UNHCR
The UN Refugee Agency

Connecting with Confidence

Literature Review

Digital Access, Inclusion and Participation

UNHCR
Innovation
Service

Connecting with Confidence

Literature Review

Made possible thanks to
the generous support of:

LUXEMBOURG AID & DEVELOPMENT

UNHCR
The UN Refugee Agency

UNHCR Innovation Service
Digital Access, Inclusion and Participation

Web edition March 2020

About this report and acknowledgements

This report has been commissioned by UNHCR and is authored by Tina Bouffet. It is part of a broader workstream of UNHCR's Digital Access, Inclusion, and Participation Programme around the safety of forcibly displaced persons when accessing or utilising connectivity services. Specifically, this literature review is a pre-cursor to a broader report to be launched in 2020 titled 'Connecting with Confidence' that explores dynamics around refugee safety when accessing and utilising connectivity services following field research undertaken in late 2019.

The author would like to acknowledge Katie Drew and John Warnes from UNHCR; Aaron Martin of the University of Tilburg; and Silvia Pelucchi from the International Committee of the Red Cross for their support and contributions.

Introduction

Various 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 (Willitts-King et al., 2019; Read et al., 2016; Meier, 2015). Volunteers used SMS and social media to crowd-map the response, monitor the situation and share potentially life-saving information with affected people (Meier, 2015).

Since then, different actors have consistently written 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 of the humanitarian response. This review will focus on connectivity as aid, i.e. the use of connectivity by humanitarians to engage with affected people.

Specifically, the review focuses on the means, barriers, and associated cybersecurity and privacy concerns that refugees face around connectivity. This includes but is not limited to mobile connectivity and social media, particularly in displacement contexts. While these subjects may at times intersect with parallel conversations on digital identity or biometrics, the latter are not the focus of this chapter. UNHCR provides support and international protection to forcibly displaced persons, including refugees, returnees, stateless people, the internally displaced and asylum-seekers. This report will reference 'refugees' and this can be read broadly to encompass refugees and other persons of concern, unless explicity stated otherwise.

This literature review is divided into different sub-themes. An annex also provides a brief overview of who are the main actors writing about connectivity in humanitarian contexts, and with what angles and / or interests.

Thematic literature review

Means to connect

The means that refugees use to connect has mostly been monitored by service providers operating in displacement contexts, or trade bodies of which they are a part (namely, the GSM Association). Globally speaking, mobile adoption continues to be on the rise, including in countries that contribute to outflows of refugees, transit countries and destination countries (GSMA, 2019a). In 2011, a needs assessment in Kenya's Dadaab refugee camp had found that "new ICTs, including mobile phones [...] are on the rise [...] registering below 20% among long-term residents and around 10% for new arrivals" (Internews, 2011: 19). Less than a decade later, in 2019, the GSM Association's report on the digital lives of refugees found that over two-thirds of refugees in the selected research locations (Jordan, Rwanda and Uganda) 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 (GSMA, 2019d).

Case studies indicate that connectivity usage rates may vary across displacement contexts and among respondent groups (for more on technology and connectivity divides, cf. **Connectivity divides**). In a refugee camp in Greece, Latonero et al. found that 94% of all 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 (2018: 5). 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 SIMs (GSMA, 2019d). 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 (Samuel Hall, 2018).

The type of device owned also varies across contexts, and has significant implications in terms of access to app-sustained services and data protection. 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 (Ibid: 14). These smartphone ownership rates contrast heavily with those found by Latonero et al. in Greece, where the overwhelming majority of mobile phone users had a phone that supported messaging apps and internet applications (2018: 5). This contrast has implications for the broader validity of research done on refugee connectivity. Indeed, much of the research cited in this review focuses on European refugee contexts, who primarily host Syrian refugees. However, the latter's ICT access and practices differ significantly from those of displaced persons in sub-Saharan Africa, for whom information is much more limited.

Moreover, even where refugees are able to obtain smartphones, these are likely to be older-generation Android devices (ICRC and Privacy International, 2018: 104). This has implications on the level of data security these devices can guarantee; or the level of

software support and patching available in order to keep certain applications and their related services available (Ibid). 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 (GSMA, 2019d). It can also be conditioned by their ability to meet or circumvent legal barriers conditioning mobile access (for more on this, cf. **Regulatory barriers and restrictions**).

Finally, connectivity can also be accessed in specific communal locations – such as internet cafés, community centers, etc. 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 (see Samuel Hall, 2018: 23 or 'Access to Technology' in Culberston et al., 2019). 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. (Ibid).

Connectivity divides

At first, connectivity was seen as a phenomenon with the power to act as a "potential equalizer" in society (Compaine, 2001). However, this optimism was quickly and repeatedly called into question as technology was shown to be a replicator, if not amplifier, of social inequalities (see Hargittai, 2003; Hargittai, 2008; or Schradie, 2013). 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 (Willitts-King et al., 2019), with some even alleging that despite these efforts, the coverage of needs by the humanitarian sector was deteriorating (ALNAP, 2018).

