FOUR

The Digital Turn in Migration

Evan Easton-Calabria

Introduction

In this chapter, digital responsibilities are considered through an international lens, considering how the deployment of digital technologies by states shapes the nature of responsibility in the context of refugees and migration. This study therefore sits at the intersection of humanitarian responsibility and digital responsibility.

When one thinks of responsibility and refugees, the obligation for states to host refugees, such as adherence to the 1951 Refugee Convention, might first come to mind. Indeed, the United Nations' (UN) 2018 Global Compact on Refugees – the current global guiding document on refugees – laid out a vision for 'more predictable and equitable burden and responsibility-sharing' for refugee situations (United Nations, 2018). It sought to 'operationalize the principle of burden and responsibility-sharing, to mobilize the international community as a whole, and to galvanize action for an improved response to refugee situations' (United Nations, 2018, p III). This vision is laudable and important: over 122 million people are currently forcibly displaced (UNHCR, 2023). Less than 1% will ever be resettled to a third country and cross-country agreements for refugee resettlement are gaining traction and growing voter support (Vrânceanu et al, 2023). Such policies

Figure 4.1: UN Global Compact

are dependent on a digital infrastructure that can administrate the cross-country movement and resettlement of refugees. This infrastructure brings with it new forms of responsibility that highlight the antecedents from how responsibility actions emerge, how they are mediated and mitigated by digital technologies.

While concerning itself with the notion of responsibility in refugee situations, this chapter narrows the focus to a similarly under-explored concept, that of digital responsibility. The issue of digital responsibility and refugees is scant in the academic literature, despite the growing focus on the importance of internet connectivity and digital administration in both transit and displacement since the 2015–16 so-called 'European refugee crisis'. In this chapter, we sketch the literature that frames the discussion on digital responsibility and refugees and present two case studies that animate the themes in the literature, focusing on the digital responsibility of humanitarian agencies, namely the UN Refugee Agency in global displacement, and the work of refugee-serving civil society organisations supporting the digital inclusion of refugees in London during the COVID-19 pandemic. We close with a

discussion of how the findings align with the book's digital responsibility framework.

Background

Responsibility in the international refugee regime

While responsibility-sharing is commonly understood as the equitable sharing of both finances for refugee assistance and intake, and numbers of refugees resettled, in reality this is not practiced by States. Instead, the global norm of responsibility-sharing remains much more idealised than real, thereby precluding more nuanced discussions of what responsibility in refugee contexts actually entails. Both discussions and references to the notion of responsibility in the international refugee regime are complicated by the fact that the term 'responsibility' is rarely defined, with many texts simply relying on the assumption, based on the 1951 Refugee Convention, that States, either alone or collectively (Hurwitz, 2009), are legally responsible for taking care of them.

However, a small body of academic literature focuses directly on responsibility and refugees. Much of this literature is policy-oriented rather than critical, focusing on how to increase responsibility-sharing by States rather than interrogating broader notions of responsibility itself. Martin et al (2018) focus, for example, on areas of responsibility-sharing including addressing underlying causes of displacement, efforts to find solutions, initiatives to enhance protection, and technical assistance and training for host countries and organisations. Taking a legal perspective, Dowd and McAdam (2017, p 867) explore the 'two main methods of sharing responsibilities, namely the provision of financial and other assistance to host countries, and the admission of refugees' as well as the principle of common but differentiated responsibilities, exploring how it might apply in international refugee law. In a similar vein, Ahmed (2018) poses the critical question of who should take responsibility for so-called 'climate refugees', using a

Figure 4.2: Unclear responsibilities

model considering climate pollution, consumption, human development and other factors to suggest that Australia and the United States should take responsibility for 10% of climate refugees, followed by Canada and other countries. Furthermore, while there is limited understanding of the responsibilities related to refugees, there is even less about the need for digital needs and the responsibilities that flow.

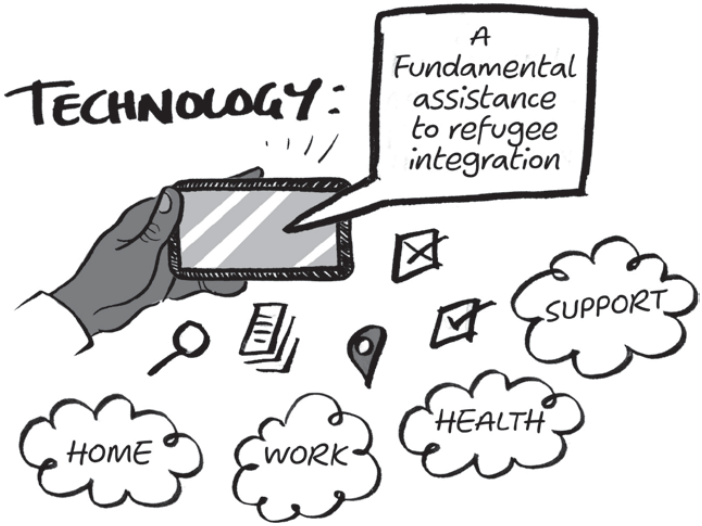
Refugees and digital technologies

Since the large-scale arrival of Syrian refugees in Europe in 2015–16, myriad digital initiatives seeking to 'include' and facilitate everything from the transit to the integration of refugees have arisen. These developed in part out of a recognition that smartphones and connectivity were key tools

