2019)

83 Ashwed Patil (2019). The role of ICTs in refugee lives: https://dl.acm.org/doi/abs/10.1145/3287098.3287144; UN Innovation Network (2019). Innovations 4 Scale – UNDP's Speak up with WhatsApp: https://www.youtube.com/watch?v=kU4lS4cPyOk; Brown et al. (2019)

SECTION 2: LITERATURE REVIEW / CONNECTIVITY AS A FORM OF AID

However, some have posited that the use of connectivity in the humanitarian response leads to affected people's identity and existence being determined by the personal data they surrender to humanitarian organizations.[84] In other words, some individuals might find themselves excluded from humanitarian assistance because of how their personal data does - or does not - define them. These fears of excluding certain people or coercing them into surrendering personal data in order to access aid, undermine arguments in favor of using connectivity to verify identity (e.g. to prevent fraud) or track an affected person's interaction with different parts of the humanitarian response.[85] These and other digital risks arising from the use of connectivity in humanitarian contexts—and particularly with refugees—are further explored below.

Congolese refugee stuyding at Kakuma refugee camp, Kenya © UNHCR/Antoine Tardy.

84 See comments in Wilton Park (2019). Digital dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation: https://www.wiltonpark.org.uk/event/wp1698/

85 Willitts-King et al. (2019)

Digital Risks to Refugees

The growing role that connectivity plays in refugees' lives also gives rise to new risks and vulnerabilities, particularly around cybersecurity, privacy and implications for the determination or acceptance of their refugee status.

The use of the internet and mobile connectivity with or among refugees often takes place in countries where data protection regulation is lacking, biased against user privacy or unable to ward off invasions of privacy coming from other jurisdictions.[86] Moreover, refugees themselves might not always be up to date or aware of data protection measures for online and mobile security.[87] Depending on the jurisdiction they find themselves in, or the access that they have granted to apps on their device, refugees may find their phone conversations - oral or written - as well as associated metadata (e.g. timestamps and location) intercepted and the personal information they reveal compromised.[88]

This may expose refugees to identification and surveillance by state and non-state actors in the country they are fleeing (with possible persecution or retaliation against their peers back home). It can also allow actors in transit or destination countries to gather information on their journey - from the migration route they used, to the persons they communicated with during their travel. In certain contexts, this information can be used to transfer them (for instance, in the EU context, to the first safe country of transit as stipulated by the EU Dublin regulations)[89] or to deny their asylum request on the grounds of demonstrated involvement with smuggling networks.[90]

While less specific to connectivity, the use of biometric registration by humanitarian organizations, or any other functional collection of data (e.g. to register individuals for an assistance program) can, if compromised, be used to identify and profile refugees for non-humanitarian purposes. This ability for well-intentioned data collection processes to be levied as means for discrimination, repatriation or retaliation has been dubbed 'function creep'.[91]

86 ICRC and Privacy International (2018)
87 SINGA France (2014)
88 ICRC and Privacy International (2018); SINGA (2014)
89 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32013R0604
90 SINGA (2014); Maria Gabrielsen Jumbert et al. (2018). Smart Phones for Refugees: Tools for Survival, or Surveillance?: https://www.prio.org/Publications/Publication/?x=11022; Privacy International (2019). Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers: https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers
91 Katja Jacobsen (2015). The Politics of Humanitarian Technology: https://www.routledge.com/The-Politics-of-Humanitarian-Technology-Good-Intentions-Unintended-Consequences/Jacobsen/p/book/9781138729322

Mitigating function creep requires that humanitarian organizations question the scope, management and security of their data collection processes, and above all, that they only retain this data for as long as is strictly necessary.[92]

Connectivity risks also manifest themselves in mobile-enabled services, such as cash transfers or smartcards. Because these programs involve financial service providers, they can invoke KYC requirements. Information collected about affected people in compliance with the requirements of a financial assistance program can eventually be used against them. For instance, someone who was registered as a cash transfer recipient may be denied loans in the future due to having received aid in the past.[93] In light of the increasingly interconnected and multinational nature of financial and financial technology (fintech) services, information collected about affected people can be accessible to multiple parties in multiple jurisdictions, including some where legislation on financial data protection has yet to catch up to mobile money markets.[94]The use of connectivity as aid in humanitarian response, or its increased availability in displacement contexts, can also further expose refugees to misinformation, propaganda, hate speech or other phenomena related to the 'weaponization' of information.[95] This vulnerability can be particularly pronounced among certain social groups, as demonstrated by Geara and Crabtree in their study of women and girls' interactions with ICT in Lebanon.[96]

Finally, connectivity and/or connected services remain inherently fallible to interruptions, hacks, design flaws or diversion (i.e. using an app for a purpose other than that for which it was intended). Increased reliance on connectivity can put people at risk should there be a power cut or network loss. Data collected or generated via connected services can be compromised or distorted, especially as attempted hacks against humanitarian organizations are on the rise. Design flaws can generate inaccurate or faulty data which, if taken at face value because of the legitimacy granted to technology, can hinder refugees' ability to assert their identity or personal history.[97] In the following section, we build on these rich observations by exploring refugee perspectives on connectivity and digital risks in Uganda and Kenya, starting with a description of the research methods and target groups.

92 ICRC and Privacy international (2018); Wilton Park (2019); UNHCR (2015). Policy on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/docid/55643c1d4.html
93 ICRC and Privacy International (2018)
94 See, for example, Oludare Senbore et al. (2019). How should Nigeria regulate its fintech industry? https://www.lexology.com/library/detail.aspx?g=92f8de68-2d59-466c-b3b4-687f2a18d131
95 Privacy International (2013). Aiding Surveillance: https://privacyinternational.org/report/841/aiding-surveillance; Katja Jacobsen (2015). Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees: https://www.jstor.org/stable/26292335; Joseph Guay et al. (2020). The Weaponization of Social Media: https://www.mercycorps.org/research-resources/weaponization-social-media
96 Geara and Crabtree (2018)
97 Privacy International (2013); ICRC and Privacy International (2018); Willitts-King et al. (2019)