Connectivity divides predominantly align with gender lines, socioeconomic divides, differentiated access to education, disability or a combination of these (Willitts-King et al., 2019; GSMA, 2019e). They can also be exacerbated by factors such as geographical location and age (Willitts-King et al., 2019; Samuel Hall, 2018), or biases built into technologies themselves – for instance, the difficulties that facial recognition software might have recognising diverse datasets of faces (ICRC and Privacy International, 2018); or the trouble that automated mapping technologies have recognising houses in crisis-affected areas (Willitts-King et al., 2019).

Among refugee populations, connectivity divides have impacted everything from the ability to travel safely (Samuel Hall, 2018), to accessing mobile money (GSMA, 2019d), connecting with family and friends, or safeguarding mental health (Latonero et al., 2018). 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 ownership and consent around the use of their data (Alam and Imran, 2015; Crabtree and Geara, 2018). 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 (UNHCR, 2016).

Finally, 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.

Regulatory barriers and restrictions

"Proof of identity" and other mobile registration barriers

Over the past decade, a growing number of governments have conditioned mobile and internet connectivity to registration and proof-of-identity processes (GSMA, 2018b). These policies place an estimated 1.1 billion people who lack recognised identification at risk of digital, social and financial exclusion. Among them are a number of refugees and displaced persons 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 (Ibid; UNHCR, 2019).

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, see Ibid: 14). 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 proof-of-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 or Kenya (UNHCR, 2016). This puts a number of individuals at risk of seeing their mobile services – and the support network that came with it – disconnected.

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 digital scans of a person's credentials (see GSMA, 2018b; UNHCR, 2019; or UNHCR, 2016). This complex and evolving shift can have real repercussions for refugees as the documentation they hold – if any – may not be eligible for registration in a centralised database. This was the case in Uganda, where only refugee ID cards were accepted as a form of identification to access SIM cards. Fortunately, new guidance has been issued, widening accepted forms of identification to other registration documents

or attestation letters (UNHCR, 2019b). Here, humanitarian organisations can play a pivotal role in the advocacy and research towards more inclusive and accessible registration processes.

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 programme). Financial service providers must comply with "Know-Your-Customer" (KYC) requirements, even where there is a humanitarian organisation acting as an intermediary (GMSA, 2018b). 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. The sharing of KYC data across different actors in the financial sector can also reversely lead to the financial exclusion or discrimination of individuals who have received humanitarian aid (ICRC and Privacy international, 2018).

Finally, there are cases in host countries deliberately restrict mobile access for refugees located on their territory. The most famous 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 (see McVeigh, 2019; or Islam, 2019).

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 (Dekker et al., 2018). Indeed, while a number of authors had confirmed refugees' awareness of digital surveillance and digital border control (from Dijstelbloem and Meijer, 2009 to Wall et al., 2017), Dekker et al. additionally mentioned strategies that refugees had developed to circumvent these – namely, cutting the Wi-Fi signal or turning off the smartphone. However, turning off a smartphone does not necessarily mean that all forms of geo-localisation 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). As such, fear of surveillance or lack of security may influence certain individuals' mobile or internet user behaviour, 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 (Yandell, 2016). 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.

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 (Ratcliffe and Okiror, 2019) – or at least, abandoning access to them from a mobile platform. 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 that the "Over the Top" (OTT) tax sought to prevent online gossip (Ibid). 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.

Connectivity among refugees

The broader role of ICT 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 (Leurs and Smets, 2018). 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 (Ibid).

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 70 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 (Elias and Lemish, 2009). More recently, drawing from interviews with more than 50 resettled refugees on their use of ICT in host countries, Andrade and Doolin (2016) highlighted five key capabilities that connectivity offered in favour of refugees' social inclusion: participation in an information society, effective communication, an understanding of the new society, social connection and cultural expression. 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 (Marlowe, 2019). 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 (Brown et al., 2019; SINGA France, 2014; Simco et al. 2018).

Connectivity also plays a key role for refugees during their flight. In 2018, Alencar et al. defined the 'refugee smartphone' as a companion, an organisational hub, a lifeline and a diversion (Alencar et al., 2018). 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 (Ibid; GSMA, 2019d). Mobile connectivity also means access to mobile enabled utilities, namely mobile money – including person to person transfers, airtime top-up and international remittances (Ibid). 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 (Dekker et al., 2018; Lloyd et al., 2013). In other words, to validate the information they find online, refugees use various strategies with links to the analog world.

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 organisations, 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 (Benton and Glennie, 2016; Brown et al., 2019). 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 (Rahman, 2019); Vodafone-supported mPower Youth uses mobile technology to advance children's rights by providing power, internet and IT material to refugee camps (Okuoro, 2019). 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 (Benton and Glennie, 2016; Brown et al., 2019).

Meanwhile, humanitarian organisations 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 programmes; 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 (Patil, 2019; UN Innovation network, 2019; Brown et al., 2019).

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 organisations (see comments in Wilton Park, 2019). 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 favour 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 (Willitts-King et al., 2019). These and other cybersecurity and privacy concerns arising from the use of connectivity in humanitarian contexts – and particularly with refugees – are further explored below.

