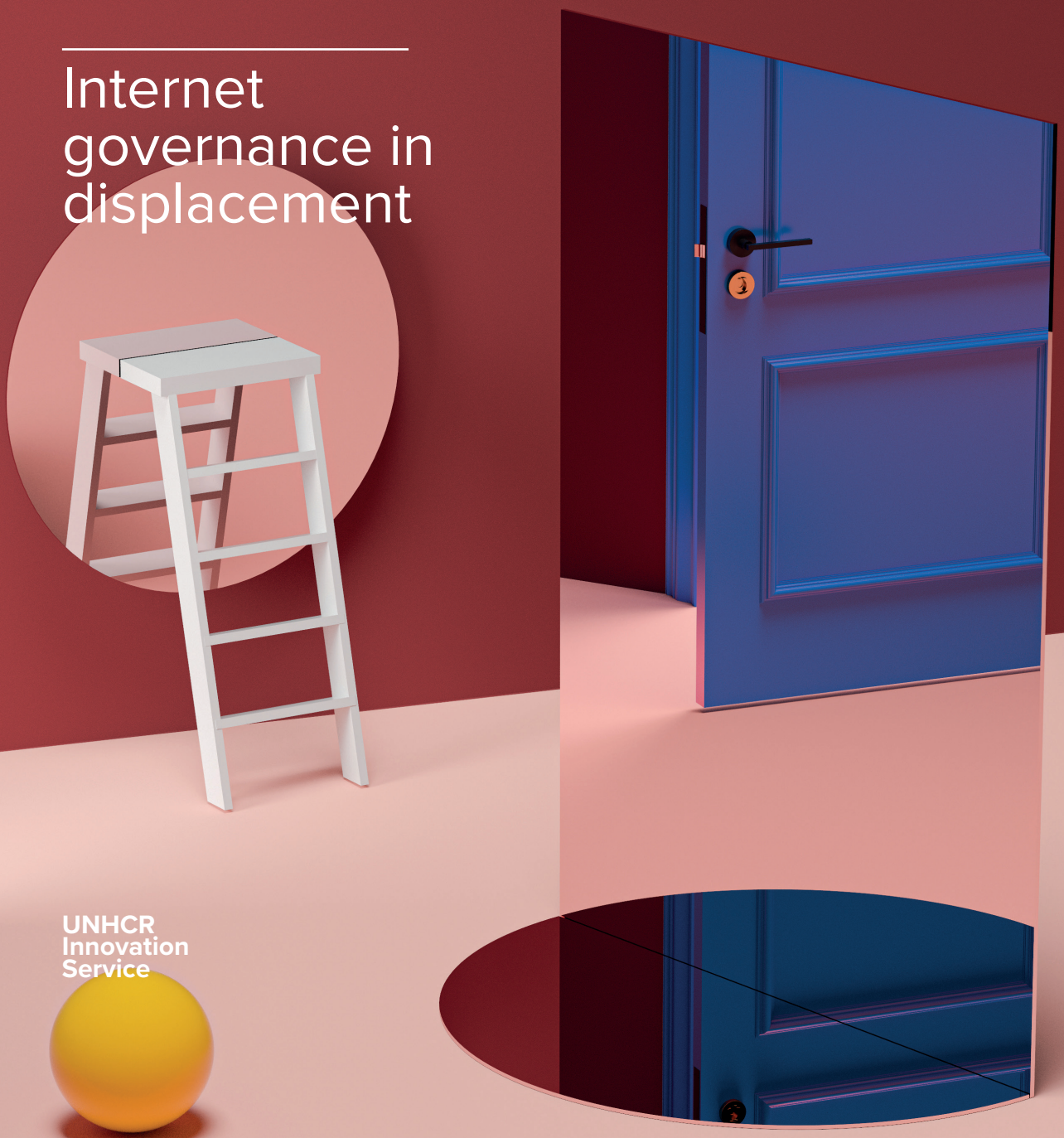
UNHCR
The UN Refugee Agency

Digital Access, Inclusion and Participation

Internet governance in displacement



UNHCR
Innovation
Service

Internet governance in displacement

UNHCR Innovation Service
Digital Access, Inclusion and Participation

Web edition April 2020
Cover art: Jungmin Ryu

Author: Dr. Eleanor Marchant
Postdoctoral Research Fellow, Programme in Comparative Media Law & Policy,
University of Oxford

Made possible thanks to
the generous support of:

LUXEMBOURG
AID & DEVELOPMENT

Digital Access, Inclusion and Participation

2019 Research briefs - an exploration

The initiative previously called Connectivity for Refugees and supported by Luxembourg is as of 2020 called 'Digital Access, Inclusion and Participation'. 'Connectivity for Refugees' exists as a work stream but will start to operate under the name Digital Access, Inclusion and Participation Programme. In this document we refer to the initiative as Connectivity for Refugees.

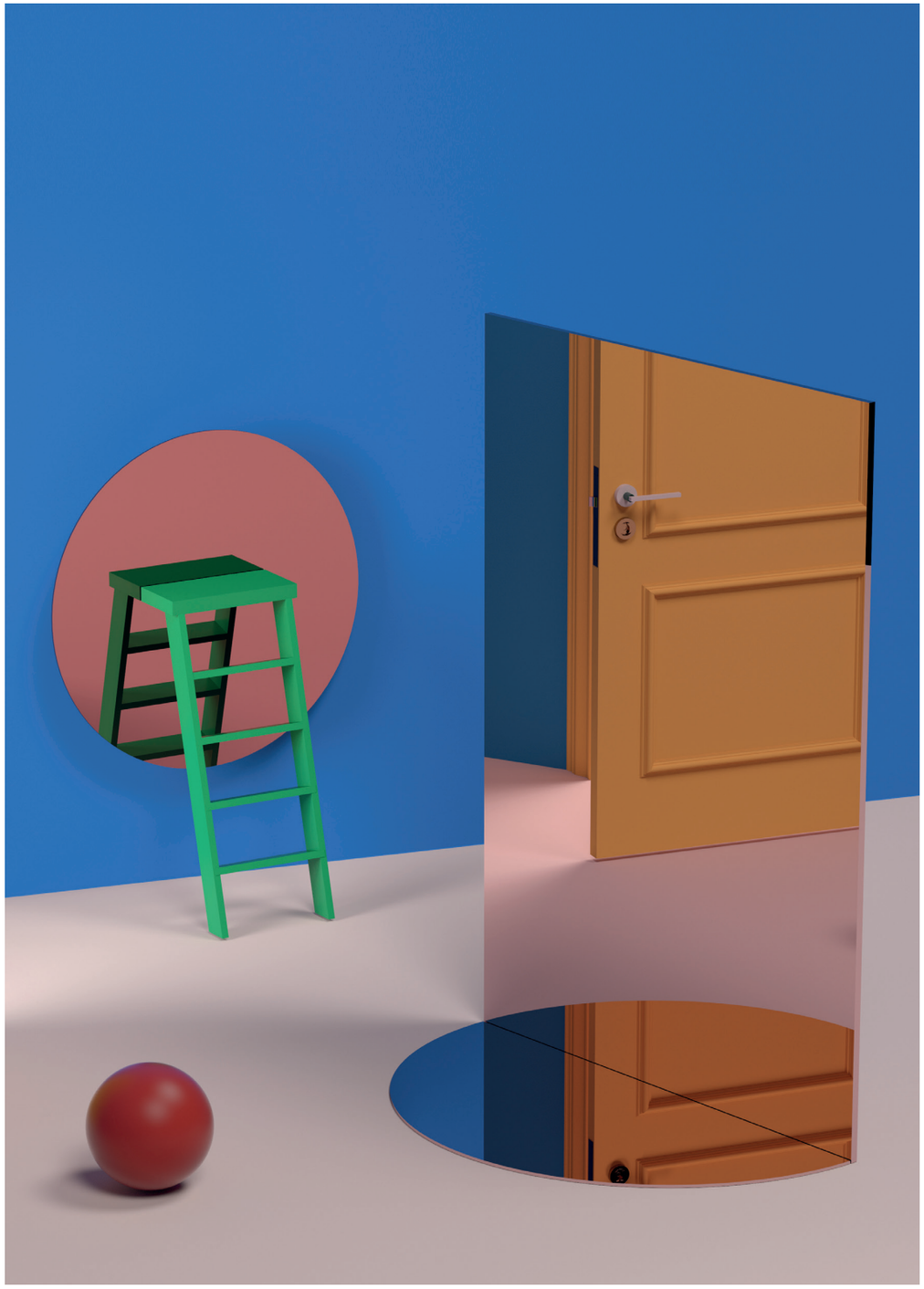
Through research and advocacy, capacity building, field experiments, and strategic partnerships, UNHCR's Digital Access, Inclusion and Participation programme works towards a future where all refugees, regardless of age, gender and diversity, have the right and the choice to access Internet connectivity. It seeks to ensure that refugees' voices are heard in humanitarian programming and that they can leverage connectivity to fully participate in the digital space. The Connectivity for Refugees initiative is part of this programme, and specifically focuses on barriers to digital access inclusion and works systematically across the aforementioned pillars

Research serves as a crucial precursor to bring insights into the complexity of digital connectivity, inform and challenge dominant views and narratives around access and inclusion of displaced persons in increasingly digital societies. The objective of Connectivity for Refugees' research stream is to provide a comprehensive outlook on connectivity, from different angles and different perspectives, to understand how connectivity intersects with other domains and fields.