Analysis and Findings

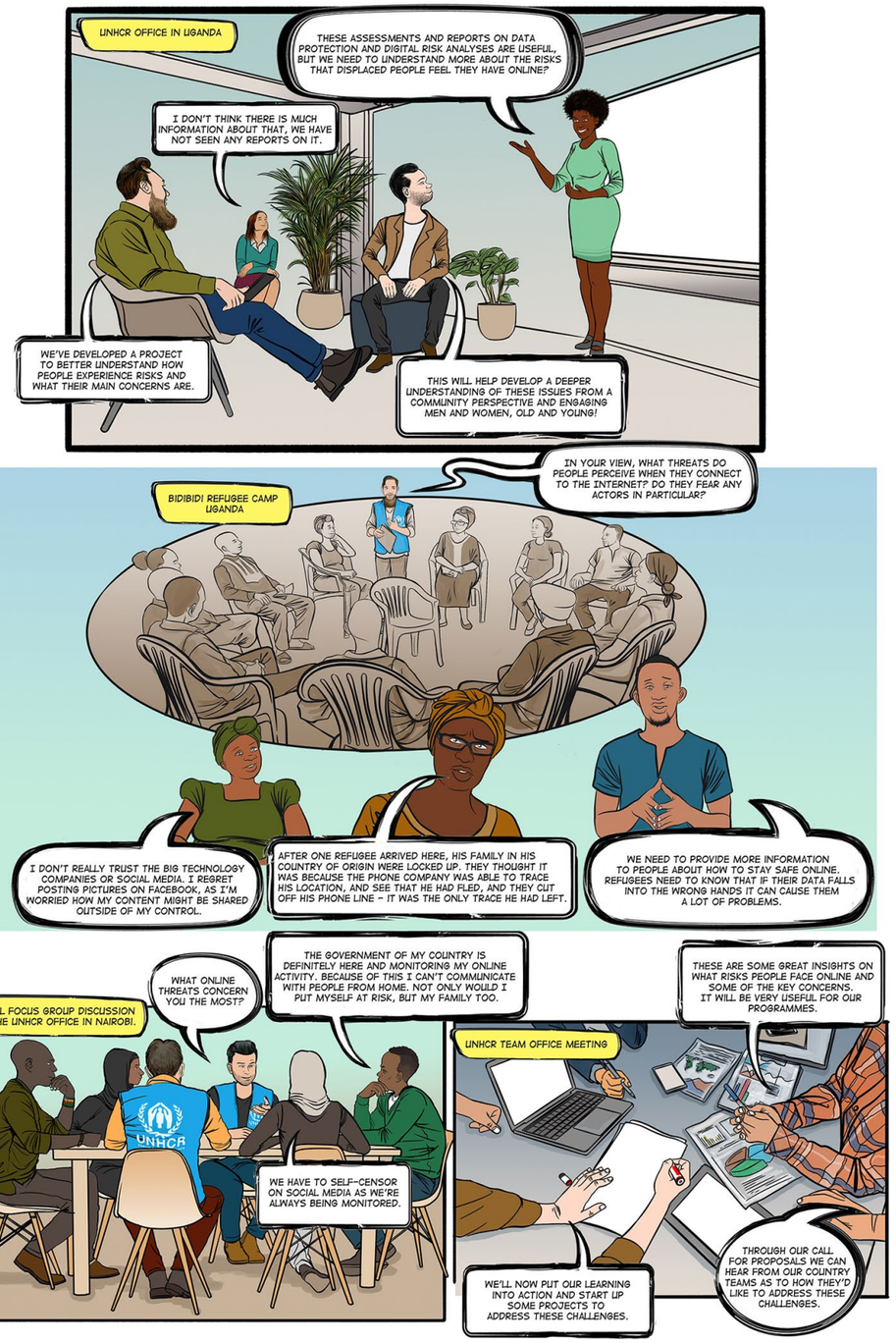
Brief note on methods

In October 2019, members of the UNHCR Innovation Service visited Uganda and Kenya to conduct key informant and focus group interviews with refugees and, in a few cases, host community members.[98] These informants were purposefully sampled from known refugee and host communities who use the internet and mobile connectivity and were selected with help from UNHCR in-country staff and community organizations. All respondents were over the age of 18. Consent was verbally obtained in advance of each interview. In total, over 80 interviewees across both urban and rural settings participated (see Table 1 for additional information on the interviewees). It is important to note that a concerted effort was made to provide women with an equal opportunity to share their views on the topics under discussion. However, due to the subject matter and unfortunate discrepancies in female access to connectivity, recruiting women as interviewees remained challenging.[99]

In addition to the interviews, the research team observed sites where refugees access the internet, namely at community connectivity centers supported by UNHCR and other humanitarian organizations. This allowed for first-hand observation of how users connect to the Internet in displacement contexts, what security and privacy practices they visibly employ and opportunities for strengthening protections at these sites.

98 While our recruitment focus for the interviews was on refugee users, during the focus groups in the settlements we discovered that a very small number of interviewees were actually Ugandan nationals living locally.

99 A fuller note regarding the research methodology and the rationale driving key methodological decisions can be found in Annex 1. Annex 2 captures the interview consent procedure. Annex 3 lists the semi-structured interview questions.



UNHCR Innovation Service has been working with Nairobi graphic artist @Noah Mukono to illustrate the findings of the Connecting with Confidence research in comic form.

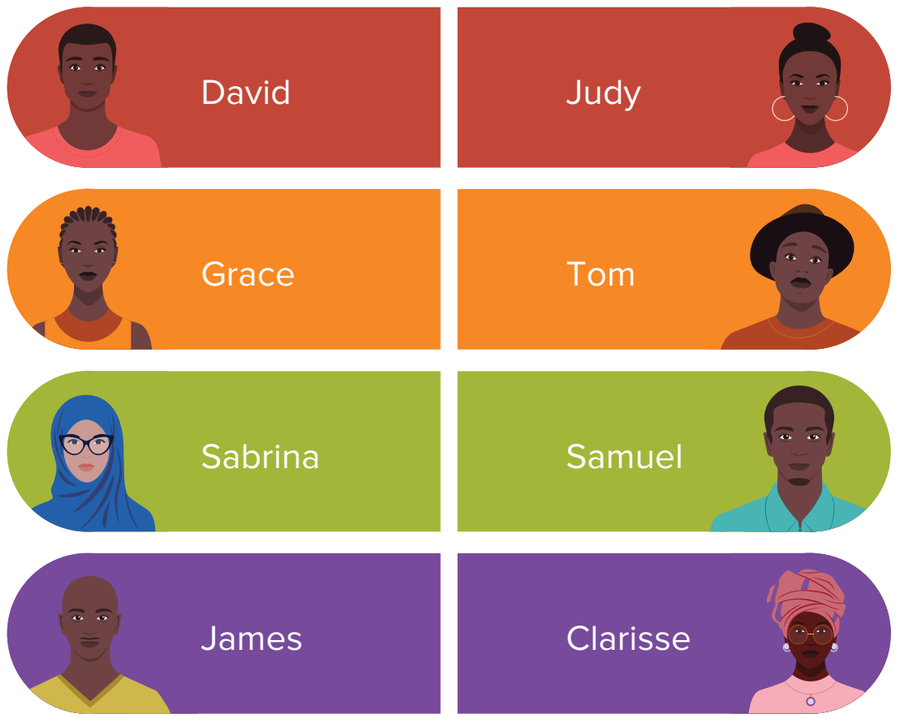
Group Number	Location	Group composition	Number of Interviewees (male and female)
1	Interaid community center Kampala, Uganda	Young[100] urban refugees	8 (6m, 2f)
2	Interaid community center, Kampala, Uganda	Young urban refugees	7 (6m, 1f)
3	Arua, Uganda	Staff of a community-based organization providing refugee connectivity	2 (both male)
4	Arua, Uganda	Staff of a community-based organization providing refugee connectivity	5 (all male)
5	CTEN community center, Bidibidi refugee settlement (zone 4)	Young rural refugees	5 (3m, 2f)
6	CTEN community center, Bidibidi refugee settlement (zone 4)	Young rural refugees	13 (7m, 5f)
7	SINA Loketa community center, Bidibidi refugee settlement (zone 2)	Community leaders (older)	7 (all male)
8	SINA Loketa community center, Bidibidi refugee settlement (zone 2)	Rural refugees	6 (3m, 3f)
9	Rhino Camp refugee settlement, Uganda	Community leaders (older)	13 (10m, 3f)
10	UNHCR country office, Nairobi, Kenya	Young urban refugees	6 (3m, 3f)
11	UNHCR country office, Nairobi, Kenya	Young urban refugees	6 (3m, 3f)
12	UNHCR country office, Nairobi, Kenya	Young urban refugees	6 (3m, 3f)

Table 1: Summary of interviewees

100 In engaging communities, the research team opted not to inquire specifically with each participant as to their reported age, beyond identifying (and excluding from selection) minors under the age of 18.

Connectivity Personas

Inspired by recent research on mobile technology use in humanitarian settings,[101] we hereby present eight 'personas' that highlight the diversity of refugee perspectives captured in our field research. We opted for the persona approach for two reasons in particular. First, it allowed us to capture the richness of the qualitative data from the interviews in a way that is readable and engaging. Second, through the personas, we could bring forward a diversity of perspectives from the discussions with refugees. While these personas are fictitious (i.e. the names are not real), they are composite profiles based on the stated views of interviewees. They represent the connectivity context and challenges facing users in the sites visited and illustrate the salient concerns of the research.



101 GSMA (2020). Human-centred design in humanitarian settings: Methodologies for inclusivity: https://www.gsma.com/mobilefordevelopment/resources/human-centred-design-in-humanitarian-settings/

David

Age: 20
Country of Origin: Burundi
Host Country: Uganda, Kampala
Devices: Android Smartphone

Connectivity Concerns and Threats:
Social Media Hacking

David, 20 years old, is originally from Burundi but now lives in Kampala, where he's an ICT student. He regularly visits the local connectivity center, run by the NGO Interaid, to access the Internet and pursue his technology studies. Like many other users at the center, David comes to the Interaid facility to do research for this course. Even though access to the center is regulated based on one's nationality to ensure fair access for all (Burundians are allocated access on Tuesdays), he manages to get online at the center a few days per week. While it's free for him to use the center, he has to take a taxi to get there, which costs him 500 UGX [0.13 USD].

David has an Android-based smartphone, which he also uses to connect to the Internet, but he's careful about using his phone to access services that consume a lot of data. He enjoys using social media, but the government's recent tax on over-the-top (OTT) media services has made it more expensive. He learned from a friend that by installing a tool called a VPN, he could avoid paying the OTT tax. So far, however, his experiences with VPNs have been mixed. He's noticed that they tend to drain his battery very fast and some of them consume a lot of data (which for him, defeats the purpose of using the tool). He recently uninstalled his VPN and instead pays the OTT tax for a day at a time in order to update his social media accounts.

> *"There are a lot of VPN apps available, but not all are safe to use. Sometimes I feel I might be putting my data at risk by using the wrong app."*

While David has never had his social media or email accounts breached or hacked, he's heard stories from friends about people's accounts being compromised. He's not exactly sure what happened, but it's generally assumed that the attacks come from abroad. Certain countries in West Africa have a reputation as being home to hackers who target Internet users in East Africa. A more pressing concern for David is mobile money fraud. He was tricked into transferring money to a fraudster once. He was desperate at the time but felt powerless to do anything about the incident and didn't report it. He's since become much more vigilant about his mobile money transactions.