Privacy concerns

Perceived threats and vulnerabilities

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 mobile and internet 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 (ICRC and Privacy International, 2018). Moreover, refugees themselves might not always be up to date or aware of data protection measures for online and mobile security (SINGA, 2014). Depending on the jurisdiction they find themselves in, or the access that they have granted to apps on their phone, 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 (ICRC and Privacy International, 2018; SINGA, 2014).[1]

This may expose refugees to identification and surveillance by the country they are fleeing (with possible persecution or retaliation against their peers back home). It can also allow 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 deport them (for instance, to the first safe country of transit as stipulated by the EU Dublin regulations) or to deny their asylum request on the grounds of demonstrated involvement with smuggling networks (SINGA, 2014; Jumbert et al., 2018; Privacy International, 2019).

While less specific to connectivity, the use of biometric registration by humanitarian organisations, or any other functional collection of data (e.g. to register individuals for an assistance programme) 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' (Jacobsen, 2015b). Mitigating function creep requires that humanitarian organisations question the scope, management and security of their data collection processes, and above all, insulate this information from other jurisdictions, including by providing it with a set shelf-life before its deletion or secured return to the data subject (ICRC and Privacy international, 2018; Wilton Park, 2019).

1 While this does not pertain directly to the subject of this review, it is worth specificying that the personal information of non or under-connected individuals can also be compromised. Indeed, they may have a digital footprint generated by data from their peers or organisations that they have interacted with in the analog world (ICRC and Privacy international, 2018; Wilton Park, 2019).

Connectivity risks also manifest themselves in mobile-enabled services, such as cash transfers or smartcards. Because these programmes involve financial service providers, they can invoke "Know-Your-Customer" 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 them being a recipient of assistance in the past (ICRC and Privacy International, 2018). In light of the increasingly interconnected and multi-national nature of financial and 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 (see Senbore et al., 2019, as an example).

The use of connectivity in the humanitarian response, or its increased availability in displaced contexts, can also further expose refugees to misinformation, propaganda, hate speech or other weaponisation of information phenomena (Privacy International, 2013; Jacobsen, 2015a). 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 information and communication technology in Lebanon (2018).

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 eventually 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 organisations are on the rise; or 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 (Privacy International, 2013; ICRC and Privacy International, 2018; Willitts-King et al., 2019).

Ongoing policy and advocacy efforts

To help mitigate the privacy and cybersecurity concerns related to connectivity, humanitarian organisations have published a series of strategies and guidelines on data protection (see UNHCR, 2015; ICRC, 2018; and OCHA, 2019 – but also DFID, 2018 or USAID, 2019), mobile money (CaLP, 2013; or UNHCR and World Vision, 2016), and even more specific topics such as the use of biometrics (ICRC, 2019).

Many of these refer to or reflect the 'Principles for Digital Development', a framework endorsed by 194 organisations including aid agencies, donor governments, connectivity service providers and media outlets (Dawson and Davies, 2019). While these principles were never translated and articulated into a specific framework for the humanitarian sector, standards and guidelines do exist around the deployment of mobile-enabled services in humanitarian contexts (for instance, the Barcelona Principles for Digital Payments in Humanitarian Response).

Meanwhile, governments, service providers and human rights organisations have also produced important work on digital and human rights. Notable examples include the Mozilla Manifesto, the Internet Bill of Rights, the African Declaration on Internet Rights and Freedoms, the EU's General Data Protection Regulation, and the GSMA's Declaration on the Digital Future. These and others have also been amalgamated into a broader "Contract for the web" (Contract for the web, 2019). These texts are not all enforceable, and many have a limited jurisdiction in which enforcement can be inconsistent or problematic. Moreover, they may not be directly relevant to the cybersecurity and privacy issues covered here. However, they do help to provide a cadre in which these issues can be analysed, and further regulations or guidelines inferred.

Finally, the extent to which such advocacy or policy efforts can truly mitigate risks by regulating connectivity service providers has been questioned. Some have argued that the organisational culture of connectivity service providers – which rewards metric-oriented, fast-paced work – is inherently at odds with humanitarian principles (Moss and Metcalf, 2019). As a result, some have pushed for "Delete your data" initiatives, or placed greater stock in advocacy before donors to reduce data collection or digital exchanges (Wilton Park, 2019).

Annex 1. Main actors writing on connectivity in humanitarian contexts

The first group of actors writing on connectivity are **humanitarian organisations** themselves, sometimes with the support, financing or cooperation from donor governments. OCHA regularly addresses the topic in both its annual World humanitarian data and trends report (the latest issue being OCHA, 2018), and dedicated, thematic publications (see OCHA, 2013; or OCHA, 2017). The IFRC's World disasters report also regularly covers the issue, be it in dedicated chapters or sections (see IFRC, 2012: 222-224 or IFRC, 2015: 180-198) or as an overarching theme (IFRC, 2013). Meanwhile, while its mandate does not (yet)[2] include research or publishing, the Emergency Telecommunications Cluster – of which many humanitarian organisations are a part – provides country-specific overviews of their operations and inter-agency responses (including situation reports, dashboards, minutes, etc.).