This research is an exploration and aims to support future experimentation; bringing in topics that are on the margins so that UNHCR remains future-focused and at the forefront of developing trends in connectivity. 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.

This publication is a part of a research brief series where UNHCR's Innovation Service has collaborated with a range of researchers to explore topics including Internet governance, digital transformation, diversity and inclusion. The briefs are all unique and reflect the author's style and individual voice.

Although the team has been extensively involved in shaping the themes and questions, and provided editorial advice, the views expressed in the publication are the views of each author. It is important to note that space was given to the authors intentionally to express their independent views and that these do not represent UNHCR. We welcome differing views and divergent perspectives and believe in the importance of challenging our own thinking, assumptions and ideas. Research offers us a platform to do this constructively and in a manner that is based on evidence and science, that ultimately helps us advance conversations on topics we identify as critical to a more just access and participation in the digital space.



Contents

List of Acronyms

ALA	American Library Association
APC	Association for Progressive Communication
CCTV	Closed-Circuit Television
CIPA	Children's Internet Protection Act
CN	Community Networks
CTEN	Community Technology Empowerment Network
CTA	Community Technology Access
CSR	Corporate Social Responsibility
ETC	Emergency Telecommunications Cluster
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
ICRC	International Committee of the Red Cross
ICT	Information Communication Technologies
IDP	Internally Displaced Person
IOM	International Organization for Migration
ISP	Internet Service Provider
IT	Information Technology
MNO	Mobile Network Operators
NGO	Non Governmental Organization
SDG	Sustainable Development Goal
SRCA	Syrian Refugee Connectivity Alliance
USAID	The United States Agency for International Development
WFP	World Food Programme

Executive summary

The Internet has long been a vital tool for those working to support people displaced by conflict, persecution, or natural disaster, connecting humanitarian workers to one another to aid coordination, and connecting them to data to provide more targeted assistance. But in the last five years, efforts have increased to provide Internet connectivity to a different population – displaced communities themselves – in what is becoming known as **"connectivity as aid".** In practice, this means that humanitarian organizations, like UNHCR, are increasingly involved in the kinds of decisions more frequently faced by governments and the private sector, like where and how to build Internet infrastructure, and what standards to put in place around acceptable use and content dissemination online. In short, they are becoming involved in **Internet governance**, making decisions that require great care when dealing with already vulnerable populations.

Yet, at the moment there is a *lack of information about what Internet governance decisions are currently being made* in displacement contexts as well as a *lack of information that could help inform that decision-making process* in the first place. This report seeks to rectify that. It begins with the central question: What does Internet governance in displacement contexts look like in practice? Through a detailed review of existing publicly-available literature from academics as well as the public and private sectors, it provides an overview of 1) who is involved; 2) what kind of connectivity is provided; 3) the legal context; 4) the decisions that are made; 5) what shapes them; and 6) how they are made in other contexts. The intent is to provide those actively involved in managing Internet networks for refugees, asylum-seekers, and internally displaced populations with an informed basis from which to determine what Internet governance in displacement *should* look like.

Who is involved in Internet governance decisions in displacement?

Even in the simplest context, Internet governance decisions – decisions, for example, about what people can do or see online – involve an overlapping array of actors. Governments make laws about privacy or hate speech; mobile operators decide where to set up infrastructure and what their terms of use will be; and over the top services like Facebook make decisions about what kinds of content are or are not acceptable for their audience. In displacement, even more actors are involved including:

Humanitarian organizations (e.g. UNHCR, Norwegian Refugee Council, World Food Programme, and the International Organization for Migration);
Mobile network operators (e.g. Orange, MTN, SetRight, Safaricom, Zain, Vodafone);
Other private sector companies (e.g. SES, Intelsat, Avanti Communications, Cisco, Ericsson, Inveno, Facebook, Google, Microsoft, salesforce, BRCK, Kakuma Ventures);
Local non-profits (e.g. CTEN in Uganda);
Community Internet networks (e.g. Airjaldi in India);
Funders (e.g. Craig Newmark Foundation, Orr Foundation, USAID, Mastercard Foundation, VISA, and Accenture);
Host governments (e.g. Jordan and Uganda).

Most of the recent efforts to connect affected populations have involved coalitions of actors, like NetHope and the UN's Emergency Telecommunications Cluster (ETC), including many of the partners listed above. With so many different actors, it is often difficult to discern who ultimately has the *authority* or the *responsibility* to make Internet governance decisions.

What kinds of connectivity are being provided?

In most contexts, Internet infrastructure varies in response to factors like population density, education levels, digital literacy, terrain, hardware costs, revenue potential, and the availability of government subsidies. In displacement contexts, these factors are joined by others like: donor appetite, risks from nearby conflicts, and the transience of many displaced communities. These factors may shape decisions about the particular backhaul technology used, including: copper cables, fibre-optic cables, microwaves, cell towers, or satellite connections. Displaced users will most likely access the Internet directly through one of two ways: mobile network operators (MNOs) using 3G or 4G networks or Wi-Fi hotspots, often based in particular sites like hospitals, schools, or community centres. In large sites, like many refugee camps or settlements, the type or quality of connectivity can vary considerably and is rarely evenly distributed.

What is the legal context around Internet governance in displacement?

The legal context surrounding assistance for displaced communities is particularly complex and multi-layered. It can involve formal laws or international conventions, including, international humanitarian and human rights law, laws of host and home countries of those displaced, or laws of countries where humanitarian organizations or other stakeholders are headquartered. It can also be guided by norms embedded in important but less enforceable policies, like the Sustainable Development Goals, humanitarian operations guidelines, and ethical codes like "do no harm".

The legal context surrounding the governance of the Internet is equally complicated. Even in the simplest situation, there are unresolved debates about issues like privacy, surveillance, hate speech, and the responsibility of various actors from governments to social media companies to make decisions and to protect people online. Globally, we are seeing the rising power of private companies unilaterally making decisions alongside government efforts to curtail such power. We are also seeing efforts to provide universal access alongside very different beliefs about what is needed to ensure safety and security once online.

What Internet governance decisions are currently being made?

For private companies working to connect people, like MNOs and other Internet service providers (ISPs), Internet governance decisions are often laid out in publicly available policy documents like privacy, fair, or acceptable use policies. For many ISPs, *privacy* policies allow them and the government to collect data about their users for "security", including protecting against attacks from militant groups. *Fair use* policies typically limit "disproportionate" bandwidth usage, restricting access for those who exceed certain limits. *Acceptable use* policies typically detail the kinds of content that are restricted, such as illegal, "offensive", "obscene", or "indecent" material, terms that are highly subjective and usually ill-defined. While most operate with some kind of acceptable use policy these documents are not always made public.

Most current connectivity as aid projects provide insufficient information – about what kinds of filtering, usage, or privacy practices are being implemented. From the little information that is available, we can ascertain that malware and virus protections are often put in place, along with content blocking for "quality and security", and even extending "parental controls" beyond underage users. There is an urgent need for more transparency about what kinds of content are restricted and why, particularly for the users themselves.

What informs these decisions?

Internet governance decision-making in displacement will vary depending on which stakeholders are involved. Private sector ISPs are typically profit-driven, while humanitarian organizations are typically mission-driven. The need for humanitarian organizations to "do no harm" also creates a more pressing need to reflect on potential risks and benefits of Internet connectivity. Beliefs about potential *benefits* include connecting refugees with family, friends, reliable information, and livelihood opportunities. While there is ample evidence that the Internet helps connect people, existing research raises doubts about the Internet's role as a source of *reliable* information, particularly with the spread of misinformation. Beliefs about potential *risks* include exposing displaced communities to dangerous content (like terrorist propaganda or pornography), hostile actors (like traffickers, fraudsters or hostile governments or militias), and mental health risks (like addiction or social isolation). While there is limited evidence that refugees seek out terrorist propaganda online, research indicates that the Internet may actually provide important psychological support for individuals disconnected from offline social networks, but there is also evidence that it exposes them to traffickers. Overall, views about potential risks and benefits are highly subjective and require more research.