Sabrina

Age: 22
Country of Origin: Somalia
Host Country: Uganda
Device: Android (Knock off Phone)

Connectivity Concerns and Threats
Mobile money fraud, Trusting Gmail

Sabrina, 22 years old, is originally from Somalia but now lives in Kampala. She, too, is an ICT student. Like David, she regularly visits the Interaid connectivity center, where she uses the workstations for her studies. She comes with her friends on Thursdays (the day allocated to Somalis).

Sabrina also owns an Android device, like most other people her age ('knock-off' phones running the Android operating system are especially common in Kampala due to their affordability and widespread availability). She's not a heavy social media user—her preferred application is WhatsApp, which she uses to communicate with family and friends. While WhatsApp is also subject to the government's OTT tax, Sabrina's mobile operator offers a low-cost bundle that already covers the tax, so Sabrina doesn't need a VPN to access these services. She prefers it this way because she's heard stories about untrustworthy VPNs that steal your data. She doesn't understand why the Android app store doesn't police these things better. When asked if she trusts WhatsApp and Google with her data, she says she does but then adds that she really doesn't have much of a choice. She uses Gmail because it was required for her to set up her Android device. And everyone in her community uses WhatsApp, so she does too. These feel like false choices to her.

Like many other of our interviewees, Sabrina has also been subject to mobile money fraud - someone conned her into transferring funds to a stranger and she was unable to recover the money. She reported the incident to her mobile operator, which provides the mobile money service, but they told her there's nothing they can do. She would like the Ugandan police to do more to crack down on these malicious actors, but her expectations for increased law enforcement are low. Since the incident, she's helped her friends and family avoid being defrauded in similar ways.

> *"There's nowhere to go to report cybercrime or online threats. The police don't know enough about it, so they aren't able to help. The only thing we can do is try to avoid it."*

James

Age: 20
Country of Origin: South Sudan
Host Country: Uganda
Devices: Several Mobile Phones

Connectivity Concerns and Threats:
Wifi Hotspot Funding

James, 35 years old, is a South Sudanese refugee who now lives in the Bidibidi settlement in the north of Uganda. Not only does James frequently use connectivity, but as a staff member at a connectivity center in one of the settlement's zones, he also facilitates access to connectivity for others living in Bidibidi. James uses several mobile devices, including smartphones, and has multiple SIM cards. These come in handy in Bidibidi because the network signal is often poor and providers cover different parts of the settlement. One risks losing connectivity if they only rely on a single operator. James hasn't had any problems registering his SIM cards because he's been issued with a refugee ID card (the legally required document). However, he knows many people who still haven't received their IDs and who have to resort to asking others to register SIMs for them. He wishes there were more SIM registration locations in Bidibidi, because people have to travel long distances to access service centers, which proves to be yet another barrier to mobile connectivity.

> *Refugees are frequently overcharged for SIM cards, paying an extra 5000 UGX (1.34 USD) on top of the usual 2000 UGX (0.54 USD) And the worse thing is that the SIM card may only last a day or two before it's blocked (due to registration irregularities).*

At the connectivity center where James works, an Internet satellite connection is available for 12 months thanks to an in-kind donation from a technology service provider. The community is very happy about this connectivity—people can connect to a WiFi hotspot with their smartphones or use one of the five available public workstations. James is worried about what will happen after the 12 months is up. The center can't afford to pay for the connection without external financial assistance. The Internet connections at the center are managed remotely by the satellite provider. Access to certain websites is blocked. The provider is normally quite responsive to requests from James and his colleagues about updating the list of restricted sites, but the community center wishes it had greater control over the filter. For example, there are periods when YouTube is unavailable due to concerns about bandwidth consumption, but the community center hosts a film editing class that needs access to the platform for educational purposes.

Grace

Age: 19
Country of Origin: Uganda
Host Country: Uganda
Device: Communal Laptop

Connectivity Concerns and Threats
Users often forget to log off the laptop

Grace, 19 years old, is Ugandan and lives in a neighbouring host community. She regularly visits the community connectivity center in the settlement to use the Internet on a communal laptop owned by the center. To do so, she has to travel a very long distance from one zone to another. She makes this journey, in part, because she doesn't own a mobile phone - just a SIM card. Her friend will occasionally let her use their device with her SIM, but they've recently been less willing to do so because recharging the battery can be a problem in parts of the settlement without reliable electricity, including where she lives. There are charging centers in different parts of the settlement, but she doesn't feel comfortable leaving her friend's phone unattended while the battery charges.

Not having her own mobile device can be quite frustrating. At least in the connectivity center, Grace can access social networking sites and use email. But with her own phone she could more readily access WhatsApp and mobile money, two increasingly essential services in her community.

> *Everyone shares their phones, or borrows them if they don't have one, usually to family and close friends. We don't really have any alternatives. On some apps like Facebook you can log out—on others like WhatsApp you can't do that so you have to trust the phone's owner.*

At the connectivity center, Grace has noticed that other users often forget to log out of their social networking and email accounts, even though there are online safety notices posted on the walls of the center advising users to do so before leaving. She's always very careful to sign off, even though she trusts her colleagues.

Clarisse

Age: 29
Country of Origin: South Sudan
Host Country: Bidibidi, Uganda
Devices: N/A
Connectivity Concerns and Threats: Information Theft, Cyber Bullying, Physical violence as a result of online activity, Resettlement scamming

Clarisse, 29-years old, is originally from South Sudan but now lives in Bidibidi. She spends a lot of time at the community connectivity center in the settlement, but not to access the internet. As a place of social gathering, the center facilitates other activities that she finds enjoyable, including arts and crafts, but by her account going online is too risky. She's heard numerous stories about people's information being stolen online, humiliating or indecent photos appearing on social media profiles, various scams and even cases of violence following from online activity.

> *Many refugees I know send and accept lots of friend requests on social media and this is a problem: I found that my neighbor who is a refugee was beaten up. He accepted a friend request from someone on Facebook and when they found him they attacked him. We need to be more vigilant.*

One type of online scam has proven particularly unsettling for people like Clarisse: resettlement scams. Clarisse recounts the story of someone from her zone in Bidibidi who was targeted by an advertisement for a resettlement program on a popular social networking site. The refugee was led to believe that he would be resettled to Canada. The refugee was asked to transfer a large sum of money to facilitate his move, but it turned out that the organization involved was fraudulent and the money was lost, never to be recovered. This incident has really stuck with Clarisse. She is especially concerned about how these false advertisements persist online and even wonders if social networking sites financially benefit from the scams.

Samuel

Age: 45
Country of Origin: South Sudan
Host Country: Rhino Camp, Uganda
Device: Smartphone

Connectivity Concerns and Threats: Online surveillance by security organs

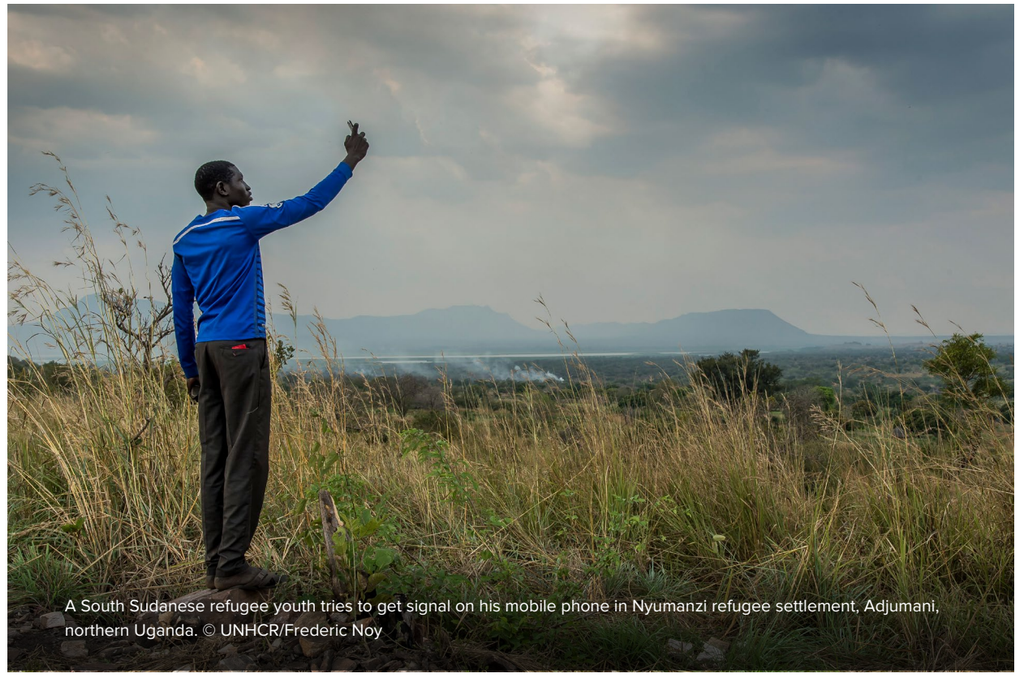
Samuel, 45-years old, is South Sudanese and lives in Rhino Camp, another settlement located in the north of Uganda, where he is a zone leader. He and the other zone leaders use smartphones that were gifted to them by UNHCR through a philanthropic effort by a global technology company. Some of the leaders have recently experienced problems with their devices. However, because the company stopped supporting those devices, they are unable to get technical support. Samuel's device is working fine though. He uses two SIM cards for the different networks available in Rhino Camp. UNHCR and its local partners provide airtime to the zone leaders to facilitate communication between the settlement and protection officers.