Meanwhile, other humanitarian actors have issued thematic publications on everything from internet and mobile connectivity for refugees (UNHCR, 2016) to how to use social media to better engage people affected by crisis (ICRC, IFRC and OCHA, 2017) to the risks associated with the digital trails that online or mobile conversations leave behind (ICRC and Privacy International, 2018). These were accompanied by a growing number of guidelines and policies for humanitarian practitioners in order to support safe practices around connectivity, including data protection (UNHCR, 2015; ICRC, 2018; and OCHA, 2019) and connected services such as mobile money (see, as an example, CaLP, 2013; or UNHCR and World Vision, 2016) or the use of biometrics (ICRC, 2019). It is worth mentioning that the displacement crisis, and specifically the 2015 'European refugee crisis', seems to have marked a shift in thematic focus, as humanitarian organisations went from writing about the role of social media in natural disasters, to its broader role in displacement and other humanitarian contexts.[3]

Broadly speaking, these publications used to focus on (successful) case studies of and opportunities for the use of connectivity in humanitarian contexts. More recently, this focus has shifted towards the risks associated with this use, and has been accompanied by recommendations grounded in *the preservation of the safety and agency of affected people.*

The second group of actors are **human rights, activist and watchdog organisations**. A number of these organisations focus on internet access and governance, including in contexts that host major humanitarian operations. These organisations include Internet without borders, Access Now, World Wide Web foundation, the Global network initiative or

2 The cluster is currently evolving from "being primarily a service provider, to broker, facilitator and convenor of technology in emergency response" (ETC website, 2020). This may have implications around the level of advocacy, research and publishing they do in relation to connectivity.

3 This shift was also accompanied by re-branding – for instance, the GSM Association's 'Disaster response' programme became the 'Mobile Humanitarian Innovation' programme, implying a broader ambition for the role of mobile before, during and after crises.

the Alliance for affordable internet. The majority of these contribute to our understanding of issues by monitoring and issuing regular communiqués on the level of connectivity in different contexts. However, some also produce research on how barriers to connectivity impact specific population groups in areas of humanitarian concern (as an example, see A4AI, 2019). Meanwhile, organisations like Ranking Digital Rights publish an annual index on how the commitments and policies of the world's most powerful internet, mobile and telecommunications companies affect freedom of expression and internet user privacy (access the latest at RDR, 2019).

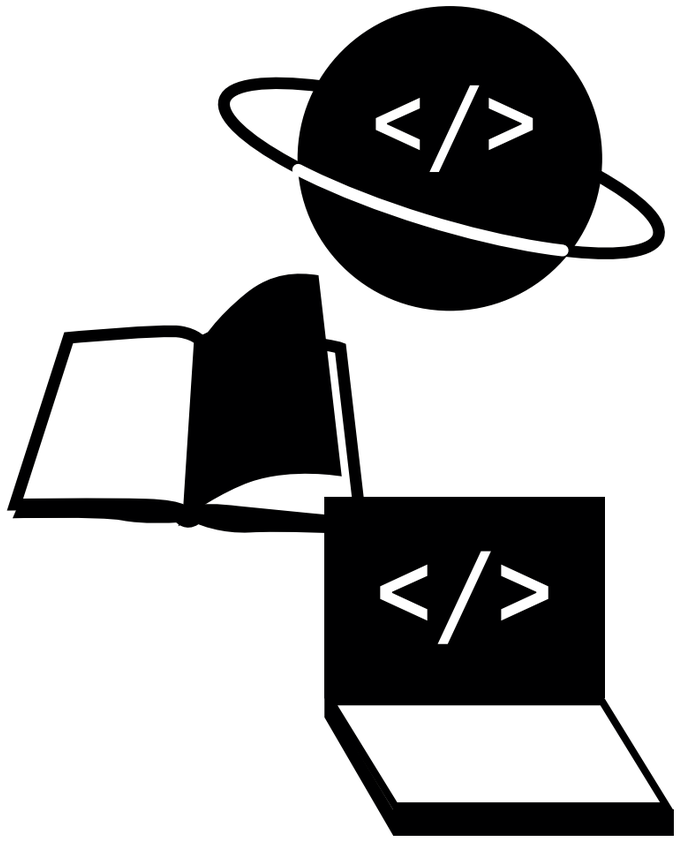
Some of these human rights, activist and watchdog organisations focus more on the surveillance risks associated with technology and connectivity, often in Western contexts. When humanitarian contexts or populations of concerned are referred to, it is often to transpose and demonstrate the pertinence of previously identified risks in other places. In other words, this research does not use the organic experiences of affected communities as a starting point. For instance, Privacy International regularly issues research on how the deployment of connected technology infringes upon user privacy in Uganda (Privacy international, 2015), Colombia (Privacy International, 2016a), Syria (Privacy International, 2016b) or Kenya (Privacy International, 2017). More recently, Amnesty International addressed how the business model of social media companies threatened human rights, including in the Global South (Amnesty International, 2019: 13-14). This research overlaps with the work done by Algorithm Watch, whose publications focus on the ethical conflicts of algorithmic decision-making – for instance, when it is used in asylum and immigration processes (Algorithm Watch, 2019: 35-38).

Publications by this second group of organisations have regularly focused more on the risks and threats posed by connectivity and the use of technology, especially by states or established companies. They often issue recommendations that are grounded in *the upholding of human rights (namely the right to privacy and the right to internet access, also known as right to broadband or freedom to connect)*.