What can we learn from Internet governance decisions elsewhere?

Looking at other cases where Internet access is provided for non-profit-seeking reasons – including in pre-digital refugee camps, community technology access centres, public libraries, and community Internet networks – it is clear that such decisions are often motivated by a combination of the legal frameworks and deeply-held beliefs, about things like the right to access information or the right to privacy, or even beliefs about the necessity of government surveillance. In some cases, where Internet regulations contradicted beliefs, Internet providers found ways to circumvent them or to advocate for change. The experience of community-led Internet networks demonstrates the potential for having end-users – the displaced communities themselves – more involved in Internet governance decision-making, while the experience of public libraries demonstrates the importance of making privacy and acceptable use policies clear and readily available.

Recommendations

The research compiled for this overview of the state of Internet governance for connectivity as aid in displacement leads to recommendations about: 1) how to improve the decision-making process for Internet governance in these contexts; and 2) how to better communicate these decisions to the public. To improve the decision-making process:

1. More evidence is needed about the real effects of Internet access in these unique contexts;
2. More clarity is needed about which stakeholders are responsible for making which Internet governance decisions;
3. More reflexivity is needed about what risks are being, and should be, considered, and what informs those decisions;
4. A better record of how decisions are currently made is needed to help inform those in the future; and
5. More effort should be made to integrate end-users – displaced populations themselves – into the decision-making process through things like feedback mechanisms.

To improve how decisions are communicated:

1. Sector-wide guidelines specifically about Internet governance in displacement, like the International Committee of the Red Cross (ICRC)'s Handbook on Data Protection in Humanitarian Action, should be put in place to help decision-makers; they should be adaptable to reflect different contexts;
2. Privacy, fair, and acceptable use policies should be written clearly and made publicly available on websites and landing pages so displaced users can see them;
3. A mechanism should be put in place to enable displaced users to appeal content filters or other Internet governance decisions.

Research Brief

Introduction

Throughout the Syrian civil war, social media platforms, like YouTube, have been sites of contestation over how the conflict has been represented, documented, and perpetuated. Extremist groups frequently upload graphic videos depicting the ongoing violence intending to recruit new members to their cause. YouTube has responded by introducing take down policies that prohibit the dissemination of such content (YouTube, 2019), by deploying machine learning algorithms to identify and automatically remove them, and by launching redirect methods to provide counter-narratives to those searching for extremist content (Counter Extremism Project, 2018). Many government policymakers have said such policies are promising but insufficient, and need to focus more on taking down all such content within an hour (Porter, 2019). By contrast, human rights organizations like the Electronic Frontier Foundation and the Syrian Archives, have argued that YouTube is in fact too quick in its take downs. They report that many accounts created by human rights defenders to document and publicize violence as it happens have been mistakenly taken down, resulting in the loss of important records of these atrocities. In such a situation where both the risk of perpetuating offline violence and the risk of losing vital records of rights violations are present, what is the correct balance between the two? What is a reasonable and proportionate decision about what to filter and what not to on the part of YouTube?

As in the case of YouTube, social media companies receive by far the most media attention when it comes to these delicate decisions about what kinds of content the public should have access to when they go online. But they are not the only ones making these decisions. What an individual has access to online is filtered through many layers of decision-makers. This begins with governments creating legislation about what should or should not be accessible, ranging from policies promoting universal Internet access, to policies restricting particular content, like hate speech, to more extreme policies that give the government the right to shut off the Internet completely in certain circumstances. But it also extends to ISPs and public Wi-Fi hotspot sites like libraries or restaurants, who interpret and often go beyond legal provisions to create their own fair and acceptable use policies about what is acceptable on the network they manage.

What informs the decisions made by these various stakeholders about what kind of Internet people should have access to? How do conflicting perceptions about potential risks – from incitement of offline violence to erasure of important human rights documentation – inform access and filtering decisions?

While such questions are pressing in any context, they are particularly urgent in the effect they have on those displaced by conflicts, like the one in Syria. Refugees and internally displaced people (IDPs) have a more urgent need than most to use the Internet to communicate with family members or to access accurate information about resources or routes. At the same time, they are often subject to more restrictions than most. Often moving across borders and lacking identity documents (IDs), many refugees struggle to access the Internet through traditional mobile network operators (MNOs) due to cost and ID requirements; and where they have access to free public Wi-Fi in refugee camps and settlements, they are often subject to an additional layer of content

filtering decisions made by the organizations that manage the camps or Internet cafes within them and their Internet networks.

For those displaced by conflict, there is ample evidence that the Internet is a vital resource, from connecting with families, gathering information about the state of the conflict back home, and helping with integration into a new community (Marlowe, 2019; Xu & Maitland, 2016; Yafi, Yefimova, & Fisher, 2018). But there is also increasing concern about the risks that come with accessing the Internet, like propagating real offline violence as in the YouTube case above. Other concerns include exposing refugees to human trafficking networks, or exposing child refugees to abuse by pedophiles or even exposing vulnerable populations to surveillance by hostile actors or to exploitation by fraudsters and other clandestine actors (UNHCR, 2017; UNHCR South Africa, 2019).

While some of these risks represent very real threats, for most, the current evidence available is inconclusive. And yet they often inform how social media platforms, government, and ISPs all make decisions about what kinds of access and what kinds of content are necessary or acceptable for people to have around the world or for refugees in particular to have access to.

In recent years, efforts to connect people affected by conflict to the Internet have increased within the humanitarian sector. Humanitarian organizations like the United Nations' (UN) Emergency Telecommunications Cluster (ETC), and technology companies, like Ericsson, have long provided Internet infrastructure to support humanitarians in their work in remote areas including in refugee camps (Ericsson Response, 2018). But that infrastructure support has often been limited to providing access to the relief workers themselves. That has begun to change. In 2012, NetHope – which brings together nonprofits, technology companies, and funders focused on using technology to solve humanitarian challenges – led a project to bring Internet connectivity directly to those living in Dadaab refugee camp in northern Kenya (MacRitchie, 2013). In the following years, this kind of **"connectivity as aid"** work – in which target recipients of the Internet support are displaced communities themselves – has slowly grown. The Connectivity for Refugees initiative at UNHCR, the UN Refugee Agency, started in 2016 (UNHCR, 2018), was designed with precisely this objective, as was ETC's own project known as "Services for Communities" that prioritizes providing technology solutions, including network connectivity for communities experiencing conflict.

When networks like DadaabNet are set up, decisions are made about where infrastructure should be located and what kind content should be transmitted over the network. And yet little is known about precisely what decisions are made, who is empowered to make them, and what policies, practices, beliefs, and values inform these decisions. The acceleration of "connectivity as aid" initiatives, particularly for communities displaced by violent conflict or natural disasters makes it a key moment in which to pause and reflect on the implications of this connectivity work and the rights and responsibilities when providing access. To facilitate this reflexive process, we adopt the term "**Internet governance**" to help make the decision-making processes around Internet access and management that affect displaced populations more tangible. We adopt the definition of Internet governance used by Georgia Tech's School of Public Policy, which describes it as "the rules, policies, standards and practices that coordinate and shape global cyberspace" (2019). Most often, this term refers to international or State-led policy-making around things like free expression online, cybersecurity, and online surveillance. But while States make the formal laws that govern the Internet, they are not, as we will see, the only actors making policies and decisions that affect

how people experience it. As a result, this research brief is driven by the question: **What does Internet governance inside sites of displacement, like refugee camps, look like in practice?**

This research brief is intended to provide an overview of what is currently known about the many layers of decision-makers who currently shape Internet governance in displacement contexts. It is also intended to provide guidance for those seeking to create policies for decision-makers about what content should or should not be accessible and how users can or should interact with networks in displacement context. For those setting up and managing networks, it should help navigate the complex decision matrix around how to balance the important benefits to communities of being connected to the Internet, against the potential of exposing them or others to new risks.

To do this, we begin by mapping out the current landscape of connectivity as aid, including: 1) the various stakeholders involved; 2) the laws and law-like norms in which they operate; 3) a sample of the Internet governance decisions being made; and 4) a sample of the beliefs that are shaping these decisions, including beliefs about the benefits and risks that the Internet poses. We conclude by looking comparatively at how Internet governance decisions have been made in other contexts, including public libraries, community networks, and even pre-digital refugee camps. While contexts differ greatly, these cases are intended to generate discussion and reflexivity within the connectivity as aid sector about existing Internet governance practices. By the end, readers should have a greater awareness of the complexity of the factors involved in Internet governance for refugee communities, and should have a basis from which to make more informed-decisions about Internet governance in complex displacement contexts.