for refugees in transit, helping them navigate, find safe places to sleep *en route* and access information about their destinations (Frouws et al, 2016; Gough and Gough, 2019). However, technology production is neither a neutral nor objective process but instead is shaped by geographies, ideologies, and multiple interests (Wahome and Graham, 2020). It then follows that the use and promotion of technology is similarly imbued with complexity. Despite the complexities inherent in digital service provision, refugees' digital inclusion is predominantly presented by governments and humanitarian and development agencies as a human right and an emancipatory tool with the potential to increase access to skills and income (UNHCR, 2022a).

A growing body of literature has also critically explored refugees' relationship to technology, as well as how humanitarian and development agencies act as mediators to digital inclusion. While not interrogating the notion of responsibility explicitly, Jacobsen and Sandvik (2018) explore UNHCR's

Figure 4.3: Digital assistance



international protection efforts and in particular their efforts to use 'accountability technologies', namely results-based management, biometrics and cash-based interventions. They argue that 'this configuration and use of accountability technologies contributes to the emergence of a particular understanding of international protection as a task best accomplished through improved techno-bureaucratic legibility and quantification practices', focusing on the role of technology in both enabling and obscuring particular practices related to 'accountability' and 'protection' (Jacobsen and Sandvik, 2018, p 1509).

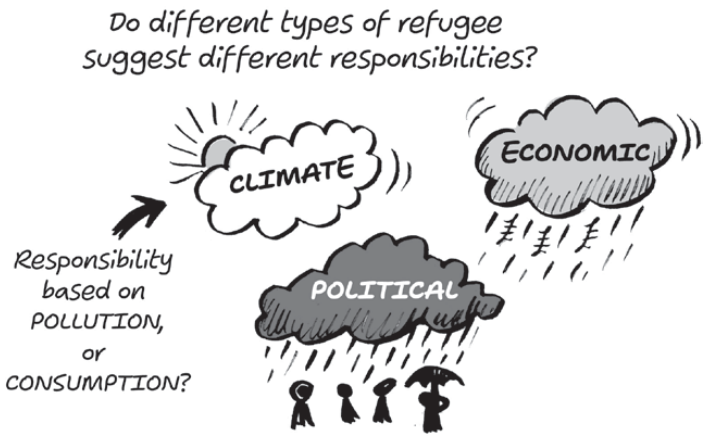
Udwan et al (2020) developed a case study of Syrians living in the Netherlands and their 'digital resilience', focusing on digital social support, digital health and digital identities. They noted that media and digital networks have been overlooked for their positive role in fostering resilience, later sharing an excerpt from one Syrian vlogger's YouTube channel: 'I am the virtual daughter, I am the virtual wife, I am the virtual friend. I am the virtual sister. I am the virtual sweetheart. … In my alienation, I hug my mobile phone at night. Every morning, I give that metallic phone a virtual kiss' (Udwan et al, 2020, p 8). At the same time that they highlight how refugees employ technology in a variety of positive ways, they caution: 'While we have emphasized several digital resilience tactics refugees mobilize for self-support, health, and identity management, we want to avoid our results being co-opted by governments to demonstrate their policies of no-policies and retraction of assistance are successful' (Udwan et al, 2020, p 9).

These areas of facilitation include communication with the government, social connectedness, participation in educational programmes, and social inclusion (Krasnova et al, 2016). Digital technology is also used to create so-called 'digital work' projects for refugees, which often include integration as an aim. Alencar and Camargo (2023) describe a digital work initiative in Brazil that reflects the tensions between the aspirations and empowerment narratives that

are woven across digital work and the barriers to access and the amplification of marginalisation that migrants can experience when undertaking work in the digital economy. AbuJarour et al (2017) posit that refugees encounter three major stakeholder groups within the bureaucratic and socio-economic structures of the asylum and resettlement process: (1) local government and public authorities, (2) local population and (3) businesses. In this view, digital technologies mediate or have the potential to increase engagement with these stakeholders.

However, other works highlight the security implications of such engagement, with a predominant focus on border and migration management (Ajana, 2013; Latonero and Kift, 2018), data privacy and usage, biometrics (Jacobsen and Sandvik, 2018; Završnik, 2021) and the concept of digital identities. Simko et al (2018) explore computer security and privacy for newly resettled refugees in the United States, finding that ICTs such as email are important in integrating into new roles while barriers to digital security are also paramount, including a lack of language and technical skills, and cultural knowledge, that

Figure 4.4: One size does not fit all



can lead to scams and other forms of digital exploitation. Other work explores, generally critically, the data-driven technologies of European border management such as EUROSUR, the European Border Surveillance Systems, and European-wide databases such as the Schengen Information System, finding that the erection of 'digital borders' and the 'European digital fortress' have – unsurprisingly – nefarious impacts on refugees and their rights (Topak, 2014).