The third group writing on connectivity in humanitarian contexts are **academics, policy institutes or think tanks**. Their publications include field research on the pros and cons of the use of technology in humanitarian operations – including biometrics (Jacobsen, 2015a), drones and satellite imagery (Lichtman and Nair, 2015) or mobile connectivity in refugee camps (Latonero et al., 2018). They also include policy briefs – for instance, on the use of smartphones among refugees (Jumbert et al., 2018) – broader literature reviews (Willitts-King et al., 2019) and pieces of journalism (Latonero, 2019). While the topics covered in each publication vary greatly in terms of scope and specialisation – and at times, intersect with activist spaces – the approach used tends to remain more scientific, and accompanying recommendations grounded in *the promotion of accountability, transparency and security in the humanitarian sector.*

Finally, the fourth group writing on connectivity in humanitarian contexts is the **private sector, particularly connectivity service providers.** The GSM Association – which represents the interests of mobile operators across the world – issues annual reports on

the state of mobile internet connectivity (see the latest at GSMA, 2019a), the use of mobile technology towards humanitarian innovation (see the latest at GSMA, 2019b) the use of mobile money (see the latest at GSMA, 2019c) and more. They also publish thematic reports and case studies, including on mobile connectivity among refugees (GSMA, 2019d); the mobile gender and disability gap (GSMA, 2019e and GSMA, 2019f, respectively); or mobile opportunities within the humanitarian ecosystem at large (GSMA, 2018a). While these publications may, at times, relay privacy concerns as expressed by affected people, or integrate consumer privacy concerns into their narrative (see GSMA, 2015), their publications remain grounded in *the promotion of mobile and internet connectivity as enablers of humanitarian aid, economic development and social inclusion*.



Bibliography

A4AI – Alliance for affordable internet. "*Who Wins? Who Loses? Understanding Women's Experiences Of Social Media Taxation In East And Southern Africa."* May 2019. https://a4ai.org/research/who-wins-who-loses-understanding-womens-experiences-of-social-media-taxation-in-east-and-southern-africa/

Alam, K. and Imran, S. "*The Digital Divide And Social Inclusion Among Refugee Migrants*" (pp. 344–365). Information Technology & People 28(2). 2015. https://pdfs.semanticscholar.org/5cf0/393c525067618618abed6b96fde35b07d11d.pdf

Alencar, A.; Knodova, K.; and Ribbers, W. *"The Smartphone As A Lifeline: An Exploration Of Refugees' Use Of Mobile Communication Technologies During Their Flight"* (pp. 828-844). Media, Culture & Society 41(6). https://doi.org/10.1177/0163443718813486

Algorithm Watch. "*Automating Society: Taking Stock Of Automated Decision-Making In The EU."* Berlin. January 2019. https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf

ALNAP. "*The State Of The Humanitarian System"* 2018 edition. London. 2018.

Amnesty International. "*Surveillance Giants: How The Business Model Of Google And Facebook Threatens Human Rights."* London. 2019. https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

Andrade, A. and Doolin, B. *"Information And Communication Technology And The Social Inclusion Of Refugees"* (pp. 405-416). MIS Quarterly 40(2). June 2016. https://doi.org/10.25300/MISQ/2016/40.2.06

Benton, M. and Glennie, A. *"Digital Humanitarianism: How Tech Entrepreneurs Are Supporting Refugee Integration"*. Transatlantic council on migration. October 2016. https://www.migrationpolicy.org/sites/default/files/publications/TCM-Asylum-Benton-FINAL.pdf

Brown, S.; Hussain, F.; and Masoumifar, A. *"Refugees and ICTs: identifying the key trends and gaps in peer-reviewed scholarship"* (pp. 687-697). Information and communication technologies for development: Strengthening southern-driven cooperation as a catalyst. 2019.

CaLP – The cash learning partnership. "*Protecting Beneficiary Privacy: Principles And Operational Standards For The Secure Use Of Personal Data In Cash And e-Transfer Programmes."* November 2013. http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf

Compaine, B. *"Information Gaps"* (pp. 105–118). The digital divide: Facing a crisis or creating a myth?. Cambridge. MIT Press. 2001.

Contract for the web. *"About"*. Contract for the web official website. Last update 2019. https://contractfortheweb.org/

Crabtree, K. and Geara, P. *"Safety Planning For Technology: Displaced Women And Girls' Interactions With Information And Communication Technology In Lebanon And Harm Reduction Considerations For Humanitarian Settings"*. Journal of International Humanitarian Action 3(3). 2018. https://link.springer.com/article/10.1186/s41018-018-0031-x

Culbertson, Dimarogonas, Costello and Lanna. "*Crossing the Digital Divide: Applying Technology to the Global Refugee Crisis."* Rand Corporation. 2019.

Dawson, E. and Davies, E. *"Embracing Digital Principles For Inclusive Development"*. Bond. 2019. www.bond.org.uk/news/2019/02/embracing-digital-principles-for-inclusive-development

Dekker, R.; Engbersen, G.; Klaver, J. and Vonk, H. *"Smart Refugees: How Syrian Asylum Migrants Use Social Media Information In Migration Decision-Making"*. Social media and society 4(1). 2018. https://doi.org/10.1177/2056305118764439

DFID – Department for International Development. "*Digital Strategy 2018–2020: Doing Development In A Digital World."* London. 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701443/DFID-Digital-Strategy-23-01-18a.pdf

Dijstelbloem, H. and Meijer, A. "*De Migratiemachine. De Rol Van Technologie In Het Migratiebeleid."* Amsterdam. 2009.