Mapping the current landscape of Internet governance in displacement

The focus of this research brief is on examining *who* makes Internet governance decisions that affect displaced communities like refugees, *what* those decisions are, and *how* and *why* they *are* – or *should be* – made. It is not a comprehensive look at all of the factors that enable refugees to access, or restrict them from accessing, the Internet. Other aspects of this have been examined effectively elsewhere (GSMA, 2019; UNHCR, 2019) showing how factors like gender dynamics and identity document (ID) requirements affect refugees' ability to access the Internet. We begin, in this section, by looking at the *who* and *what* of Internet governance for displacement. We look first at the different kinds of stakeholders that have been involved in building and managing the infrastructure for Internet networks for displaced communities; followed by a look at the laws and policies that affect how Internet access is provided to these communities. We bring these together by looking at a case of a coalition setting up Internet access for Syrian refugees in Europe and examine what Internet governance decisions were made.

Who's involved in connectivity in displacement?

Much of the recent work to connect displaced communities to the Internet has been defined by collaborations between humanitarian, government, and private sector stakeholders. For example, a United Nations' network called the Emergency Telecommunications Cluster (ETC) – which brings humanitarian organizations, like UNHCR, together with local NGOs, private sector companies and donors – is primarily responsible for leading connectivity efforts for internally displaced communities, or for those displaced by natural disasters (ETC, 2019). Whereas responses specifically focused on refugees are often led by UNHCR itself, or a consortium called NetHope. For example, DadaabNet – a project to bring low-cost high-speed broadband Internet to the over 200,000 residents (UNHCR Kenya, 2019) of the Dadaab refugee camp in northern Kenya back in 2012 – was led by NetHope, funded by the USAID Global Broadband and Innovations Alliance, UNHCR, Microsoft, Cisco, Craig Newmark Foundation, and the Orr Foundation; drew on private sector partners like Cisco and Inveneo to design the network architecture, and provide the hardware; worked with Kenyan ISPs, including Orange, SetRight, and Safaricom to develop discount pricing and a competitive Internet ecosystem for Dadaab; and worked with non-profit partners including the Norwegian Refugee Council, USAID, UNHCR, and the World Food Programme (WFP) to measure impact and provide hosting and logistical support (NetHope, 2019a). Similarly, an ongoing project called the Smart Communities Coalition, led by Mastercard Foundation and USAID launched in early 2018 with a network of 35 partners to deliver essential services, including Internet, to refugees and host communities, focusing initially on camps and settlements in Kenya and Uganda (Mastercard Foundation, 2019). While this project is still in the early stages, it is indicative of how such collaborative efforts have played a large part in the connectivity as aid work to date.

Private sector companies – from local MNOs and start-ups to international satellite companies, and international hardware, software, and platform corporations – have played a number of different roles in these initiatives. Local MNOs with pre-existing infrastructure nearby are enlisted to extend their infrastructure into camps or otherwise reduce the costs and barriers to access to their networks for refugees, often facilitated by GSMA, the global association of mobile network providers. For example, Zain, a prominent mobile telecom company in the Middle East, has worked with UNHCR to provide unlimited minutes on calls between refugees and UNHCR in Jordan and to provide discounted rates for Syrian refugees on voice, SMS, and data on their network (GSMA, 2017c). Similarly, Vodafone installed a new 3G tower in a refugee camp in Tanzania in 2016 that it has since agreed to share with other local MNOs to reduce the costs of providing access (GSMA, 2017a). Satellite companies like SES, Intelsat, or Avanti Communications, can also be involved as technical partners where camps are particularly remote and hard to reach for terrestrial broadband. Some do so as part of the corporate social responsibility initiatives as with Avanti's work in 2019 delivering free broadband connectivity to a Ugandan non-profit that educates orphans and refugees in Bidi Bidi (Global Business Coalition for Education, 2019). In the case of large multinational companies, IT companies, particularly Cisco and Ericsson, have divisions (Cisco Tactical Operations and Ericsson Response respectively) specifically set up to help deliver Internet infrastructure in conflict or disaster relief contexts. Large software and social media companies like Facebook, Google, and Microsoft have also become involved both through funding others in their work and through more hands-on collaborations. For example, Facebook provided funding to support Zain's Wi-Fi connectivity work in Jordan (GSMA, 2017c), while Google.org has given millions in grants to nonprofits working to connect Syrian refugees (Maganza, 2017). Microsoft, in addition to funding projects like DadaabNet, has also taken a hands-on approach through its Airband Initiative to develop TV white space technologies to improve rural connectivity and has piloted it to help connect a refugee camp in Malawi (Ghelli, 2017). Google and Facebook have both also been involved more in the infrastructure side of the Internet, including financing new underwater fiber cable construction (Shapshak, 2019), and delivering Internet to a wider area through hot air balloons, like Project Loon, a subsidiary

of Alphabet, currently being piloted for commercial viability in Kenya (Etherington, 2019), or low earth orbit satellite constellations that promise more affordable Internet than traditional satellites (Shieber, 2019). While these technologies could theoretically cover wide areas that would help those in transit displaced by conflict, they have not yet been used in connectivity as aid initiatives. For profit startups have been known to get involved in connectivity as aid work as well. In Kenya for example, the local hardware startup BRCK was involved in the DadaabNet project by providing portable modems to facilitate connectivity, and a company called Kakuma Ventures is working to develop a project to install Wi-Fi hotspots in another refugee camp in Kenya (Zimmerman, 2019).

International humanitarian organizations and local NGOs also play an important role in these initiatives. Many of the sites intended to support displaced communities, like refugee camps, are managed by international organizations like UNHCR, and many also provide important funding for specific connectivity initiatives. For example, in NetHope's work connecting Syrian refugees in Europe, when funding from private sector partners ran out, the International Organization for Migration (IOM), a UN Agency, stepped in to provide support (NetHope, 2019e). In many cases, other organizations, such as local NGOs, also play a role in managing particular sites like community centres or Internet cafes where refugees go to access the Internet. For example, in Rhino Camp in northern Uganda, CTEN – a local grassroots organization that grew out of a South Sudanese refugee community and has been funded by UNHCR as well as individuals and diaspora donations (Batali, 2019) – manages a multipurpose community technology centre that, among other things, provides refugees with Internet access, phone repairs and mobile banking services (Batali, Christopher, & Drew, 2019). While the technology companies bring the technical expertise, these organizations bring a greater understanding of the logistics, the situation on the ground, and the information needs of those working and living in the camps. International humanitarian organizations often have staff with extensive experience working in particular communities, though they are also often limited by their size and bureaucracy in their ability to translate that knowledge into evidence-based Internet governance decision-making. By contrast local NGOs, particularly those started and run by refugees, are inherently embedded in the refugee communities and tapped into their particular technological needs, and because of their size are often better able to practice in response to community feedback.

With so many different actors involved, it is often difficult to discern who ultimately has the authority to make Internet governance decisions about things like where access should be set up in a refugee camp or whether or not to restrict access to particular website like YouTube or particular types of content like pornography. For a refugee logging into a network, there is limited transparency about what those decisions are and who has the authority to make or change them.

What kind of connectivity is provided?

When a decision is made to connect a particular location to the Internet, other decisions remain about what kind of network should be set up. Variations can result from a number of different factors including perceptions about the target populations (things like data needs and digital literacy levels), geographic factors (like the region's topography or population density), or other things like local existing Internet infrastructure, and even which technical partners are interested in being involved.

The most common types of networks chosen are mobile networks and Wi-Fi hotspots. Mobile networks are set up by the MNOs and allow refugees to connect directly to their service using their mobile phone, as in the case of Vodafone's mobile towers in Tanzania. By contrast, Wi-Fi networks are usually set up in specific locations like community centres, schools, or clinics, as in the case of NetHope and UNHCR's work to connect sites that Venezuelan refugees traveled through in Colombia (NetHope, 2019c; Suardiaz, 2019). They are usually connected to the Internet through a variety of backhaul technologies, including terrestrial fiber or older copper cables, microwaves, or satellite link, each bringing its own advantage and limitation. For example, fiber cables offer particularly fast broadband access, but can be time-consuming to lay, making it unappealing in remote locations. A third type of network, a community network – where communities build their own network to connect to the Internet – is still quite rare in displacement contexts. One example, however, is Airjaldi, a non-profit community network in India that actually began life as early as 2005 as a project to connect a Tibetan refugee community that the existing commercial ISP, AirTel, had overlooked (RCRWireless News, 2016; Riemens, 2011). Like many other community networks, Airjaldi enlisted the help of the community to build the last-mile infrastructure needed to connect the community to the main ISP's network and bought bandwidth directly from the ISP.