Digital responsibilities and refugees

While rich and varied, much of this literature does not address the question of: Where does responsibility for refugees lie in these digital arenas?

The United Nations High Commissioner for Refugees (UNHCR) is mandated with the legal protection of refugees. While, at least on paper, host states are legally responsible for refugees, UNHCR has been called a 'surrogate state' (Deardorff Miller, 2017) and commonly steps in to support host states with functions such as asylum status determination and, through its implementing partners, everything from livelihoods to education. Increasingly since 2015, UNHCR has shown a heightened awareness of the importance of digital connectivity for refugees and some nascent efforts to connect refugees to digital work, complemented by a longer-term focus on biometric identification and other aspects of digital identity. Each of these arenas raises questions of how UNHCR addresses and indeed perceives its own digital responsibility towards refugees.

One of the most intriguing elements of digital responsibility in relation to UNHCR and refugees is the additional role of host states, as it is ultimately their policies and practices that define the legal and operational scope and context for humanitarian action. This extends to data management and other digital practices (Schoemaker et al, 2018). While UNHCR does offer support to connect refugees to the

internet (expanded on in the following quote), it makes clear that digital inclusion is not solely its responsibility:

> Identity in the 21st century is no longer just paper-based and centred on breeder documents, such as birth certificates and ID cards. With new technologies providing access to the internet, mobile phones and related services, to information, education, banking, and other economic opportunities, the concept and realities of identity broadens. *States have the responsibility to provide for the digital inclusion and identity of their citizens and those living on their territory.* UNHCR assists member states in ensuring that refugees and asylum seekers, stateless persons, and other forcibly displaced are – digitally speaking – not left behind. (UNHCR, 2022b) [emphasis added]

Despite this position, UNHCR has steadily increased its engagement with digital inclusion. Some of this early work was piloted through the UNHCR Innovation Unit, established in 2012 to experiment and problem-solve within the agency. Focusing at the time on areas called Innovation Labs, the unit emphasised self-reliance in addition to ICT, access to energy, data and communication, and field delivery. One of these projects was Community Technology Access (CTA) in Kenya's Dadaab refugee camp (UNHCR, 2022c). This project has since expanded to both camps and urban areas and forms the practical basis for UNHCR's focus on helping refugees access digital work – what UNHCR originally termed teleworking activities – and wider digital skills.

It is notable that UNHCR has been involved with digital data such as biometric data collection for much longer than other efforts such as digital work for refugees. It has, for instance, used identity technology such as iris-recognition technology since 2002, when it was first employed for Afghan refugees returning from Pakistan (Jacobsen and Sandvik, 2018). What has vastly

expanded, as well, is UNHCR and other humanitarian and development actors' focus on internet connectivity, which is often termed 'digital inclusivity' in policy documents and practitioner guidance. With this expansion has come a growing recognition of the risks and responsibility of acting as the mediator between refugees and internet connectivity, particularly in terms of actors such as the private sector that became collaborators (UNHCR, 2020a).

This more recent focus on digital responsibility – though rarely termed as such – largely comes from UNHCR's Digital Inclusion Programme, part of the Innovation Unit which brings together projects providing internet connectivity to refugees ('Connectivity for Refugees') with efforts to help refugees be better listened to within UNHCR through digital technology ('Communicating with Communities') (UNHCR, 2022a, 2022d). These strands of work bring together responsibility in multiple ways, with UNHCR presenting internet connectivity as an important right for refugees, that itself as a surrogate state has the responsibility to safely provide, and communicating with refugees as a humanitarian imperative that technology can enable. One 2020 UNHCR policy document evokes the concept of digital responsibility along with clear areas for institutional reflection and learning:

> Understanding how displaced communities find gateways to access the Internet, which factors influence and determine their choices, *what UNHCR' s mandate of protection means in a digital space*, or the extent to which specific technologies or tools can reduce or exacerbate inequalities, will inform and shape future efforts in providing connectivity to refugees in a safe, adapted, and dignified manner. (UNHCR, 2020b) [emphasis added]

Alongside this, a strong focus on digital identity has emerged. In 2017, UNHCR High Commissioner Filippo Grandi stated his aim for every refugee to hold a unique digital identity,

stating that, 'This will enhance accountability and facilitate two-way communication between refugees and service providers' (UNHCR, 2018a). This has been echoed elsewhere in UNHCR as well, such as by UNHCR's Deputy Director of the Division of Programme Support and Management and backed up in programming: 'It is not only logical to promote the digital inclusion of refugees; in the digital age, *a digital identity for all is the only possible way* to make sure that no one is left behind' (UNHCR, 2017) [emphasis added].

This focus is intertwined with a rhetoric of empowerment for refugees. UNHCR posits that digital identity provides internet access, mobile phones and connected services, and that it is through this digital inclusion that 'empowerment passes through': 'Access to jobs, income and remittances, online learning and web-based economic activities will make a difference in the lives of people we care for' (UNHCR, 2017). There are a number of digital identity programmes used by UNHCR, including ProGres, PRIMES and SCOPE (UNHCR, 2018b). However, such programmes have been critiqued for not enabling refugees to access the services they need, and in the manner in which they need to access services (Ungar and Seymour, 2024). Moreover, such systems have been found to restrict interoperability with third-party tools and restrict choice as to how and when such identity systems are to be used.