Elias, N. and Lemish, D. *"Spinning The Web Of Identity: The Roles Of The Internet In The Lives Of Immigrant Adolescents"* (pp. 533-551). New media and society 11(4). 2009. https://journals.sagepub.com/doi/abs/10.1177/1461444809102959

Emergency Telecommunications Cluster. *"About The ETC"*. ETC website. 2020. https://www.etcluster.org/about-etc

GSMA. "*Privacy And Data Protection In The Internet Of Things."* January 2015. https://www.gsma.com/iot/wp-content/uploads/2017/11/Privacy-and-Data-Protection-in-the-Internet-of-Things.pdf

GSMA. *"Landscaping The Digital Humanitarian Ecosystem."* December 2018a. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/12/Landscaping-the-digital-humanitarian-ecosystem.pdf

GSMA. *"Access To Mobile Services And Proof Of Identity: Global Policy Trends, Dependencies And Risks."* 2018b. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

GSMA. "*The State Of Mobile Internet Connectivity Report 2019."* 2019a. https://www.gsma.com/mobilefordevelopment/resources/the-state-of-mobile-internet-connectivity-report-2019/

GSMA. *"Mobile For Humanitarian Innovation: Annual Report 2018."* 2019b. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/M4H-2018-Annual-Report.pdf

GSMA. *"2018 State Of The Industry Report On Mobile Money."* 2019c. https://www.gsma.com/mobilefordevelopment/resources/2018-state-of-the-industry-report-on-mobile-money/

GSMA. "*The Digital Lives Of Refugees: How Displaced Populations Use Mobile Phones And What Gets In The Way."* 2019d. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/The-Digital-Lives-of-Refugees.pdf

GSMA. *"The Mobile Gender Gap Report 2019."* 2019e. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA-Connected-Women-The-Mobile-Gender-Gap-Report-2019.pdf

GSMA. "*Understanding The Mobile Disability Gap."* 2019f. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/12/GSMA_Understanding-the-mobile-disability-gap_116pg_Accessible.pdf

Hargittai, E. *"The Digital Divide and What to Do About It"* (p. 824). New Economy Handbook. 2003.

Hargittai, E. *"The Digital Reproduction Of Inequality"* (pp. 936–944). In Grusky, D. Social stratification Boulder. Westview Press. 2008.

ICRC - International Committee of the Red Cross. "*Handbook On Data Protection In Humanitarian Action: Second Edition".* Geneva. 2018. https://www.icrc.org/en/document/handbook-data-protection-humanitarian-action-second-edition

ICRC – International Committee of the Red Cross, IFRC – International Federation of Red Cross, OCHA – United Nations Office for the Coordination of Humanitarian Affairs. "*How to use social media to better engage people affected by crises."* Geneva. 2017. https://media.ifrc.org/ifrc/document/use-social-media-better-engage-people-affected-crises/

ICRC – International Committee of the Red Cross, Privacy International. "*The Humanitarian Metadata Problem: 'Doing No Harm' In The Digital Era."* 2018. https://www.icrc.org/en/download/file/101039/final_web_the_humanitarian_metadata_problem_-_doing_no_harm_in_the_digital_era.pdf

IFRC – International Federation of Red Cross. "*World Disasters Report: Focus On Migration And Forced Displacement".* Geneva. 2012. https://www.ifrc.org/Global/Documents/Secretariat/2012_WDR_Full_Report.pdf

IFRC – International Federation of Red Cross. “*World Disasters Report: Focus On Technology And The Future Of Humanitarian Action”.* Geneva. 2013. https://www.ifrc.org/PageFiles/134658/WDR%202013%20complete.pdf

IFRC – International Federation of Red Cross. “*World Disasters Report: Focus On Local Actors, The Key To Humanitarian Effectiveness.”* Geneva. 2015. http://ifrc-media.org/interactive/wp-content/uploads/2015/09/1293600-World-Disasters-Report-2015_en.pdf

Internews. “*Dadaab, Kenya - Humanitarian Communications And Information Needs Assessment Among Refugees In The Camps: Findings, Analysis And Recommendations”.* September 2011. https://internews.org/sites/default/files/resources/Dadaab2011-09-14.pdf

Islam, M.Z. *“Rohingyas use 3 lakh mobiles”*. The Daily Star. 28 November 2019. https://www.thedailystar.net/backpage/rohingyas-use-3-lakh-mobiles-following-forgery-1832767

Jacobsen, K. *“Experimentation In Humanitarian Locations: Unhcr And Biometric Registration Of Afghan Refugees”.* Security Dialogue 46(2): 144–164. 2015a. https://www.jstor.org/stable/26292335?seq=1

Jacobsen, K. “*The Politics Of Humanitarian Technology: Good Intentions, Unintended Consequences And Insecurity.”* London. 2015b.