Samuel laments the distances between parts of the settlement and mobile agents, which make cash-in/cash-out mobile money transactions especially difficult. Many people have to travel all the way to Arua (a nearby town circa 1 hour drive away) to visit mobile service centers, for example to complete their SIM registration. Due to changing identification requirements, Samuel has had to re-register his SIM cards on several occasions.

The community connectivity center in Rhino Camp offers WiFi connectivity to the settlement's inhabitants, which Samuel uses when he can. He mostly goes to the connectivity center when he needs to download updates for his smartphone. He can't do this over his mobile connection because it consumes too much data. But on occasion the center's WiFi connection isn't working, which means sometimes it's weeks or months before he can download the latest updates for his device. He worries that this might make his device insecure.

Samuel has heard young people at the connectivity center talking about VPNs but he doesn't use one. He thinks it's easier to pay the OTT tax. Anyway, someone told him that his brand of smartphone doesn't have a lot of reliable VPN options in the app store. When asked about who might be interested in monitoring his communications, Samuel immediately responds that authorities from his home country are his primary concern. Whenever he calls family members in South Sudan, he is very careful about the language he uses and refrains from discussing anything politically sensitive. He prefers to share information by phone instead of over social media.

> *Direct phone calls are probably safer than using social media, as people are less likely to record and share audio, whereas it is easy for someone to take a screenshot of something you've written on Facebook.*



A South Sudanese refugee youth tries to get signal on his mobile phone in Nyumanzi refugee settlement, Adjumani, northern Uganda. © UNHCR/Frederic Noy

Judy

Age: 20
Country of Origin: Rwanda
Host Country: Kenya
Devices: Smartphone and Laptop

Connectivity Concerns and Threats:
Online government surveillance.

Judy, 20 years-old, is originally from Rwanda and now lives in Nairobi. By all accounts, she is 'well-integrated'. Not only does she have the required identity credential to register a SIM card in her own name, she's also managed to open a bank account, which she needs to receive the salary from her job.

Judy owns a laptop, which she uses for her studies and work, but like most young people she prefers to connect to the Internet using her mobile phone. She has an Android device and is an active user of social media. She worries about mobile device theft in Nairobi and is super cautious about 'snatchers' getting away with her phone in public.

Judy thinks a lot about what information she puts online and how it might be used against her. She voices her concerns about a wide range of potential threat actors: she says she doesn't trust the Kenyan government because they have politicized refugee issues. Her mother has also warned her not to post any information that criticizes the Rwandanese government. She fears that, otherwise, they might harm family members who are still in the country.

> *The government of my country is definitely monitoring my online activity. Because of this, I can't freely communicate with people from home. Not only would I put myself at risk, but my family too.*

Judy says she trusts UNHCR and is willing to provide personal information to the agency, but she does sometimes wonder how much of it is shared with Kenyan authorities.

> *We trust UNHCR to take care of our data and not misplace it. We don't always trust our host government. There are some questions we have, though, on the relationship between UNHCR and governments.*

Tom

Age: 23
Country of Origin: Uganda
Host Country: Kenya
Devices: Laptop and Smartphone

Connectivity Concerns and Threats
Cyber Threats, Social Media Impersonators

Tom, 23-years old, is a Ugandan refugee who lives in Nairobi. Tom spends a lot of time online using both a laptop and his mobile device. He spends a lot of time online looking for scholarships to study in North America. He is extremely cautious in his online activities. Unlike other people in Tom's social circle in Nairobi, he never accepts invitations on social media from strangers abroad. His online social network is therefore quite limited and that's fine by him, even if others like to brag about how many connections they've made online.

> *People are eager to find friends abroad, specifically from Europe and North America, and they put themselves at risk as scammers disguise themselves as being from these places.*

Tom believes that cyber threats are commonplace and sometimes dangerous. He explicitly mentions the 'dark web'—a part of the Internet where vicious things happen. He's never been on the dark web but a friend of his once came close, he says.

> *He heard about the dark web and tried to access it as he was curious. He tried to be careful but found some dangerous things, and extremely bad content including torture images, so he stopped accessing it.*

Despite his cautious approach to connecting online, Tom's access to the Internet and digital services is precarious. He isn't able to legally access mobile connectivity due to not having the right form of identity credential. This means he was forced to pay a local to register a SIM for him. He also experiences problems verifying the identity registered against the SIM whenever he has issues with his money mobile wallet.

These personas capture many of the concerns voiced during the interviews with refugees. In what follows, we elaborate the key thematic findings from the analysis.

Findings on Community Perceptions

The first set of findings center on the perceptions of interviewees regarding connectivity and digital risk, as well their expectations of UNHCR in this domain.

I. Connected refugees recognize the importance of security and privacy online

Members of the different communities we interviewed were highly engaged with the issues under discussion, finding the topics highly relevant to their own connectivity experiences. While certain gaps were revealed in their understanding, for example around the business models of major technology companies, interviewees' familiarity with a host of complex issues ranging from Virtual Private Networks (VPNs) to the 'dark web' illustrated the capacity for some refugees to be engaged with and active on matters of community protection online. As such, community members using social media in particular were more likely than not to actively self-censor their online activity.

> *We have started using coded language in our online conversations so we can speak more freely about issues without worrying about people listening in.*

II. Communities in many ways feel powerless to do much about cyber threats and digital risk.

A recurring theme among interviewees was a feeling of powerlessness to do much about the cyber threats and digital risks present in their use of connectivity. Some of those who had experienced hacks or fraud reported attempts to alert service providers and in some cases law enforcement about the incidents. In nearly all cases, incidents were not resolved.

Some interviewees expressed a hope that UNHCR could do more to detect and assess cyber threats, as well as to help them mitigate digital risks, in their use of connectivity. Concrete ideas around the role of both humanitarian organizations and the private sector in helping refugees stay safe and secure in their use of connectivity are offered in the next section.

> *As refugees, we don't always enjoy the same rights as others. Some police officers don't want to help us as much as they do host community members.*

III. Connectivity is highly valued, despite awareness of digital risks.

Despite the range of digital risks discussed and experiences shared, interviewees stressed the critical importance of being connected and deciding on their own terms how they engage and present themselves online. Their appetite to connect has not waned despite increased awareness of - and concerns about - online security and privacy. Without explicitly suggesting they would trade their privacy or security for access, it was clear that access to connectivity is a high priority for nearly everyone who was interviewed.[102]

> *For us the reliability of the cell service matters more than how much we trust the operator.*

> *For me the biggest challenges aren't related to network security or safety online, but internet speeds. I can't do anything with the speeds I'm getting where I live.*

102 It is worth repeating that the interviewees were purposefully sampled. This finding should be interpreted with this caveat.

IV. Communities generally trust UNHCR to protect their data, but this trust should not be taken for granted.

Many interviewees believed that with the range of digital risks faced, there were limited mitigation strategies available, with the primary one being the provision of more systematic information around the different risks that exist online. UNHCR was identified as a trusted actor who could play a role in supporting and enhancing communities' understanding through information campaigns according to the preferred channels of the different user groups. It was also noted that UNHCR should work with other actors - in particular MNOs - to help them devise appropriate strategies to help protect their customers. Many refugees were not overly concerned with UNHCR having access to data or metadata on themselves and their activities, or it being transferred as a part of provision of connectivity services. However, it was noted that they expect it to be kept safe and the specifics of the data-sharing relationship between UNHCR and other actors including governments to be clarified.

> *In general, people trust the mobile operators. They've seen services get better and coverage increase, though there are still gaps and the operators frequently overestimate their coverage. They could definitely do more to provide information to their customers on staying safe online.*

Young South Sudanese refugees charge their mobile phones at the Community Technology Empowerment Network centre at Rhino Camp Settlement in northern Uganda © UNHCR/Michele Sibiloni

Findings on Real-World Impacts

These findings concern the impacts of the digital risks environment facing connected refugees, as well as the role of the policy environment in shaping digital risks.