Regarding data collection by humanitarian agencies more broadly, recent scholarship has identified key concerns including 'organisational data responsibility', defined as the ways different organisations understand (or don't understand) privacy rights and data security practices (Latonero et al, 2019). The growing use of digital and mobile technologies in the humanitarian sector poses a variety of risks for recipients such as refugees, including unauthorised third-party access that can lead to both data exploitation and indeed actual harm for people who have been identified (International Committee of the Red Cross, 2024); the risks more broadly of 'digital by

default' has led to calls for a people-centred security practice that helps users become active participants in security learning (Coles-Kemp et al, 2020).

While digital responsibility in theory lies with organisations collecting data, some research finds that digital literacy and understandings of security management is severely lacking in many NGOs, particularly smaller and more grassroots ones. As one study focusing on Italy explained, 'The risks in the Italian situation stem from organizations that lack the knowledge to protect the information they collect or, if they possess that knowledge at the headquarters level, lack the ability to implement policy to those working locally' (Latonero et al, 2019, p 37). These researchers gave the example of visiting the office of a refugee-serving agency that claimed beneficiary data was secure but which in fact had an unsecured Wi-Fi network and transmitted data via a website lacking basic security/encryption protocols (Latonero et al, 2019, p 37).

Although not commonly invoked in discussions on refugee assistance and protection, the concept of digital responsibility has the potential to be a useful tool as humanitarian organisations continue to grapple with when and how much data to collect, the need for digital literacy by both employees and refugees, how to improve accountability to affected populations through digital means, and how practices of protection and digital responsibility interrelate. If UNHCR and other humanitarian organisations are serious about protecting and upholding refugees' rights and increasing digital inclusion, then centring discussions on digital responsibility – their own and that of States – is an important next step.

Research approach and methods

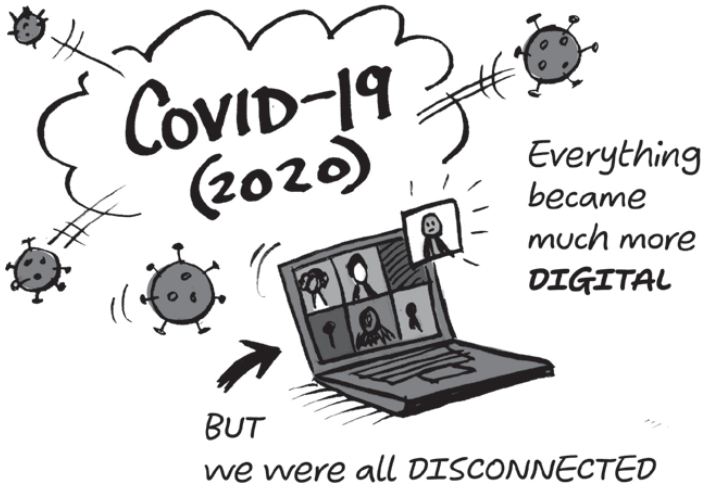
Drawing on semi-structured qualitative interviews, desk-based research and participant observation of monthly meetings of a London-based civil society network focused on digital exclusion, this case study focuses on the 'in between' and

mediating role of digital access and exclusion by refugee-serving civil society organisations in London.

The case study was carried out in the second year of the COVID-19 pandemic when UK society had become widely regarded as a digital-first society where essential and statutory services had become digital-default and where the digital was the foregrounded mode of access for the majority of services. It captures a moment in time when responsibilities emerging from, mitigated with and distributed by digital technologies were a point of discussion in the public discourse. It was also a point at which digital responsibilities with and for minoritised and underserved communities became recognised as an issue of public importance (Coles-Kemp and Hall, 2023). One such community is that of refugees and asylum seekers.

According to UNHCR, as of mid-2021, over 135,000 refugees, 83,000 pending asylum cases and almost 4,000 stateless people were in the UK (UNHCR, 2022e). Even before the start of the pandemic the number of refugees and asylum seekers in poverty in the UK was rising. Research shows

Figure 4.5: The COVID-19 context



that they are less likely to receive vital public health information due to language barriers and digital exclusion; they are also part of a minority population more at risk of severe illness and death from the virus. Barriers to public health information contributed to outbreaks in hostel accommodations in the UK and chaotic government responses to them (Faulkner and Lee, 2022). Refugees are also more likely to suffer from depression and PTSD than the local population. These challenges have been linked to both 'pre-migration experiences' (such as war) and 'post-migration conditions', such as inadequate housing and difficulties with asylum procedures (Porter and Haslam, 2005). The disruption to necessary welfare and health services that were experienced by the local population had therefore an amplified impact on refugee groups, thus making access to digital services vital.

As this study shows, voluntary and third sector organisations are both providers of digital access for refugee groups as well as often neglected actors in terms of government recognition and funding for digital inclusion. Digital responsibility lies both within these organisations as well as within actors such as the UK Government, which must provide further support in the form of digital literacy for refugee-serving organisations, and funding for digital technologies for both refugee-serving organisations and refugees themselves. The following sections present key themes raised in interviews and literature and their links to digital responsibility as it is enacted within the UK context of refugee resettlement.