Jumbert, M.; Bellanova, R.; and Gellert, R. *“Smartphones For Refugees: Tools For Survival, Or Surveillance?”.* PRIO Policy Brief, 4. Oslo. 2018. https://www.prio.org/Publications/Publication/?x=11022

Kaurin, D. *“Protection And Digital Agency For Refugees”.* World Refugee Council research paper series. 15 May 2019. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees

Latonero, M. *“Stop Surveillance Humanitarianism”.* The New York Times. 11 July 2019. www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html

Latonero, M.; Poole, D.; and Berens, J. “*Refugee Connectivity: A Survey Of Mobile Phones, Mental Health And Privacy At A Syrian Refugee Camp In Greece.”* Harvard Humanitarian Initiative. 2018. https://hhi.harvard.edu/publications/refugee-connectivity-survey-mobile-phones-mental-health-and-privacy-syrian-refugee-camp

Lichtman, A. and Nair, M. *“Humanitarian Uses Of Drones And Satellite Imagery Analysis: The Promises And Perils”.* AMA Journal of Ethics 17(10): 931–937. 2015. https://journalofethics.ama-assn.org/ article/humanitarian-uses-drones-and-satellite-imagery-analysis-promises-and-perils/2015-10

Leurs, K. & Smets, K. *“Five Questions For Digital Migration Studies: Learning From Digital Connectivity And Forced Migration In(To) Europe”*. Social media & society 4(1). 2018. https://doi.org/10.1177/2056305118764425

Levin, B.; De Sa, P. ; and Aleinikoff, T. *“Policy Brief: A Global Broadband Plan For Refugees”.* Migration policy institute. May 2017.

Levin, B.; De Sa, P.; and Milkman, R. “*Global Broadband Plan For Refugee Inclusion”.* 2019. https://static1.squarespace.com/static/5a0f82f67131a5ac3ca77f03/t/5c9cd941ee6eb02afe82469a/1553783109805/GBP4RI+March+FINAL_For+Posting.pdf

Lloyd, A.; Kennan, M.; Thompson, Kim.; and Qayyum, A. *“Connecting With New Information Landscapes: Information Literacy Practices Of Refugees”* (pp. 121-144). Journal of Documentation 69(1). January 2013. https://www.researchgate.net/publication/236615520_Connecting_with_new_information_landscapes_Information_literacy_practices_of_refugees

Madianou, M. *“Digital Inequality And Second-Order Disasters: Social Media In The Typhoon Haiyan Recovery”.* Social Media and Society. 2015. https://doi.org/10.1177/2056305115603386

Maitland, C.; and Bharania, R. *“Balancing Security And Other Requirements In Hastily Formed Networks: The Case Of The Syrian Refugee Response”.* March 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944147

Marlowe, J. *“Refugee Resettlement, Social Media And The Social Organization Of Difference”.* University of Auckland. 18 April 2019. https://onlinelibrary.wiley.com/doi/pdf/10.1111/glob.12233

McVeigh, K. *“Bangladesh imposes mobile phone blackout in Rohingya refugee camps”.* The Guardian. 5 September 2019. http://www.theguardian.com/global-development/2019/sep/05/bangladeshimposes-mobile-phone-blackout-in-rohingya-refugee-camps

Meier, P. “*Digital Humanitarians: How Big Data Is Changing The Face Of Humanitarian Response”.* Boca Raton FL: CRC Press. 2015.

Moss, E.; and Metcalf, J. *“The Ethical Dilemma At The Heart Of Big Tech Companies”*. Harvard Business Review. 14 November 2019. https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-tech-companies

Mutua, J. “*New rules to end SIM card hawking, fraud”.* Business daily Africa. 27 November 2019. https://www.businessdailyafrica.com/corporate/companies/New-rules-to-end-SIM-card-hawking--fraud/4003102-5365266-106trnuz/index.html

N.a. *“Gov’t moves to regulate financial technologies”*. The Independent. 30 November 2019. https://www.independent.co.ug/govt-moves-to-regulate-financial-technologies/

OCHA - United Nations Office for the Coordination of Humanitarian Affairs. “*Humanitarianism In The Network Age: Including World Humanitarian Data And Trends 2012”.* New York. 2013.

OCHA - United Nations Office for the Coordination of Humanitarian Affairs. ***New Way of Working***. New York. 2017.

OCHA - United Nations Office for the Coordination of Humanitarian Affairs. "***World Humanitarian Data And Trends 2018".*** New York. 2018. https://reliefweb.int/ report/world/world-humanitarian-data-and-trends-2018

OCHA – United Nations Office for the Coordination of Humanitarian Affairs. ***Data Responsibility Guidelines: Working Draft.*** May 2019. https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf

Okuoro, S. "Mpower: Enabling Refugee Children In Kenya To Learn". Standard Media. 19 November 2019. https://www.standardmedia.co.ke/article/2001349988/mpower-enabling-refugee-children-in-kenya-to-learn

Patil, A. "The Role Of Icts In Refugee Lives". Conference paper for the Tenth International Conference. 2019. https://www.researchgate.net/publication/330265040_The_role_of_ICTs_in_refugee_lives

Privacy International. ***"Aiding Surveillance".*** London. 2013. https://privacyinternational.org/report/841/aiding-surveillance

Privacy International. ***"For God And My President: State Surveillance In Uganda".*** 2015. https://privacyinternational.org/feature/1169/ugandas-grand-ambitions-secret-surveillance