Additionally, Internet infrastructure to connect refugees can be further affected by the wide variety of geographies in which they find themselves. For example, some refugees settle in densely populated urban areas with well-established Internet infrastructures, while others are in camps or settlements that while densely populated are often in very remote rural areas, making terrestrial fiber connectivity difficult. Others, like those fleeing violence in Venezuela, are constantly on the move. The topography, particularly how hilly a region is, creates further challenges for network engineers as many of the more affordable technical solutions, like microwaves, require line of sight to work properly. Similarly, for large or very dispersed areas, like some camps or settlements, multiple solutions may be used providing different levels of connectivity throughout. For example, in Kakuma refugee camp there are two cell towers that were installed by the largest MNO in Kenya, Safaricom, but they are insufficient and are only able to provide 3G and 4G coverage to two zones in the camp, while the other two are limited to 2G coverage at best (HIF, elrha, & Samuel Hall, 2018). There is also a handful of Wi-Fi hotspots in Kakuma, including in the base camp from which the camp staff work and ad-hoc hotspots set up by entrepreneurial refugees (Lambropoulos, 2019), but at the moment, more than 95% of refugees living in the camp who go online do so using mobile networks (HIF et al., 2018).

Finally, much like the general population, those fleeing conflict or persecution can vary widely in their access to, and familiarity with, mobile phones and other devices necessary to get online, which can lead to variations in how much bandwidth they may need or want. Some, like those escaping civil war in Syria – where the Internet penetration rate is 30% even with the ongoing civil war – have particularly high exposure to smartphones and experience using them (GSMA, 2017b). Others like many internally displaced in Chad – where the Internet penetration rate is just 6.5% (Internet World Stats, 2019) – have never owned a phone. For most connectivity projects, private ISPs use data they have collected about a population's existing data usage to inform what kind of network they want to build and where. Such data is much harder to come by for transient displaced populations; as a result, technical network decisions about bandwidth requirements for displaced populations must be informed by more of a best-guess approach.

All of these factors – the type of location, the type of network, the type of technological needs, and the layers of actors involved in setting up and maintaining a network – can influence how Internet governance decisions are made, and by whom. For example, when a refugee connects directly to an MNO-provided network, they will be accessing through the MNO's own fair and acceptable use policies. By contrast, for stationary Wi-Fi spots, the technology company involved in setting up the infrastructure, the satellite company providing the network, and the organization managing the site may all have some influence over the governance of that network. For example, for a network Cisco was involved in building and maintaining, they would typically be able to restrict access to streaming platforms if they were concerned about the bandwidth requirements overloading the network. While the private sector companies often manage the networks in this way from a technical perspective, more substantive decisions about access to particular kinds of content are usually made by or in partnership with the humanitarian organizations and local NGO partners that manage camps, computer centres, or other sites through which refugees pass. For example, at the community centre managed by CTEN in Uganda, it is CTEN that has the primary responsibility of maintaining the network and determining what the terms for using that network should be (Batali et al., 2019).

What laws and policies shape connectivity in displacement?

In many ways, the legal context in which connectivity projects operate shapes them as much as if not more so than difficult terrain like mountains that they must cross. It can also be more complicated than physical terrain to identify and address. While local State laws certainly apply, the legal context in which refugee assistance operates is decidedly plural. It is affected by other laws, like international humanitarian and human rights laws, as well as by less visible socio-legal norms that shape the policies and guidelines for the humanitarian sector, as well as similar norms embedded in the cultures of host countries and the cultural communities of refugees themselves.

While all work with refugees faces this overlapping and hybrid legal landscape, work specifically with the Internet is further complicated by the extremely variable nature of modern Internet governance. For many of the early creators and adopters of the Internet, the principles of free and unfettered access to information are intrinsic to the platform. Yet more recently, the desire to have more sovereign control over the shape of the Internet within national borders has led to more walled gardens, firewalls, censorship, and even in extreme cases Internet shutdowns. Even for those who believe in the open principles of the Internet, the rise in incidents that appear to be fueled by the spread of hate speech or terrorist propaganda online, particularly through social media, has led to increased acceptance of the need for legislation to restrict the proliferation of certain kinds of content online. Those working in connectivity as aid are confronted by a profound lack of legal certainty about how Internet governance decisions should be made. While it is of course essential to understand the local laws of countries hosting refugees, it is also extremely useful to look at some of the trends in Internet governance globally, both to help prepare for future changes, and to make the best possible governance decisions for the refugees being connected.

Fundamental to all UNHCR work with refugees are the 1951 Convention relating to the Status of Refugees and the 1967 Protocol, both of which reinforce the right of people to seek asylum, from Article 14 of the Universal Declaration of Human Rights, and create a humanitarian obligation to

protect people fleeing persecution. While these early texts of course make no mention of the Internet, in 2016 the UN General Assembly adopted a non-binding resolution regarding "the Promotion, Protection and Enjoyment of Human Rights on the Internet" (UN General Assembly, 2016) extending the protection of human rights to the online world. It is a fair interpretation that the obligation to "protect" refugees also extends online, creating an obligation to protect them from online as well as offline threats. More recently, the Global Compact on Refugees was affirmed by the UN General Assembly, which calls for international cooperation to support refugees in a more sustainable way. Among its four key objectives is the goal of enhancing "refugee self-reliance" (UN General Assembly, 2018). Providing refugees with Internet access could certainly be seen as helping refugees to become more self-sufficient by providing them with tools to access information directly.

Beyond the refugee context, there is an ongoing debate about whether access to the Internet should be considered to be a human right. For many, the Universal Declaration of Human Rights' provision in Article 19 for the right to "receive and impart information and ideas through any media and regardless of frontiers" (UN General Assembly, 1948) creates an obligation to connect more people around the world to the Internet. While the Declaration does not mention the Internet specifically, its mention of "any media" has created a foundation from which many have argued that Internet access should itself be treated as a human right (Reglitz, 2019). A number of States have also adopted this position, including Finland in 2010 (BBC, 2010) and Estonia as early as 2000 (Borg Psaila, 2011).

While not going so far as to agree that Internet access itself should be a fundamental human right, the increasing efforts we have seen in the humanitarian sector to provide connectivity for refugees are reflective of a policy shift in the international community towards prioritizing universal Internet access. Goal 9 of the United Nations' 2015 Sustainable Development Goals is "Industry, Innovation and Infrastructure", which includes universal Internet access. It sets a target to "significantly increase access to information and communication technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020" (UN Sustainable Development Goals, 2019). Refugees are an important target community of this kind of universal access policy. Separately, a group of independent experts created a Global Broadband Plan for Refugees, which proposes increasing international collaboration in order to address the access, adoption, and usage gaps for refugees (B. Levin & de Sa, 2019). While this is not a binding legal document, it does reflect desires to create more policies that support universal access initiatives for this particularly vulnerable population.

Beyond the refugee context, the landscape of global Internet governance is currently defined by a number of juxtaposing trends. First, we have seen the rising power of private sector Internet companies (now actively involved in promoting connectivity, whether for corporate social responsibility initiatives (CSR) initiatives or genuine interest in increasing customer base or access to data), alongside stronger national approaches to internet regulation that seek to curtail the power of these Internet companies (Radu, 2019). At the same time, we have seen a trend towards increasing universal access, while also seeking to ensure people, and the networks they use, are secure once connected. For example, many governments have implemented universal broadband plans accompanied by universal service funds that provide financial incentives to ISPs willing to

connect more remote regions. This includes many countries that host refugees, like Kenya and Uganda. At the same time, an emphasis by many States on the need to protect "security" can vary widely in practice, ranging from parental guideline policies to protect children to more restrictive policies intended to curtail "immoral" behavior online. For example, Uganda has also policies, like a controversial tax on social media usage, intended to curb excessive time spent by Ugandan youths on these platforms and the spread of false information (Schlindwein, 2019), while other countries like India, Sri Lanka, and Cameroon have at times decided to cut off access to the Internet entirely for fear of online behavior leading to offline violence. Below, we look at two important trends in State-level Internet governance decisions that give a good illustration of how and why policies are adopted that limit peoples' experiences online.

Content moderation trends

As with many of the media that preceded it, the Internet has also been surrounded by concerns about how its use could harm children. Such concerns have proliferated in recent years, particularly around matters like cyber bullying, screen addiction, and sexual abuse as well as exposure to pornographic content. These concerns have led to content filtering in schools in many parts of the world and to guidelines for parents on how to support safe use of the platform. But it has also led many ISPs to extend such "family friendly" content filters to the public Wi-Fi access points they control, limiting access to often unspecified "harmful" content for adults and children alike (Spacey, Muir, Cooke, Creaser, & Spezi, 2017). While this may protect children, others, as we will see later on, would argue that it is also infringing on the right of adults to have unfettered access to information.