Findings

The findings reflect three main themes that relate to responsibility and the roles digital technology played during the initial phase of the COVID-19 pandemic for the refugee groups taking part in this study. The first theme reflects the tensions that relate to the operationalisation of digital access in a digitally enabled society. The second theme highlights the

digital responsibilities that were conferred upon voluntary and third sector organisations serving refugee groups and some of the challenges experienced by those organisations in actioning those responsibilities. The third theme considers the importance of trust if digital responsibilities are to be successfully actioned. These findings combine to paint a more nuanced picture of what happens when a State initiates the actioning of digital responsibilities without ensuring that the necessary policy and technology infrastructure is in place for individuals and groups to complete the actioning of those responsibilities. The case study also illustrates how voluntary and third sector organisations step in to absorb and co-ordinate the actioning of digital responsibilities. Above all these findings combine to underscore how difficult it becomes for digital responsibilities to be effectively actioned without a coherent framework that foregrounds and operationalises digital responsibilities.

The right to internet?

Although internet is increasingly considered a public good, with some cities having city-wide free public internet access, the pandemic has shown that this is not by any means always the case. In London, public spaces, like libraries and organisations where refugees and asylum seekers have typically been able to receive a variety of assistance and services such as free Wi-Fi, were shut during the pandemic. To add to this burden, the near overnight shift of services online as well as the digitalisation of normal everyday bureaucracy created a double challenge. Asylum seekers in the UK are not allowed to work and at the time were provided only £37.75 per week by the government. While many of them were previously able to make use of libraries, shopping centres and other public spaces for internet, during the pandemic they were often forced to shoulder these costs alone.

As one member of the UK Red Cross asked, 'Do you pay for phone data to speak to family or help your child

access online classes? Or do you buy food?' One informant explained that some asylum seekers he worked with previously accessed Wi-Fi through a local community centre; when it closed during the pandemic, the only way they could get Wi-Fi was through a nearby bank, often just by standing outside it. 'Can you imagine?' he asked, 'Three or four young people standing outside of a bank for hours. This can seem suspicious, they may seem like they're causing trouble and are gangsters. People will wonder: why are they loitering outside of a bank?'

Although in June 2020 the UK Home Office began providing internet access via SIM cards for asylum seekers in certain accommodations based on Public Health England advice, no smartphones were provided to those that lacked them. During long stretches of the pandemic, social mixing was not allowed, so asylum seekers couldn't even go to each other's rooms in hostel accommodation to use internet through a friend. These and other situations illustrate significant gaps in helping asylum seekers access not only public health information but other crucial services, as well as make desperately needed social contact with family and friends. Even refugees and asylum seekers who do have smartphones often have no contract due to its cost, so instead use 'pay as you go' data as their only access to internet. One informant explained,

> In the past it might not have been so tricky to budget for data because you paid 5 pounds a month for it. But now it is 20, even 25 pounds. People are spending more than they expect. One lady I worked with used to spend 10 pounds per month but is now paying 35 pounds per week. Her language skills aren't very good and she didn't realise she could get a monthly package that would be cheaper.

Refugees and asylum seekers also may not be housed and thus deal with the added intersecting challenges of homelessness.

One informant who volunteers with refugees and asylum seekers as well as homeless populations in London stated,

> Parts of London look like camp site cities, areas completely covered with tents. In all these situations of homelessness you find a lot of immigrants and refugee populations. With the pandemic, homeless people are really struggling with access to services. For example, what happens when you don't have credit on your phone? People assume others have technology, but that's not the case. It has shocked me in terms of the discrimination people are facing.

The Department for Education's schemes to increase children's access to remote education during COVID-19 also extends to refugees and asylum seekers and includes increasing data allowances on mobile devices and providing 4G wireless routers. In this way, the responsibility for providing education was taken by the UK Government, with enabling digital access as the means to do so. However, there has been significant criticism that the scheme has not been extended far enough and that many were left out or under-served. Some informants also mentioned it being common for one family to share one device, such as a laptop, among themselves, with competing interests for school, job searches and social contact with family and friends leading to inadequate digital access.

And having some access to internet does not necessarily equate to having the *right* access. One organisation explained that several refugees they worked with were trying to gain job qualifications or get jobs but were stymied:

> In some instances clients wanted to attend CECS, which is a qualification to work on a construction site, or SAI training (security warden training), but there was a barrier there – they were unable to attend as they needed a laptop with access to Wi-Fi because of the nature of the training.

> Others have been asked to attend a job interview with a laptop – but they didn't have one so they couldn't attend the interview at all!

Such examples illustrate the importance of accounting for restricted or lack of digital access through both increased flexibility and increased provision of necessary technological devices. The evident risk of not doing so is allowing already marginalised populations to be left further behind.