Privacy International. ***"Discussion About Cyber Security In Colombia".*** 2016a. https://privacyinternational.org/feature/1145/discussion-about-cyber-security-colombia

Privacy International. "***Open Season: Building Syria's Surveillance State".*** London. 2016b. https://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state

Privacy International. "***Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya".*** London. 2017. https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

Privacy International. ***"Surveillance Company Cellebrite Finds A New Exploit: Spying On Asylum Seekers"***. Privacy International. 3 April 2019. https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

Rahman, F. ***"Generation Start-Up: Ustad Mobile Helps Those Living Remotely Access Digital Learning".*** The National. 1 December 2019. https://www.thenational.ae/business/generation-start-up-ustad-mobile-helps-those-living-remotely-access-digital-learning-1.944740

Ratcliffe, R. and Okiror, S. ***"Millions Of Ugandans Quit Internet Services As Social Media Tax Takes Effect".*** The Guardian. 27 February 2019. https://www.theguardian.com/global-development/2019/feb/27/millions-of-ugandans-quit-internet-after-introduction-of-social-media-tax-free-speech

RDR – Ranking Digital Rights. ***2019 RDR Corporate accountability index.*** May 2019. https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf

Read, R., Taithe, B. and Mac Ginty, R. ***"Data Hubris? Humanitarian Information Systems And The Mirage Of Technology".*** Third World Quarterly 37(8): 1314–1331. 2016. www.tandfonline.com/doi/abs/10.1080/01436597.2015.1136208

Samuel Hall. "***Opportunities And Barriers To Using Mobile Technology And The Internet In Kakuma Refugee Camp And Nakivale Refugee Settlement."*** January 2018. https://static1.squarespace.com/static/5cfe2c8927234e0001688343/t/5d1f1b83bfecef0001fb6621/1562319758732/Innovating_mobile_soultions_report_2018.pdf

Schradie, J. ***"The Trend Of Class, Race And Ethnicity In Social Media Inequality"*** (pp.555-571). Information, Communication & Society (15). 2013. https://doi.org/10.1080/1369118X.2012.665939

Senbore, O.; Arome, I.; and Obuka, C. ***"How Should Nigeria Regulate Its Fintech Industry?"***. Lexology. 29 November 2019. https://www.lexology.com/library/detail.aspx?g=92f8de68-2d59-466c-b3b4-687f2a18d131

Simko, L.; Lerner, A.; Ibtasam, S.; Roesner, F.; and Kohno, T. ***"Computer Security And Privacy For Refugees In The United States".*** 218 IEEE Symposium on security and privacy. 2018. https://adalerner.com/simko-refugees-sp18.pdf

SINGA France. "***Refugees and ICT***." Paris. 2014. https://marcopolis.org/wp-content/uploads/2017/04/SINGA-International-Study-2014-Refugees-and-ICTs.pdf

UNHCR. "***Policy On The Protection Of Personal Data Of Persons Of Concern".*** May 2015. https://www.refworld.org/docid/55643c1d4.html

UNHCR. "***Connecting Refugees: How Internet And Mobile Connectivity Improve Refugee Well-Being And Transform Humanitarian Action."*** Geneva. 2016. https://www.unhcr.org/5770d43c4.pdf

UNHCR. ***"Displaced and Disconnected".*** 2019. https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Displaced-Disconnected-WEB.pdf

UNHCR. *“UNHCR Welcomes Uganda Communications Commission Directive To Improve Refugees’ Access To SIM Cards”.* UNHCR Press releases. 20 August 2019b. https://www.unhcr.org/afr/news/press/2019/8/5d5ba4274/unhcr-welcomes-uganda-communications-commission-directive-to-improve-refugees.html

UNHCR and World Vision. “*Know Your Customer Standards And Privacy Recommendations For Cash Transfers.”* January 2016. http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf

UN Innovation Network. *“Innovations 4 Scale – UNDP’s Speak up with WhatsApp”*. Youtube. 23 October 2019. https://www.youtube.com/watch?v=kU4IS4cPyOk

USAID. *Draft USAID digital strategy*. Washington DC. 2019. https://www.ictworks.org/wp-content/uploads/2019/10/USAID_Digital_Strategy_Draft.pdf

Wall, M.; Campbell, M.; and Janbek, D. *“Syrian Refugees And Information Precarity”* (pp. 240-254). New Media & Society (19). 2017.

Willitts-King, B.; Bryant, J.; and Holloway, K. *“The Humanitarian Digital Divide.”* The Overseas Development Institute and Humanitarian Policy Group. November 2019. https://www.odi.org/sites/odi.org.uk/files/resource-documents/digital_divide_lit_review_web_0.pdf

Wilton Park. *“Digital Dignity In Armed Conflict: A Roadmap For Principled Humanitarian Action In The Age Of Digital Transformation”.* WP1698 Monday 21-Wednesday 23 October 2019. 2019. https://www.wiltonpark.org.uk/wp-content/uploads/WP1698-Report.pdf

Yandell, A. *“’All Refugees Have Smartphones…’ And Here’s What We Can Do About It”.* Medium. 26 July 2016. https://medium.com/@ayandell/all-refugees-have-smartphones-and-heres-what-we-can-do-about-it-511b5bf848b0

UNHCR Innovation Service