I. Both real and perceived risks and their impacts, vary significantly across age, gender and other characteristics, though there are commonalities.

In general, younger connectivity users who were interviewed were more attuned to the specifics of technology and digital risk, however older interviewees came to appreciate the importance of the issues through the focus group discussions in spite of a generally lower level of technical knowledge. Female interviewees, who in some cases were less frequent users of connectivity due to disparities in access, demonstrated different understandings of digital risk compared with men. A lack of knowledge contributed to a more conservative approach when engaging with such technology, and sometimes complete reticence to engage in certain applications such as social media, where gender issues were flagged as an area of real and perceived concern. Issues of access for people with disability were flagged in discussions as a point of concern, however this was more related to physical risks linked to connectivity access, rather than specific risks when accessing digital spaces. Emphasis was placed on those with impaired movement, rather than communication impairments (hearing, visual). This is related to users having to walk/move to get to agents to buy airtime, purchase devices and sometimes even find cellular signal or other connection opportunities.

> *People are divided in their use of technology and connectivity. Youth are more switched on, and women are less likely to use smartphones, mainly due to the cost as they often bear the brunt of other priorities.*

> *Disabled people have a right to use phones. Those who are not mobile face extra risks so we need to do more to support them.*

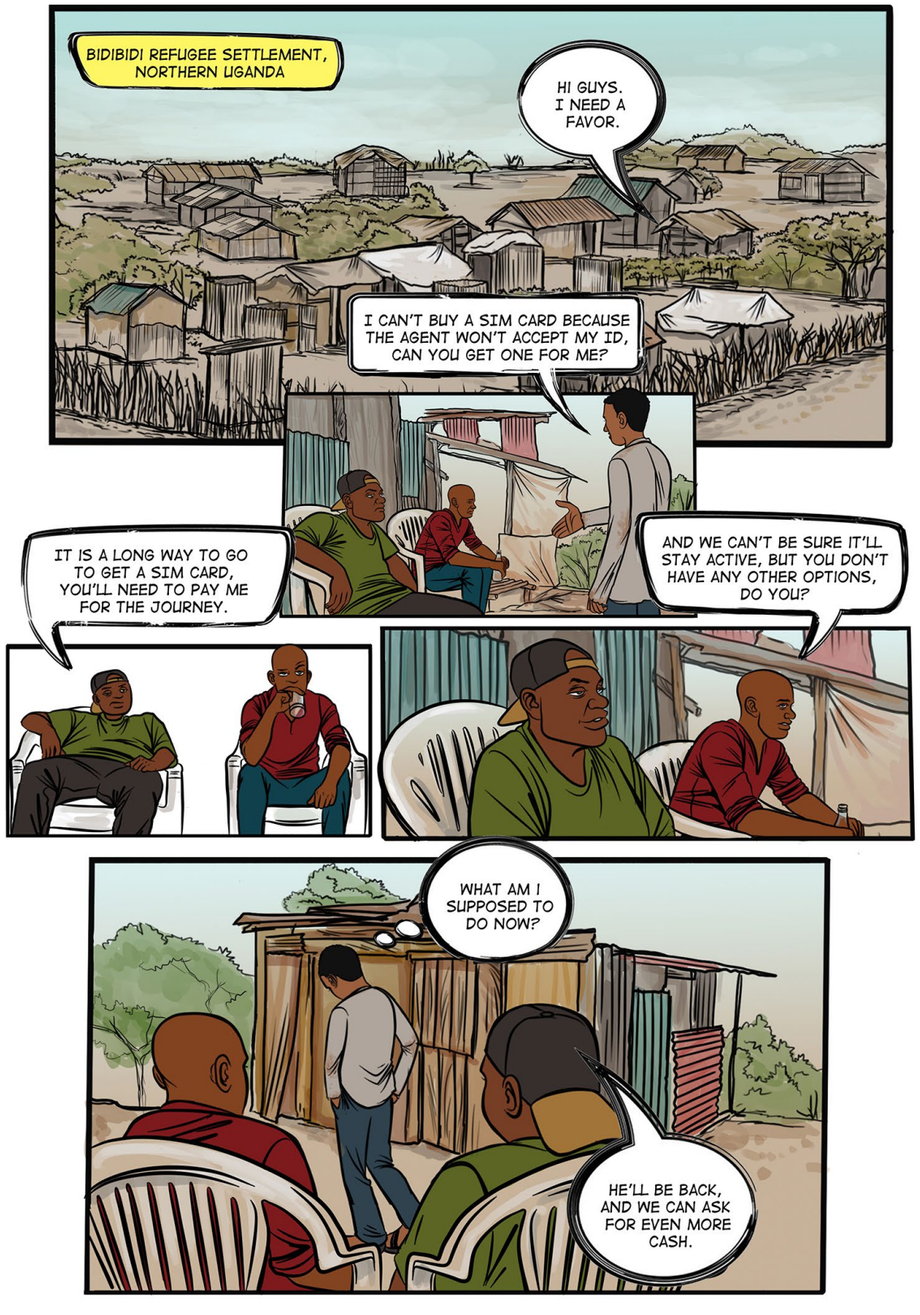
SECTION 3: ANALYSIS AND FINDINGS / ON REAL-WORLD IMPACTS

II. Real-world impacts of policy - where frameworks exclude access, workarounds - put people at risk

It was clear from the discussions that government policies around telecommunications access (e.g. SIM registration and different forms of digital taxation) have had a profound impact on refugees' lives. Many had built facets of their daily or weekly routine around specific aspects of policy, whether an economic barrier to circumnavigate or a lack of legal pathway to access, leading to time-consuming and sometimes cumbersome workarounds. While progress has been made in Uganda in the area of SIM registration,[103] it is still difficult for people in both Uganda and Kenya to legally access connectivity. Many have SIM cards registered in others' names—whether a friend or an unknown person—resulting in precarious access to digital and financial services. Some users have to pay continuously for the use of workarounds. As much as these policy barriers may deter some individuals from accessing community, as a whole, they do not stop communities from finding ways to access telecommunications services. They do, however, add another layer of vulnerability (economic, legal or otherwise) to people's day-to-day lives. This goes to show that small modifications to the policy frameworks governing access to telecommunications may have a significant impact on people's day-to-day lives.

> *Not being able to register a SIM card in our own name puts us at risk. We rely on others, and if they do something wrong we can be held responsible. This happened once to me, and I received phone calls about crimes that the person [whose name was registered against the mobile number] had committed.*

103 UNHCR (2019). UNHCR welcomes Uganda Communications Commission directive to improve refugees' access to SIM cards: https://www.unhcr.org/afr/news/press/2019/8/5d5ba4274/unhcr-welcomes-uganda-communications-commission-directive-to-improve-refugees.html



@Noah Mukono

III. Online fraud and scams are widespread among participants.

Across the board, a majority of participants had been targeted or victims of a mobile money fraud or scam. Commonly, users receive SMS messages or phone calls relating to receiving sums of money if they transfer a smaller amount to an unknown recipient, among other types of transactional fraud. Many had fallen victim to such scams. In terms of response measures, users said they would not go to the police. Rather, they preferred to go directly to MNOs. UNHCR noted this would be an important consideration to take into account as part of its Cash-based Intervention work. Another commonly experienced scam involved resettlement or visa offers. Interviewees noted that these were commonly shared or advertised through social media, highlighting the need for the humanitarian community to engage with different social media companies in order to ensure vigilance and timely removal.

> *Some [resettlement] scammers pretend they are from UNHCR. Usually we can tell, but UNHCR needs to try and stop this.*

IV. Serious protection incidents in the physical world are increasingly likely to have a digital dimension to them.

At numerous junctures in the discussions, anecdotes were given that highlighted how refugees' online activity and digital access may increase the risk of a serious protection incident taking place. These concerns were less about the possibilities of high-tech surveillance, for instance the interception of one's communications by a government and instead focused more on the misuse or misappropriation of social media content. A common concern that was raised was how one's posts or activities on social media in the host country might somehow be used to put one's family or friends in their country of origin at risk. Risks that may be exacerbated by the digital environment include kidnapping, physical violence and abuse (including sexual and gender-based violence) and further flight.

> *In some of the scams there are threats of physical violence. Whenever there's a scam and they want to meet somewhere it's often because they're looking to rob you.*

Findings on Humanitarian Intervention

These findings account for the role of UNHCR, other humanitarian organizations, and connectivity partners both in providing connectivity as aid and raising the bar in terms of digital risk management.