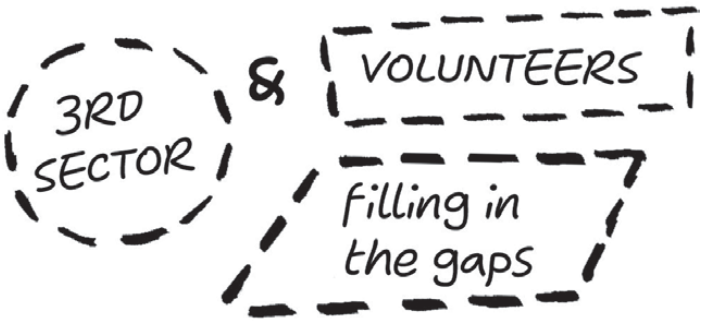
The digital responsibilities of refugee-serving organisations

The shift to remote service provision matters for many reasons. An obvious one is language barriers that can be exacerbated by a lack of in-person assistance. Importantly, the challenge of addressing language barriers remotely is not just one that refugees and asylum seekers must deal with, but those civil society organisations working to assist them. These organisations appear to have both taken on the responsibility to foster digital literacy for refugees as well as had this responsibility in some cases foisted on to them, as refugees increasingly called on them for help navigating UK bureaucracy as it digitised during the pandemic.

Organisations described the initial challenge familiar to many of us of adapting to different technologies, such as launching zoom on a phone or downloading an app, but with the added struggle of explaining this to someone speaking a second, third or even fourth language. One organisation sought to overcome this by involving Arabic-speaking colleagues and using a tactic they referred to as 'nudging':

> We initially wanted to tap into the existing tech and skills that clients had, there was no point in insisting on them using something they didn't know how to use. But we did do some nudging. We asked them, why don't you try to touch this button or try a video call instead of a voice one?

Figure 4.6: Assuming responsibilities



For refugees and asylum seekers themselves, a lack of language skills contributed to a fear of forms that either must be filled out on paper or are hard to access online without help. As one employee of a refugee-serving organisation explained, 'At the beginning, everyone was asking about the office being closed and when it would open again. People wanted help with paper forms – they were used to coming with forms for school registration, GP application, provisional driver's license, and so on.' Whereas previously clients could come to organisations or even sessions at public libraries to receive help with this bureaucracy, once the pandemic started everything had to happen remotely.

Yet some refugees and asylum seekers don't know how to write in English and might not have even gone to school in their home country. For these people, completing anything official or bureaucratic is overwhelming, and they need support for even so-called small undertakings like calling a water company to check about a bill. Many refugees, regardless of literacy, were also confused about changes to council benefits given changes in Universal Credit. This led to an increased reliance on help from organisations that refugees know and trust. One informant described a lengthy process of supporting a refugee who didn't speak English to receive clarification about

Figure 4.7: Bureaucratic complexity

apparent rent arrears; as everything was remote, the employee's colleague had to phone up the council with the client on the line, who had to confirm their identity and approve that someone else was allowed to speak on their behalf. It was only then that the actual issue could begin to be addressed.

There is also a broader issue which extends beyond refugees and asylum seekers: the possibility that some services cannot provide the same duty of care remotely as they can in person. This was mentioned in several interviews regarding social services like mental health support. There were concerns, for example, about the quality of mental health assessments over the phone, particularly for people for whom English is not their first language. This was brought up against a larger backdrop of declining services due to higher levels of demand, as well as the fact that only certain members of populations

were accessing digital and remote services in the first place. As one employee of a charity working with refugees put it bluntly, 'We only [virtually] see the clients that are reaching us. We don't know about those who don't call.'

Digital responsibility and challenges of trust

Many of the challenges mentioned previously feed into a less tangible yet incredibly important one: that of trusting and gaining trust remotely. Several organisations interviewed discussed a drop in client numbers during the pandemic attributable not only to a lack of information but also to a fear by many refugees and asylum seekers of providing personal data online or over the phone (for example, through intake forms) to unknown and thus personally un-vetted organisations. It also was hard for organisations themselves, that had to quickly adapt to new working arrangements while attempting to retain access to clients. As one organisational employee stated, 'It was also a problem for us: how is this going to work? How are we going to communicate with these people and keep them involved in the project?'

Another employee of an organisation seeking to increase refugee employment explained,

> When a potential client used to come to our office, they saw people working there and others getting help. It looks like a charity, it's an actual physical environment – people can talk to someone with face-to-face contact. … When a potential client used to come to the office, they would figure out who they were dealing with, which increased their trust. So face-to-face is very important.

The shift to remote working, which meant that organisations in some cases could only communicate with refugees and asylum seekers over phones and text messages, was described as denying people the opportunity to have more natural human

contact that fosters trust. While crucial for everyone, this is particularly important for forced migrants who often have a deep mistrust of institutions due to past experiences of violence and persecution and may also have significant language barriers that makes remote communication all the more daunting.

Thinking about digital responsibility

Throughout the pandemic, refugee-serving organisations in London took on digital responsibilities by supporting refugees with unforeseen tasks while also dealing with their own digital challenges, be it trying to run their own activities over Zoom or navigating new digital systems and databases for their work. In this way, charities and other civil society organisations, as well as individual volunteers, supporting refugees and asylum seekers in London and beyond played an enormous role in getting people the support they need. As one charity worker put it, 'The third sector helped massively because we were inundated with requests for support.'