The dissemination of hate speech and content that incites violence is another area of concern for many legislators of the Internet, and increasingly so. While traditional media, like radio, have long been monitored for their potential role in such dissemination as well, many legislators worry about the speed with which information spreads online and about the challenge of curtailing dissemination in such a decentralized system. This concern grew horrifyingly real after the live streaming of an attack on a mosque in Christchurch, New Zealand, became virtually impossible to permanently remove from the Internet. Even with Facebook content moderators belatedly removing the video, others continue to simply re-upload copies of it to the platform many months later (Solon, 2019). Internet companies, like Facebook, typically prefer to moderate the content that appears on their platforms in-house rather than have governments decide what content should be accessible. They make their own internal policies, like "community standards" and often employ third party firms of human content moderators combined with internally developed Artificial Intelligence (AI) tools to proactively take down content before or soon after it is published. But they do so in ways that continue to be largely non-transparent and unaccountable to the public.

However, in recent years governments have moved towards greater regulation of online speech, including on social media platforms, like Facebook. For example, even in the USA, where First Amendment protections of freedom of speech pervade much of American legal culture, discussions have begun about what methods, including regulation, are necessary to stem the flow of hate speech, including from white nationalists, online (Romm, 2019). Given this increase in discussion about how the responsibility of addressing the challenges posed by online hate speech should lay with government regulators instead of private sector technology companies, it is likely that a number of new regulations will be passed in this area in the years to come.

As we will see in greater detail later on, the balancing act between protecting users and enabling their human right to access information is a constant challenge for regulators, online platform companies, and Internet providers and administrators alike. However, it is often unclear whose ultimate responsibility it is to do so. Are ISPs legally responsible for content disseminated over their platforms? Are social media companies? Facebook alone is a good illustration of the contradictions that lie within this debate. It has historically argued that it is just a "tech platform", often in order to shift the responsibility for content published on its platform away from itself and to its users. At the same time, it retains a vast amount of content moderation authority in its community standards in-house, and in a recent court case in the US argued it was indeed a publisher in order to protect its "editorial decision" to remove third party apps from its platform (S. Levin, 2018). Yet, in 2019 the company began calling for more State regulation around things like harmful content on its platform admitting it was beyond its capacity to do so (Isaac, 2019).

By contrast, some laws actually put responsibility for content directly on ISPs. For example, until very recently, Germany had a law known as "Storenhaftung" or "interferer's liability" that held public Wi-Fi providers responsible for copyright infringement that occurred over their platforms. In practice, this meant that despite being Europe's largest economy, Germany had about half the number of public Wi-Fi hotspots, including in cafes and shopping centres, as other countries in Europe (Heaphy, 2018). Those setting up and managing Internet networks need to be cognizant of where local laws put responsibility for content disseminated.

Privacy and surveillance trends

Another trend in Internet governance has been the increase in contradictory laws that protect users' privacy and those that erect frameworks for lawful government surveillance online. The General Data Protection Regulation (GDPR) adopted by the European Parliament in 2016 is the most prominent example of the former, with numerous countries around the world following suit and adopting comparable policies to protect users' privacy online. While many countries that host refugee communities have not yet adopted such laws, efforts in the humanitarian sector itself have been made to integrate the principles of data privacy more clearly in its work, including in documents like ICRC's *Handbook on Data Protection in Humanitarian Action*.

By contrast, surveillance requirements often create tensions for Internet providers who want to protect users' privacy, but who are required to include mechanisms to enable government surveillance of their users. Most ISPs operate under "lawful access" regulations that require them to allow the government to access content transmitted over their network through a kind of virtual backdoor, which may pose particular problems for refugees and IDPs fleeing government-led persecution. Some governments have become more heavy-handed in recent years with their surveillance efforts. For example, new regulation in Tanzania passed in 2018 requires all cyber cafes to install surveillance cameras and requires online content creators to store contributors' details for up to 12 months (Dark, 2018). While a *proposed* new law in Kenya uses social media licensing requirements to create new obligations on the part of WhatsApp group managers to monitor discussions in their group and ensure that content is "fair, accurate and unbiased" and "does not degrade or intimidate a recipient" and report to government authorities any transgressions. Failure to do so could even be punishable with one year in prison (Indeje, 2019).

Together, what these numerous legal shifts make clear is how exceedingly prone to change Internet regulations can be at the moment. As a result, it is often unclear who, aside from the State, actually has the authority to make Internet governance decisions, and who has a legal obligation to control content and surveil or protect users. Below, we look at how a particular category of actors, ISPs, both in refugee contexts and more broadly, have made decisions about how to navigate the complex landscape of responsibilities and liabilities around Internet governance.

What Internet governance decisions are being made and why?

What decisions are being made about how to balance the information and communication needs of those inside refugee camps with the desire to protect them and others from potential harm? Does it matter which actors – MNO, satellite company, international IT company, humanitarian organization, or local NGO – are involved in setting up or managing a network? For example, might humanitarian organizations like UNHCR be more concerned with digital exclusion than an MNO; or might a local NGO be more concerned about the experiences refugees have online than simply providing access? And if so, how, if at all, does this affect Internet governance decisions? Do they have Internet policies that guide their approach to connectivity and the governance of their networks? Do Internet governance decisions made in a refugee context differ in any way from Internet governance decisions being made by commercial service providers elsewhere?

Unfortunately, at the moment there is limited public information available about how Internet networks in refugee camps are managed and governed. There is a great need for both more transparency on the part of those managing these networks and more research into how such decisions are made. As a result, in this section we examine some of the documents that are available, including reports, blogs, and fair and acceptable use policies, to assess what governance decisions are made that might affect refugees. First, we look at publicly-available documents from select private sector MNOs and satellite companies operating in Kenya that illustrate their positions on “fair” and “acceptable” use of their networks. Kenya provides an important illustration here both because of the large number of refugees and asylum-seekers it hosts, and because of the often unclear policy documents available from these companies that are typical of many developing countries hosting displaced populations. Second, we look at one specific case of an Internet network setup to support refugees – the case of NetHope’s work for Syrian refugees in Europe – to discern Internet governance decisions that were made. This leads to a broader discussion about what beliefs about the benefits and risks of Internet access shape the decisions made by NetHope and others about how to manage networks in displacement.

Decisions made by private-sector Internet service providers

The operations of ISPs and MNOs are, of course, governed by the laws of the countries in which they operate, like the ones mentioned above. But beyond that which is prescribed by the letter of the law, how are private sector ISPs making decisions about where to extend their networks and about what kind of filtering or acceptable use policy they might implement for their users once there?

We will look at the case of ISPs in Kenya to give some idea of the state of things in a country

that is home to a number of refugee camps. Kenya is unique but does give some indication of the trend towards a duality of both more connectivity and more restrictions on behavior online that are becoming increasingly common. In 2013, the Kenyan government released a National Broadband Strategy with the goal of connecting 94% of the population to 3G broadband coverage by 2030 (Government of the Republic of Kenya, 2013). With this came financial support for ISPs that connected new and more remote parts of the country. This incentivized ISPs to connect more disparate parts of the country, but it is limited if ISPs cannot foresee sustained revenue from the newly connected location. As for profit companies, they must factor in whether new users will be able to afford access and what the demand will be in the area once government incentives have dried up. Donor funding made available for projects like DadaabNet likely provided a similar incentive to local ISPs to extend connectivity into refugee camps in Kenya. Some do undertake such projects for CSR or for a public relations boost, but such effects are temporary. **To integrate private sector ISPs into connectivity as aid in a more sustained way, there must be some expected sustainable return on their part.**

In addition to making decisions about *where* to provide access, ISPs also have to make decisions about the backhaul infrastructure, how much capacity (bandwidth) to provide, and what kinds of usage of their network will be “fair” or “acceptable”. In some cases, these are interrelated. For example, video streaming requires a higher amount of bandwidth than sending WhatsApp messages. As a result, in contexts where bandwidth is limited, some ISPs decide to restrict access to streaming content at certain times in order to maintain a reasonable level of connectivity for all users. While this can result in what may appear to be censorship to the end user, in these cases the decision is made in order to enable better access for everyone, rather than to restrict access to particular content.

Many ISPs around the world, including some in Kenya, make a few policy documents public that lay out certain rights and responsibilities of both the ISP and its users. These include in particular privacy policies, fair use policies, and less frequently acceptable use policies.