I. Where communal connectivity is provided, suboptimal security practices are commonplace.

Whether using a personal device or a laptop (most commonly a shared laptop), a number of suboptimal security practices were identified at community connectivity centers, despite the presence of 'security rules' posted in many locations. Frequently, users would share devices without taking care to log themselves out of social media or email accounts. Often, due to the small number of laptops available to users in connectivity centers, many would gather around one device, thus increasing the likelihood of personal information (including login credentials) being misused. Yet, interviewees generally seemed trustworthy of fellow users, which reflects a different conception of threats in context. Some good practices existed: for instance, at the community center in Kampala, the computers were running a Linux variant that deleted all local files after use (many users were previously storing private files locally on shared computers).

> *We see a lot of users at the center leaving their accounts open and logged in. We're receiving an increasing number of requests from community members to help them improve their digital skills, like showing them how to sign off securely and keep their details private.*

II. Communities lack information on digital risks.

Despite being relatively well informed themselves, participants (who had been sought out for their frequent use of connectivity) continually noted a lack of information in their communities around the risks under discussion. Many provide support and advice to friends and family on an as-needed basis (i.e. usually when a problem arises), but the lack of systematic information provision from MNOs, technology companies or the humanitarian community means many users lack knowledge and information. This is particularly the case for the most vulnerable who are less likely to be sufficiently digitally literate to understand more nuanced aspects around digital risks. While some digital risk management guidance is shared at certain connectivity centers, this is not always widely consumed or practiced, nor does this standard guidance translate directly into the mobile environment.

> *We need to provide more information to people about how to stay safe online. Refugees need to know that if their data falls into the wrong hands it can cause them a lot of problems.*

III. Threat models are relatively sophisticated, but may benefit from additional information about the range of existing cyber threats.

Interviewees were relatively well informed about the threat actors that may seek to monitor or disrupt their communications online (including their use of social media), particularly state actors from their home countries. However, there appeared to be less of an appreciation of the local and more mundane threats that may introduce digital risks, e.g. not logging out of one's email or social media account on a shared computer or the possibility of mobile money agents defrauding customers.

> *We need more awareness among communities about hackers. There are many who don't know about them and some who do but don't know how to avoid them or take care of themselves.*

IV. Communities, particularly youth, are eager to support humanitarian organizations in minimizing digital risk and have a key role to play in building the knowledge and skills of their peers.

Young people were eager to be empowered by humanitarian organizations like UNHCR to lead local efforts to raise awareness of digital risks and improve skills of community members, particularly older people. A targeted recommendation on how to support such initiatives follows in the next section.

> *We want to give back to the community with the knowledge we have. We see older people, not having been to school, not knowing how to use mobile money and doing things like sharing their PINs. We want to help these people understand.*

Phone and internet brin Tom Remo, a South Sudanese refugee and businessman at his mobile phone shop at Rhino Camp Settlement, northern Uganda, where internet connectivity is changing lives. © UNHCR/Michele Sibiloni

Context-Specific Findings

Last, a final set of findings explores findings that were specific to the refugee contexts and national policy settings.

I. Context-specific needs and risks must be weighed when conceiving of mitigation measures.

Respondents were clear that other connectivity-related needs are also important to their communities. Access to reliable and affordable connectivity was a repeated point of concern among interviewees, particularly in remote areas. Likewise, in the settlements in particular, the lack of electricity makes charging devices challenging. While these are important concerns in and of themselves, it is important to note that they also introduce security and privacy risks, for example when people seek out forms of connectivity that may be unsafe (e.g untrusted wireless access points at petrol stations, for example) or when they leave their devices unattended at communal charging stations.

> *Sometimes we are desperate for WiFi, so we connect to the open network at the petrol station. It's probably not safe but there are times when you just want to get online.*

II. Uganda's digital tax regime encourages VPN usage with unclear implications for digital risk.

In Uganda, a social media tax (known as the OTT tax) was implemented in 2018 that requires users to pay a levy if they want to use a social media service. These services are some of the most commonly used in Uganda and the tax has impacted virtually all of the individuals spoken to in discussion. Some users find workarounds by downloading VPNs, while others are willing to pay the tax. VPNs were commonly said to consume significant amounts of data and battery charge from devices. The VPNs used by refugees were generally freeware from the Android Play app store. Given these findings, we suspect that many of the different VPNs being used contain malware or other undesirable code that may present different risks (for instance, apps that covertly mine bitcoin), even though VPN use is generally thought of as a good security practice.

> *When I use my VPN it uses a lot of data and it also drains my phone battery. I'm not sure why. Because of this I sometimes choose to pay the OTT.*

III. Kenya's SIM registration policy regime continues to frustrate refugee connectivity efforts.

In Kenya, there was robust discussion on matters of SIM registration. There was inconsistency in the application of SIM registration rules with different credentials (depending when they were issued) Some users benefit from differing validity periods depending on when the SIM card was registered. It was highlighted that there was a difference among the operators in their approaches, with more thorough checks being undertaken by certain operators and less rigorous procedures by others.

> *I once had a call from scammers pretending to be from Safaricom customer care. They said that the line was double registered and they wanted us to go to the office to remove a line. They then ask for a code sent to your mobile, but actually they're fraudulently recovering your account and hacking the two-factor authentication. I learnt from others it's an elaborate and sophisticated scam and they're targeting those that don't have a SIM card in their own name.*

Recommendations

This section draws from the above findings to put forward three sets of recommendations concerning digital risk management in the refugee connectivity context. The first set of recommendations addresses actions that humanitarian organizations can take to help refugees better protect themselves online. The second set is focused on pathways for the private sector to engage the humanitarian community in furtherance of these goals. The third set is aimed at the research community interested in further investigating the topics of refugee connectivity and digital risk.

Recommendations to Humanitarian Organizations

In advancement of improved digital risk management for refugee connectivity, humanitarian organizations should:

1. **Work with community organizations to develop tailored awareness and training campaigns based on the local context:**
   During the research, it was observed that in many cases, connectivity centers operated by community organizations already disseminate information on how to practice good security and privacy online, usually in the form of printed notices posted in communal areas. This is a good start, but more engaging forms of awareness raising (e.g. videos or social media campaigns, or over SMS channels for those without access to the Internet) may be better at informing users about evolving cyber threats and risks. A broader range of digital risks - including those associated with online disinformation - could also be addressed in these campaigns. Crucially, community connectivity centers offer spaces in which technical information about digital risks could be translated into actionable guidance, particularly in the mobile environment. Humanitarian organizations should closely engage these groups during the rollout of any digital risk awareness or training initiative targeted at refugees.

2. **Empower early adopters in displacement contexts to support digital risk management:**
   In line with the previous recommendation, it was discovered that tech savvy refugees are well positioned to help lead local efforts around refugee digital risk management. In many cases, these will be young people who more closely track digital innovation and are familiar with the risks of new technology. Their understanding of technological advancements, especially in the mobile domain, would be helpful in sharing good practices among community members, especially older community members. Supporting these individuals through formal certifications and financial rewards would help create additional incentives for community engagement.

3. **Sponsor information security knowledge exchanges:**
   While community organizations and tech savvy refugees are essential to improved awareness and mitigation of digital risks, there may be value in creating short-term knowledge exchanges between digital risk specialists and community organizations to stay apace with technological developments. For example, humanitarian organizations could set up an exchange program that would bring external experts to refugee contexts in order to help communities learn about emerging digital risks or the technological state of the art in terms of risk mitigation. Vice-versa, tech-savvy refugees can be invited to learn from humanitarian action in this space and alongside technology partners. While such exchanges may be challenging to organize in-person during COVID-19 lockdowns, humanitarian organizations could explore ways of facilitating virtual exchanges until site visits are again possible.

Matthew Lubari (centre), 26, volunteers at the Community Technology Empowerment Network centre at Rhino Camp Settlement, teaching digital skills to fellow refugees and locals who dream of careers as scientists, engineers and doctors. © UNHCR/Michele Sibiloni

4. **Better police fraudulent activity targeting persons of concern:**
   The research identified different types of online fraud in which refugees are specifically targeted. The first is financial fraud related to humanitarian cash assistance, which is increasingly delivered via mobile money or other digital channels. In these scenarios, scammers attempt to divert funds through a variety of cons. The second involves online resettlement-related scams in which refugees are tricked into paying for resettlement services which in fact do not exist. Both humanitarian organizations and governments of countries receiving resettled refugees could do more to stay abreast of such fraudulent offers and the actors involved, and redouble efforts to crack down on malicious activity. Increased collaboration across the humanitarian sector to address such misconduct, for example through better information sharing between agencies and with communities, and coordinated efforts to dismantle identified scams, would serve to reduce risks to affected persons.