While the responsibilities for supporting refugees have been established in law, and there is consensus about the need, these findings suggest there is no consensus about how responsibilities should be actioned in a society that is digital by default. This case study reveals how established responsibilities are not discharged because the actions are refused or avoided. It therefore shows that even if a responsibility is realised and established there still needs to be consensus on what it means for an individual to be response-able to action the responsibility. The study shows that this disconnect is especially profound where there is no enforcement and significant existing barriers to accessing digital services to action the response.

Refugees and asylum seekers in London and in the UK faced digital exclusion as both one challenge among many during the COVID-19 pandemic as well as an exacerbating factor in other challenges. A lack of or limited access to internet due to reasons such as prohibitive costs, lack of devices and lack

of digital literacy all contributed to this population struggling to access the services they need. Language barriers remain significant and heavily impact the ability for many to navigate online bureaucracy without external support.

The case study explored here raises several particular elements of digital responsibility by humanitarian and civil society organisations towards refugees. At the core of these considerations is the notion of responsibility itself in refugee situations. As overviewed in the introduction, by its very definition, a refugee is no longer under the responsibility of their home country, but instead has a host state, UNHCR as a 'surrogate state' (in displacement) or a resettlement country which legally 'takes responsibility' for them. In this light, a lack of responsibility in the refugee context is one inherently related to the breakdown of the state-citizen contract or in fact relates to the lack of fulfilment of the (new) state-citizen contract. This in turn highlights refugee-serving organisations in the third sector as important actors in refugee assistance, which either explicitly or de facto take responsibility for various aspects of helping refugees. The contexts explored here illustrate that just as this responsibility occurs 'in real life' so does it manifest digitally, as well.

While more should be done to support refugee-serving and other civil society organisations in bridging the digital divide, many of the challenges refugees and asylum seekers have faced could in large part be overcome through the government either fulfilling or expanding its promises to provide devices and internet access to those that need them – in essence, by taking digital responsibility. In this context, digital responsibility means first and foremost taking concrete steps to enabling digital inclusion for refugees and asylum seekers, thereby inserting additional digital responsibilities before refugee resettlement responsibilities can be actioned. Some of the digital exclusion experienced by this population could also likely have been avoided through government functions and services remaining open and in-person with safety protocols in place, out of a

Figure 4.8: Responsibilities in bridge building

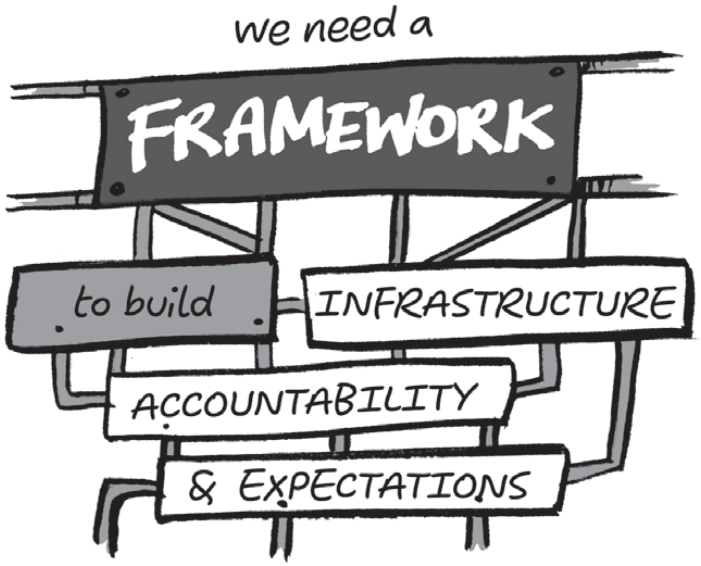
recognition that there are certain segments of populations for whom digital services will never be a good option.

To mitigate the administrative barriers and challenges they experienced, many refugees and asylum seekers turned to the organisations they know and trust. In turn, these organisations supporting refugees and asylum seekers inserted themselves into the responsibilities related to the digital delivery of refugee support services in a bid to absorb these digital responsibilities for the greater good. As the study shows, refugee-serving organisations absorbed these responsibilities by spending significant amounts of time supporting their clients in ways often beyond their existing mandate – while also battling with their own organisational challenges of funding, remote work and an uncertain future. Examples include helping refugees navigate Universal Credit over phone sessions, filling out paper forms online, helping clients access online forms (all often while battling language barriers) and seeking to continue outreach and intake with a significantly digitally disadvantaged population. These refugee-serving organisations are from the voluntary and third sector, in contrast to being community responses or self-organising community networks. Such organisations are, as this study highlights, struggling with

organisational insecurities related to funding, policy status and legal responsibilities.