In Kenya at the moment, perhaps in response to the global attention that GDPR has received, privacy policies are the most common of these three policy documents at private sector ISPs. For example, the privacy policy of Safaricom – the largest of the country’s MNOs owned in part (35%) by the Kenyan government – allows it a wide berth in tracking and collecting data about its users. This includes everything from users’ IDs, credit card information, demographic information, and account information to their location, call history, medical information, biometrics, and voice recognitions, as well as any closed circuit television (CCTV) footage collected by Safaricom cameras installed in shops and around major urban centres (Otuki, 2017; Safaricom, 2019). Perhaps unsurprisingly because of their relationship with the government, Safaricom’s privacy policy also indicates that they share this information with law-enforcement, regulatory authorities, and courts. This data sharing agreement is an integral part of the Kenyan government’s strategy to identify and counter the operations of terrorist organizations in Kenya.

Beyond privacy policies, some ISPs release a “fair use” policy. These documents usually lay out what kind of user behavior would lead an ISP to restrict or limit its users’ access. The most common reason given is for disproportionately high bandwidth usage. Safaricom does not provide

much detail about its fair use policies, but buries some of it inside its terms of service agreements (Safaricom, 2015). SES, a satellite company that often provides connectivity in humanitarian contexts, with satellites that cover Kenya (SES, 2019a), makes their fair use policy public and readily accessible online. In it, they explain how they use algorithms to identify "disproportionate" (i.e. very high) bandwidth consumption. Once it is identified, that user's bandwidth is "gradually restricted" and "a higher priority is assigned to end users with lower volume consumption" (SES, 2019b). Most terrestrial MNOs take a similar approach, but because the extent of their coverage varies more from location to location due to variations in backhaul infrastructure available, they are more likely to make decisions about what amount of bandwidth consumption is "fair" depending on the level of service provision in a certain area (e.g. whether there is 2G or 4G coverage in a particular village).

Finally, ISPs sometimes make a third policy document available, often called an "acceptable" use policy, which focuses on content that is acceptable for people to access using their network rather than the amount of bandwidth they are allowed to use. Few of Kenya's ISPs have made such policy documents public, even though they are undoubtedly filtering certain kinds of content to meet Kenyan government directives, such as those from the Kenyan Film and Classification Board that prohibit accessing certain content, like gay and lesbian films (Article 19, 2018). One example of an acceptable use policy relevant to Kenya comes from Seacom, Africa's first broadband submarine cable connecting eastern and southern Africa starting in 2009. Their acceptable use policy document lays out a number of things that they consider to be "unacceptable" to transmit through their cable. These include not only the transmission of illegal content (such as gay and lesbian films under Kenyan law), but also "the creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material" (Seacom, 2019). Like many ISPs eager to avoid legal transgressions, Seacom prohibits more content than the law requires. In fact, as they do not provide a definition of what they consider to be "offensive" or "indecent" material, there is scope to interpret this widely. It is unclear whether they are tracking such content and filtering it, or whether they are simply retaining the right to punish users who choose to transmit such content.

Overall when making decisions about where to build a network, private sector ISPs in Kenya are concerned with increasing their customer base and maximizing revenue, and are unlikely to provide connectivity for remote regions or displaced communities in a sustained way unless it makes sense for their business model. Similarly, when making decisions about how to manage a network once established, they typically prioritize maintaining the best quality coverage for the most number of people, even if that means reducing bandwidth allowances at certain times or for certain users. They also are likely to share a great deal of data with the Kenyan government and will err on the conservative side in their policies, sometimes adding more restrictions than the law requires to avoid transgressing it.

Decisions made in NetHope's free Wi-Fi for Syrian refugees

As in the case of DadaabNet mentioned above, NetHope has played an instrumental role in facilitating Internet connectivity in a number of humanitarian contexts around the world. Perhaps the most prominent recent example is a project called the Syrian Refugee Connectivity Alliance (SRCA) in which NetHope worked with partners, including UNHCR, Cisco, Facebook, Google, Microsoft, and The Patterson Foundation to bring Wi-Fi connectivity to 98 sites in Greece, Slovenia, Northern Macedonia, and Serbia, including refugee camps and transit centres through which Syrian refugees would pass (NetHope, 2019e). What decisions were made and by whom about what kind of content or data should be transmitted over the network? Are their fair or acceptable use policies that indicate what blocking or filtering provisions, if any, NetHope and its partners have put on their network?

When refugees or other individuals attempt to connect to NetHope's free Wi-Fi in these locations they would typically be directed first to a landing page with the following message:

> "Welcome to #NETHOPE FREE WIFI. NetHope Free Wifi – Provided by NetHope. org. This is a free service for refugees. **Some content is blocked for quality and security**. You may be sent to http://refugeeinfo.eu which has important information for your journey." (NetHope, 2019d)

Being directed to this kind of landing page is typical when logging into many public Wi-Fi spots around the world. Similarly, being redirected to the refugeeinfo website afterwards is also typical of many connectivity for refugees initiatives eager to provide refugees with a clear path to accurate information about services and resources in the new location in which they've found themselves. As we saw in the previous section, ISPs typically have policies about what kinds of content is "blocked for quality and security" as NetHope does here, but in this case, there is little information made available to users by NetHope about what specific content is blocked and why, nor do they make an acceptable or fair use policy available on their website. The ISPs that NetHope works with to set up these networks typically have their own policies about network traffic and filtering, as we saw in Kenya above. To the extent that NetHope makes its own Internet governance decisions in collaboration with the ISPs and other involved partners, any additional blocking or filtering they implement would likely sit on top of existing ISP policies already in place.

A report NetHope published in 2017 about the SRCA initiative provides a little more insight about what their blocking and filtering policy might entail in this case.

> "It is important that appropriate protections and filters are put in place to protect refugees, particularly children and vulnerable populations. NetHope assists by **implementing parental controls, time and data limits as well as malware and virus protection**." (Farrell 2017, p. 38)

Earlier in the report, the author notes that some of the older teenagers had been unhappy with the content restrictions NetHope had placed on "sexy" adult content, leading the author to conclude that "it was apparent that the parental control filters were effective" (Farrell 2017, p. 20). This raises the question of to what extent adult refugees were also governed by these "parental controls"? Were they implemented across all of NetHope's connectivity as aid networks or are there different policies depending on the intended users? For example, does connectivity provided directly to the humanitarian organizations themselves (which is often separated from connectivity for the refugees) also come with the same "parental controls" or are these reserved for the refugees? Or do certain organizations have even stricter policies about what their staff can access online

than there are for refugees? In order to answer such questions, there is a great need for more transparency about what particular filtering and blocking policies have been adopted by NetHope and other connectivity as aid stakeholders. For example, fair or acceptable use policies as we saw in the case of the ISPs could help provide more insight about what kind of content refugees may be restricted from accessing and why.

What informs Internet governance decision-making in displacement?

Now that we've seen a little about what kinds of Internet policies are adopted by Internet providers working on connectivity as aid, we turn to the question of why. What is it exactly that informs the decisions about what Internet governance policies to adopt. What informed the particular decisions that were made in the SRCA project, for example? Are Internet governance decisions made in refugee connectivity projects the same as in any other commercial ISP connectivity project or are there other underlying beliefs that shape them? For example, NetHope's report about the SRCA project mentions "time and data limits" in its policy but doesn't indicate what motivates these limits. Are these limits in place exclusively for technical reasons to manage bandwidth capacity, as in SES's fair use policy above, or are they informed by more substantive concerns about things like the potential for Internet access to cause "sleep deprivation" and "screen-time addiction" among refugees? To what extent should policies be put in place to protect refugees from the potential risks of going online? To what extent should refugees be informed and supported in making such decisions themselves?

A deeper look at NetHope's 2017 report about the SRCA initiative (Farrell, 2017) and some of its other documents available online gives some indication that, unlike exclusively commercial initiatives, decisions-making in this case was informed by *more* than a cost benefit analysis, particularly underlying beliefs about the benefits of connectivity and concerns about some of the particular risks it might pose to refugees.

Benefits

A belief in the power of technology to bring about positive social change is clearly central to the work that NetHope does. It is evident in their stated mission as laid out on their website: "NetHope empowers committed organizations to change the world through the power of technology" (NetHope, 2019b). This mission informs all of their projects. For its connectivity work, like SRCA, it is not just a general belief in the "power of technology" but a more specific belief in the power of Internet connectivity to improve the lives of refugees that propels the project. Their 2017 report gives some indication of the more specific ways in which they believe that Internet connectivity can support Syrian refugees. These include:

> "After fleeing their countries of origin, refugees urgently want to **reopen contact with family,** friends…and the wider society." (Farrell 2017, p. 24)

> "**Access to reliable information** and advice is crucial for refugees to be able to successfully find safe routes to asylum." (Farrell 2017, p. 10)

It is clear in this case that the Internet is seen as a tool for positive social change that, for refugees, enables communication with family and key contacts, and access to information about safe routes and services.