@NoahMukono

5. **Partner with the third and private sectors for increased effectiveness and scale:**
   Across each of the four previous recommendations, there are opportunities for strategic engagement with actors from both the third[104] and private sectors to help increase the positive impacts of different initiatives. For example, in-country civil society organizations focused on digital rights issues could be engaged to help refine and deliver digital risk training and awareness alongside local community organizations and governments can consider leveraging the reach of local MNOs to extend public awareness campaigns. Expertise from the private sector could inform knowledge exchanges or help address fraud targeting refugees on digital platforms. Working in partnership with such organizations will help ensure that digital risk mitigation efforts are more effective and achieve greater scale. It is also possible to build on existing initiatives such as the cybersecurity bootcamp aimed at refugees which was recently launched in the region.[105]

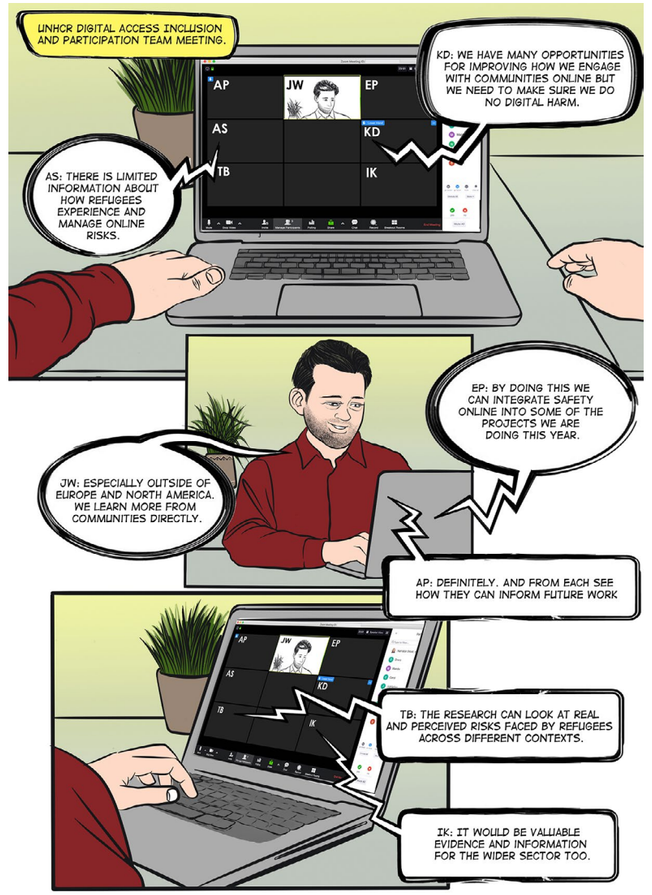
6. **Engage with government authorities and local security officials on threats facing refugees:**
   Humanitarian organizations could develop closer ties with local authorities to facilitate the greater sharing of information at an operational level to attain improved situation awareness of cyber threats affecting refugee populations. This information may address primarily offline threats which could potentially include a cyber threat component, or it could consist of so-called cyber threat intelligence regarding actors mainly targeting refugees online. The maturity and sophistication of any such operational relationships between host governments and humanitarian organizations will very much depend on the specifics of the local context.

7. **Advocate for the inclusion of refugee digital protection into national strategies on trust and security:**
   Where countries are developing national strategies that address trust and security online, including in national digital economy and cybersecurity strategies and increasingly through policy measures to address disinformation and misinformation, humanitarian organizations should actively promote the inclusion of refugee digital protection issues and priorities in host government strategies. This may require close engagement with a range of government bodies depending on the configuration of the national policy-making apparatus.

104 What is the third sector and what does it do? http://toolkit.northernbridge.ac.uk/engagingwithpolicymakers/engagingwiththethirdsector/whatisthethirdsectorandwhatdoesitdo/

105 Jake Epstein (2020). Israeli startup Cybint equips African refugees with cybersecurity skills:https://www.timesofisrael.com/israeli-startup-cybint-equips-african-refugees-with-cybersecurity-skills/

8. **Sponsor further research on relevant topics:**
   Finally, humanitarian organizations can deepen the evidence base on the critical topics of refugee connectivity and digital risk by sponsoring further empirical research in this area. There is a clear need to conduct similar research in other displacement contexts and regions to understand both similarities and differences with the current case. Critically, humanitarian organizations should support future research that includes an explicit focus on how age, gender and disability dynamics[106] shape perceptions of digital risk in connectivity contents. There is also a need to broaden out research approaches and questions to focus on a wider range of topics related to refugee digital protection. Some specific ideas for a future research agenda are developed later in this section.



@NoahMukono

106 GSMA (2020). Human-centred design in humanitarian settings: Methodologies for inclusivity: https://www.gsma.com/mobilefordevelopment/resources/human-centred-design-in-humanitarian-settings/

Recommendations to the Private Sector

Recognizing that the private sector plays a central role in the provision of connectivity to refugees, and in light of the UN Secretary General's Roadmap for Digital Cooperation[107] which highlights the importance of the private sector's involvement in developing inclusive, trustworthy and secure digital economies and societies, there are a number of actions that industry can take to help ensure refugee protection in the digital domain:

1. **Engage more closely with community organizations on digital risk identification and mitigation:**
   For technology providers servicing connectivity centers that are operated locally by community organizations—a common feature in the contexts studied—it was observed that in many cases, day-to-day decisions about network security configurations or blocked content were handled remotely by the private sector partner with minimal to no involvement by the local partner. Not only is this a source of frustration among local actors who often feel that they do not have sufficient control over the connections they help facilitate, it is also a missed opportunity to make better risk management decisions informed by the specificities of the local connectivity context. Technology partners could help empower community organizations by providing them with greater autonomy over day-to-day network management decisions.

2. **Build better security into humanitarian technology offerings:**
   A diversity of digital technologies and offerings have been proposed or developed over recent years to facilitate refugee connectivity, particularly in the mobile environment. These include specialized apps,[108] mobile service offerings targeted at refugees,[109] and zero-rated connections and content tailored to refugee communities.[110]

107 Secretary General's Roadmap for Digital Cooperation: https://www.un.org/en/content/digital-cooperation-roadmap/
108 See, for example: http://appsforrefugees.com/
109 See, for example, the proposal regarding the "deployment of a mobile offering for all refugees in need" in France's 2020 strategy for the digital inclusion of refugees: https://accueil-integration-refugies.fr/2020/09/16/inclusion-numerique-des-personnes-refugiees-la-diair-met-en-place-une-strategie-de-lutte-contre-la-fracture-numerique-pour-les-personnes-refugiees/
110 See, for example, the Praekelt Foundation Incubator for Free Basics https://www.praekelt.org/workfreebasicslearnmore

Without assessing the viability or sustainability of these various efforts, it is incumbent that developers build security features such as encryption into these tools and services to raise the baseline for refugee digital protection. In other cases, security gains for refugee connectivity will come not from interventions targeted at refugees, but instead, in the general uplift of widely used technologies and services, such as security improvements to popular mobile operating systems (e.g. Android) and in particular those running on low-end devices.

3. **Consider extending digital security initiatives to include a refugee focus:**
   Certain App stores have recently announced initiatives to extend efforts to help identify scammy and malicious apps before they are published and potentially do harm to users.[111] There is an opportunity to leverage these efforts to better police bad apps that are commonly encountered among refugee users or which are popular in displacement contexts by working closely with organizations like UNHCR to understand refugee experiences in the mobile environment and with apps in particular. Similarly, the relaxation of controls on 'sideloading' apps or the opening up of app stores[112] may have unintended security consequences for certain users, including refugees. These could be better understood and anticipated through closer engagement with humanitarian actors and refugee groups.

4. **Amplify humanitarian efforts to shape the digital policy environment:**
   The private sector is uniquely situated to share its perspectives with government authorities regarding the unanticipated consequences of digital policy interventions and to advocate on behalf of policies for greater digital refugee protection. For example, the mobile industry has been instrumental in raising policy makers' awareness of the implications of customer identification requirements for refugee access to mobile connectivity, and have advocated for new systems that facilitate access in privacy-sensitive ways.[113] This research has uncovered other policy areas, specifically in the area of digital taxation, which might unintentionally introduce digital risk into everyday connectivity practices, namely through the use of free VPNs that potentially include malicious code. Private sector actors should help policy makers understand how these interventions affect the digital risk landscape and work collaboratively for better policies.