Some of the situations and challenges shared raise concerns explored in the previous section about organisations' ability to manage data privacy and security. It also builds on past research on UK civil society's ability to manage data, which found that civil society organisations face barriers of limited time, funds and expertise to make use of data (Easton-Calabria and Allen, 2015). Although there have been calls to explore how 'civil society can play a role in shaping the direction and application of technology in policy and development', it is likely in reality that many organisations are struggling to cope, let alone lead, in the so-called digital turn. This is in large part because such organisations do not have a clearly identified position within a digital responsibility framework. However, this is in fact hard to know as civil society organisations are rarely included in

Figure 4.9: A new framework



efforts to measure digital progress in society (Lynn et al, 2022). The findings show that such organisations find themselves in a position of trying to enable minoritised groups to action responsibilities realised and established through an outcomes-based framework. In a bid to become recognised as legitimate partners in this framework, refugee-serving voluntary and third sector organisations try to enable responsibility actions using the same outcomes-based framework. However, the findings suggest that a constitutively based framework might be more effective when working with refugee groups so that they can both build trust and negotiate responsibility actions to take different cultural practices and viewpoints into account.

In contrast to other sectors such as the private sector, where attempts have been made to create frameworks of digital responsibility for practice, no guiding framework of digital responsibility appears to exist for humanitarians and others engaged in refugee assistance. Some work posits that poor data management practices regarding refugees should be addressed through institutional capacity-building, such as including funding for data management systems and trainings into host government support (Schoemaker et al, 2018). At the same time suggestions such as these place the onus of digital responsibility in terms of data security onto host governments, other recommendations focus on the role that UNHCR plays in collecting identity data, such as the creation of a 'multi-stakeholder working group on interoperability chaired by UNHCR … to support a longer-term standards body focused on identity data' (Schoemaker et al, 2018, p 3).

The case study findings indicate that, aside from the digital responsibilities of personal data management, there is little or no recognition by the entities that realise and establish responsibilities for the resettlement and care of refugees that digital-first or digital-by-default policies create additional (digital) responsibilities that need to be inserted into the responsibility framework set out in law for the care of refugees. Instead, there is a greater focus on digital technologies being

used to reduce the costs of refugee care and regulate migratory movement, thereby focusing on a digital responsibility towards indigenous rather than displaced or mobile populations. Digital responsibilities related to the care of refugee groups are, in contrast, almost totally silent.

Conclusion

Several compelling overlaps emerge from both case studies and the wider research, although organisations examined differed in size and scope. First, refugee-serving organisations seem to feel a responsibility to promote the digital inclusion of refugees, even if this is not explicitly within their mandate. Instead, this work towards digital inclusion comes in part through their efforts to provide other services, be it language classes or helping refugees secure jobs. In this way, whether in a context of resettlement or of global displacement, the responsibility to provide access to and literacy of digital technologies often comes out of a wider responsibility to provide support, rights and protection to refugees.

Among other points, this reinforces the centrality of technology to the everyday lives of some – though not all – refugees and asylum seekers and clarifies the importance of further exploring digital responsibility. At the same time, organisations often lack the skills and knowledge to digitally protect refugees the way they intend to, which represents an important area of increased attention related to both digital and 'in real life' responsibility. We would therefore argue that at a minimum, humanitarian agencies should issue guidance for staff to follow data protection and privacy standards outlined by the International Committee of the Red Cross (ICRC) Handbook on Data Protection, which provides detailed information on a range of digital technologies including mobile messaging apps, blockchain and AI to ensure that both risks and good practices are clear (2024). This literacy should also extend to refugees. As one key informant summarised,

> We need more participatory research and to show pathways where digital responsibility can really be implemented. This has to do with granting rights to refugees, such as partnering with actors to redesign pathways of asylum applications or digital asylum hearings. Refugees also need to understand that the digital identity they construct can affect the kind of opportunities and even the kinds of rights that are granted to them. Refugees need to understand how their data is being used. Humanitarian organisations – big and small – are responsible for organising data literacy and digital literacy practices towards refugees.

Second, some of this responsibility appears to come not only from organisations' own ambits or expertise but due to a lack of responsibility taken by others – host states lacking data and privacy protection regulations, the UK Government not fulfilling its own promises for increasing digital inclusion, and so on. How differently might have the work of some of these organisations been if the UK Government had provided smartphones as well as SIM cards to those asylum seekers that needed them, for example, or provided more direct support to civil society organisations working to address these barriers for refugees and asylum seekers themselves? The UK Government must further acknowledge and address the fact that its lack of responsibility-taking is in essence the delegation of responsibility to others with fewer resources to take it on. But responsibilities must not be delegated unless the delegator ensures that the delegated responsibilities are capable of actually being actioned.

From the findings and analysis, a variety of recommendations arise from this case study, which include:

- More government support (responsibility-taking) to help organisations fostering digital inclusion for refugees and asylum seekers in the UK.

- The development of a framework of digital responsibility for refugee-serving organisations that is relevant in international humanitarian settings as well as in domestic resettlement contexts.
- Increased sharing of information with refugees on how their data is used, on the level of online and other surveillance that may exist along migration routes and in countries such as those within the EU or in the UK.
- Further research could explore what the concept of 'refugee-centred digital responsibility' might look like for refugee-serving organisations and host and resettlement states, which places the needs, skills and interests of refugees at the core of digital inclusion, rights and protection today and in the future.