111 Jay Peters (2019). Google teams up with security companies to catch bad apps before they hit the Play Store: https://www.theverge.com/2019/11/6/20952333/google-android-app-defense-alliance-eset-lookout-zimperium-bad-apps-play-store
112 Adi Robertson (2020). Google says Android 12 will make using third-party app stores easier: https://www.theverge.com/2020/9/28/21472139/google-android-12-app-store-installation-payment-fees
113 GSMA (2020). Proportionate regulation in Uganda: A gateway for refugees accessing mobile services in their own name: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Uganda_Case_Study_Web_Spreads.pdf

Recommendations to Researchers

Finally, this research represents a modest step in the development of a stronger evidence base with which to inform protection efforts in the area of refugee connectivity. We call upon the research community interested in these topics to take up the mantle by considering future investigations across the following dimensions:

1. **Explore additional research sites and use contexts:**
   It is incumbent to examine the intersection of refugee connectivity and digital protection in other displacement contexts and among other users. While this research has aimed to move the focus from European and North American settings, where most research has taken place to date, to displacement contexts in Uganda and Kenya, these are by no means the only areas where digital risks are present. Beyond conducting similar research as this study in settlements and camps in other countries, investigators may want to look at specific digital risks that emerge at borders, for example, where mobile data may be used by authorities to monitor refugee movements or assess asylum claims.[114] Another site for potential ethnographic work are the charging stations that are essential to meet the energy needs of connectivity users in camps and settlements - in particular, it is worth exploring local power dynamics (gendered or otherwise) at these sites and how they shape the risk landscape.

Young South Sudanese refugees charge their mobile phones at the Community Technology Empowerment Network centre at Rhino Camp, Uganda © UNHCR/Michele Sibiloni

114 See, for example: Amar Toor (2017). Germany moves to seize phone and laptop data from people seeking asylum: https://www.theverge.com/2017/3/3/14803852/germany-refugee-phone-data-law-privacy

2. **Tackle emerging questions inspired by this exploratory research:**
   Researchers should also explore new questions than those pursued in this report. While this study has focused on exploratory research questions meant to better understand a broad range of digital risks within refugee connectivity, future research could look more closely at some of the issues that were uncovered. For example, future research should hone in on how gender dynamics shape perceptions of digital risk, the specific experiences of LGBTI people, disability considerations, specific concerns about how sexual and gender-based violence intersects with digital connectivity, and/or the use of digital technology by children.[115] To take a different approach, it may also be worth exploring whether there is a correlation between digital taxation in countries pursuing such measures and rates of access to/use of connectivity services by refugees.

Celebrating the third anniversary of UNHCR's #IBelong campaign, Kenya. © UNHCR/Nathan Siegel

3. **Leverage a range of qualitative, quantitative and interdisciplinary methods:**
   Lastly, it may also be worthwhile to use different methods to assess the extent of digital risks facing refugees in their use of connectivity. For example, where VPNs are commonly used, researchers could systematically survey users to understand the most popular VPN applications and analyze their security dimensions and shortcomings. Such research would likely require an interdisciplinary collaboration between social and computer scientists. The prospects for such collaborative undertakings to better document and mitigate digital risks in refugee's use of connectivity are exciting. In some cases, this research could be refugee-led and would benefit from their lived experiences.

115 Cf. Save the Children (2020). Digital Safeguarding for Migrating and Displaced Children: An overview of the current context and trends, potential risks and practical next steps https://resourcecentre.savethechildren.net/library/digital-safeguarding-migrating-and-displaced-children-overview-current-context-and-trends

Concluding Remarks

As the UN Secretary General observes in the 2020 Roadmap for Digital Cooperation,

"over the past few years, important efforts have been under way to address the rising threats to the online world. The initiatives have helped to bring about important progress for multi-stakeholder engagement, in the area of digital trust and security. However, these efforts are not yet universal, and their reach, though broad in some cases, does not yet cover large swathes of the world."[116]

The concerns of refugees and other forcibly displaced persons should be incorporated into ongoing efforts to manage digital risks. As this research has demonstrated, refugees' experiences and perspectives of digital risk are unique, but their digital protection needs are still unmet. UNHCR is committed to help advance this critical discussion through targeted interventions, particularly in the realm of refugee connectivity, as well as through increased engagement with key partners.

116 Secretary General's Roadmap for Digital Cooperation, p. 20: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

Annex 1: Explanatory Note on Methods

This note explains some of the key methodological decisions that were taken during the research.

While the research team had planned to record all of the interviews, it was observed during the first meeting that the presence of the audio recorder was alienating for certain interviewees, potentially due to the sensitive subject matter. It was then decided to discontinue the use of the recorder and instead designate a member of the team to manually transcribe notes. Moreover, the interview guide was adjusted after the first focus group interview to revise certain terms to make them more accessible.

Despite attempts to organize group discussions with only female participants, we were unable to achieve gender segregated groups. This would have made for more conducive discussions on risks such as sexual and gender-based violence. This shortcoming should be improved on in future research.

It was decided in the planning stages of the research that we would not interview children regarding their use of connectivity as doing so raises additional ethical and safety considerations.

The research made considerable efforts to ensure that participants were informed that their participation was entirely voluntary, that there was no direct benefit from participation in the research, and that risks from participation were unlikely. Participants were told that they could refuse to answer any question, and could choose to withdraw from the discussion at any time without penalty. Anonymity for all participants was assured. Annex 2 explains the consent procedure in further details.

Annex 2: Interview Consent Procedure

The following information was delivered verbally at the start of each interview. Consent was also obtained verbally.

Please consider this information carefully before deciding whether to participate in the research.

1. **Purpose of the research:** To understand the experiences of refugees in their use of mobile phones, specifically with respect to cybersecurity and privacy concerns.

2. **What you will do in this research:** If you decide to volunteer, you will be asked to participate in an interview. You will be asked several questions about your use of mobile devices and the Internet, what threats and risks you perceive when connecting online, and how you protect yourself. With your permission, we will manually record notes from the discussion. You will not be asked to state your name for the record.

3. **Time required:** The interview will take approximately 1 hour.

4. **Risks:** While we have done my best to avoid sensitive topics, it is possible that some of the questions may cause discomfort or embarrassment. You are not obliged to answer any questions that make you uncomfortable.

5. **Benefits:** This is a chance for you to tell your story about your experiences in using a mobile device and the Internet to connect with others and to access important information, as well as how you go about protecting yourself and your information in the process.

6. **Confidentiality:** Your responses to interview questions will be kept confidential. At no time will your actual identity be revealed. The information you provide will be used for a report for UNHCR and may be used as the basis for articles or presentations in the future. We will not use your name or information that would identify you in any publications or presentations.

Uganda. Phone and internet brings advancement in isolated northern settlements © UNHCR/Michele Sibiloni

7. **Participation and withdrawal:** Your participation in this study is completely voluntary, and you may refuse to participate or withdraw from the study without penalty or loss of benefits to which you may otherwise be entitled. You may withdraw by informing the researcher that you no longer wish to participate (no questions will be asked). You may skip any question during the interview, but continue to participate in the rest of the study.

8. **Agreement:** Do you believe that the nature and purpose of this research have been sufficiently explained to you? Do you agree to participate in this study?

Annex 3: Interview Questions

Note that the interviews that were undertaken were designed to be semi-structured and open to dynamic dialogue. The following questions are only indicative of the conversations that took place.

I. Introductions and consent procedure

II. Device ownership and connectivity

- Do you own a mobile phone?
- Where do people buy their mobile devices?
- Do you share your phone with anyone else? Do you use other people's phones?
- Which networks do you have SIM cards for?
- Do you trust the operator(s)?
- Where did you register your SIM card? What information did you have to provide when you registered?
- Do you use laptops / computers? In a community center?
- Do you think these laptops are safe to use? Has anything ever happened?
- What apps do you use on your mobile?
- Do you have an email account? Is it Gmail?
- How often do you change email? Have you ever forgotten your password?
- Do you use social media?

III. Social media

- Do you ever feel unsafe online? Using social media?
- What are you worried about when you are online?
- Do you trust Google, Facebook, etc.?
- Are you worried about the government where you come from looking at your information? What about your host government?
- How do you stay safe online?
- How do you learn about staying safe?
- Do you teach your friends or family?

IV. Incidents

- Has your account ever been hacked?
- Did you recover your password? Did you use your phone or email?
- Has this happened to your friends or family? In what ways?
- Have you had people trying to get money from you over mobile money?
- What did you do? Who did you go to? Did the police do anything?
- Are you aware of any other problems due to connecting to the Internet?

V. Context-specific questions

- Do you pay OTT?
- Do you use a VPN?
- How did you learn about this?
- Are there problems with it?
- How many have you had?

VI. Role of UNHCR and others

- Do you think UNHCR can do anything to help with these problems?
- What can they do?
- Do you think people would trust information coming from UNHCR?
- Have you used the helpline?
- Do you trust UNHCR with your data when you access connectivity or other services?


UNHCR
UNHCR Innovation Service
Connect
@unhcrinnovation
UNHCR Innovation
innovation@unhcr.org