These beliefs are also reflected in wider connectivity efforts in displacement beyond the work of NetHope. For example, UNHCR's Connectivity for Refugees initiative takes the position that Internet access should be treated as a basic right, and uses clearly rights-based language on its website:

> "UNHCR believes that displaced populations and communities that host them **have the right, and the choice, to be part of a connected society,** and have access to technology that enables them to build better futures for themselves, their families and the world." (UNHCR, 2019)

In ETC's overview of its Services for Communities initiative, which works to connect those affected by conflict, it takes a slightly different approach avoiding the explicitly rights-based language but still echoes NetHope's beliefs about the importance of communication and access to information.

> "Humanitarian response is most effective if **communities have the information and communications capacity** they need to make informed decisions. To respond, to recover, to redevelop – in humanitarian **operations the ability to communicate is vital** for all those involved, including the affected communities themselves."

Finally, similar language is often used by local NGO partners that manage Wi-Fi networks in community centres. For example, CTEN's director in Uganda describes himself as guided by the belief that technology and the Internet can "improve and promote access to information" (Batali, 2019).

Academic and practitioner research certainly supports the view that access to the Internet can help improve communication. For example, researchers have shown that mobile Internet connections have enabled refugees in camps or in transit to contact family, friends, and smugglers (Gillespie, Osseiran, & Cheesman, 2018; Poole, Latonero, & Berens, 2018), and have enabled those relocating to a new city to maintain a virtual sense of family through video and voice chats, and even emoticons (Kaufmann, 2018; Madianou, 2019), and to feel "in place" after relocation (Marlowe, 2019).

However, while there is ample evidence that access to the Internet also helps refugees access information, it is unclear whether that information is always *reliable*. In fact, existing research indicates that there is cause for concern that access to the Internet, particularly to social networks is more likely to increase the dissemination of false information and misleading rumors (Poole et al., 2018, p. 10), a problem that many refugees themselves are worried about (Alencar, Kondova, & Ribbens, 2019; Dekker, Engbersen, Klaver, & Vonk, 2018). Efforts to redirect refugees to pages, like refugeeinfo in the case of NetHope's SRCA project, with verified and reliable information are important tools to help counter this problem.

NetHope's report also lays out other beliefs about the power of connectivity for refugees, which

focus more on specific outcomes, like enabling education or employment or other practices that facilitate refugee self-sufficiency. In particular, the report states that Internet connectivity is "vital" "to **enhance their education, enterprise, and employment** opportunities" (Farrell 2017, p. 37).

This view is also reflective of beliefs that inform connectivity as aid initiatives more broadly. One of the most common of these more specific arguments about why Internet access is important for refugees is that it provides them with the means to build a livelihood through access to things like mobile financial resources, education, and remote employment opportunities. As a result, considerable effort has been put into projects that support distance learning platforms, mobile money for refugees, and remote work opportunities based on this belief. Some projects built around this belief include those designed to help refugees work remotely. One such project from Refunite, an NGO tech platform that connects refugees with families, which created a separate platform called LevelApp to allow refugees to make additional income by training algorithms remotely (Batha, 2018). While they tested this in Uganda there has been no publicly released impact data yet around to what extent refugees were actually using the platform and able to collect money from it. Nonetheless, virtual work is not the only kind of work in which Internet access may be involved. A recent GSMA report, *Mobile is a Lifeline* found that mobile Internet access did help refugees build and sustain their own offline businesses (GSMA, 2017a).

Risks

Beyond such beliefs about the power of the Internet, Internet governance decisions are also often informed by concerns about the potential risks that Internet access presents to its users. In NetHope's SRCA report, the narrative largely focuses on the benefits of connectivity, and only briefly mentions concerns about "potential downsides to Wi-Fi provision". But it is important to look at these as well because they are more likely to inform Internet policies around content filtering and blocking that can shape the online experience. The potential downsides that the NetHope report acknowledges include:

> "The risk that users could be exposed to **pornography**; potential **trafficking or grooming; cyber bullying; sexting; fake news; violence; identity theft**; and so on. Other concerns include users developing a **screen-time addiction**; **body image problems**; or **sleep deprivation.**" (Farrell 2017, p. 38)

This is quite a long list of potential risks, that is, unfortunately not fleshed out in greater detail. But it does give some indication that certain kinds of content or nefarious actors are believed to pose risks to the refugees through their Internet usage. The risks it covers roughly fall into three categories: 1) exposing refugees to **dangerous content** that could harm them or incite them to harm others; 2) exposing refugees to **hostile actors** who could harm them; or 3) Creating Internet addictions and **mental health** problems.

Dangerous content could include rumors or misleading information, terrorist propaganda, hate speech, or other content that incites violence, or exposure to "immoral" content like pornography. For example, wider trends about concerns about the dissemination of terrorist propaganda online have led some governments to choose to restrict access for the Internet to certain refugee populations.

While research does indicate some correlation (though not causation, which is particularly difficult to study) between terrorist propaganda and offline violence (Klompmaker, 2019; Von Behr, 2013), there is little evidence thus far that refugees are at greater risk of radicalization than the general population. In the case of hate speech, the use of Facebook to disseminate anti-Rohingya hate speech which led to real world violence (Mozur, 2018) provides some indication that there can indeed be a link between exposure to hate speech on violence. But there is also a long history of more traditional media, like radio and television, being used for similar purposes, as in the case of the Rwandan genocide; and the data about whether social media is qualitatively different from traditional media in this regard is mixed.

Exposure to **hostile actors** could include exposure to traffickers, fraudsters, or surveillance from hostile forces. There is certainly anecdotal evidence from practitioners to support the belief that misinformation online can lead to refugees becoming targets. In one case, a refugee reported having been deceived by a contact on Facebook who claimed to be from the "Lebanon embassy" who convinced the refugee to pay $3,000 for a European visa that was never delivered (Alencar et al. 2019, p. 838). While this kind of fraud is likely quite common, some research suggests that offline methods, particularly personal networks, are still a far more common way in which refugees connect with fraudsters, smugglers, and traffickers (Mandic 2017, p. 32). Of more concern to many refugees is the ability of hostile government forces to track them using the Internet, including through spies on platforms like WhatsApp (Alencar et al., 2019; Marlowe, 2019).

The third category of risks to refugees that may be considered by those managing Internet networks are **mental health** issues. Refugees are a particularly unique category when it comes to Internet usage and mental health. By definition, they are removed from their home, and also often removed from friends and family. While mental health researchers in the US worry about teenagers isolating themselves from their "real world" social community by spending excessive amounts of time online (Panova & Lleras, 2016), in the case of refugees they are already often isolated from their existing real world social communities. As a result, the role that the Internet plays in the mental health of refugees seems to depend somewhat on where refugees are in their journey. For example, in the case of refugees living in camps, there is some evidence to suggest that Internet access, including for entertainment purposes, has a positive effect on mental health, including reducing the probability of being depressed (Poole et al., 2018) and increasing self-confidence and self-sufficiency (Bletscher, 2019).

Overall, perceptions of risk are highly subjective. While the NetHope report mentions certain risks, others involved in connectivity projects might perceive risks differently. For example, an engineer may consider risks directly to the network, like hacking or cyberattacks; an ISP manager may think about the risk of not making enough revenue to sustain their operation; a humanitarian worker may think about the risk of misleading information being communicated to refugees about their services; while a refugee may be thinking about the risk of surveillance from a hostile government or the risk of not being able to connect at all.

Even when focused exclusively on risks to affected populations themselves, perceptions of risks can vary. The case of pornography is a particularly illustrative one. While there is certainly at least anecdotal evidence that Internet access in refugee camps has been used for watching pornography

or accessing other sexually explicit content (Yafi et al., 2018), whether this represents a real "risk" is decidedly subjective, often informed by cultural or religious norms. For example, exposure to online pornography would be a particular concern for refugee camps in Muslim countries where pornography is often expressly forbidden by law. By contrast, pornography is legal in most Western countries, though there are exceptions. In the USA, for example, since 2016, 16 States have voted to treat pornography as a "public health issue" (KC, 2019) Many who view exposure to pornography as a public health threat often also express concern about the potential for it to validate or even inspire offline sexual violence (Long, 2016),. While there is evidence that exposure to pornography leads to sexist perceptions of women (Omori, Zhang, Allen, Ota, & Imamura, 2011; Wright & Tokunaga, 2016), whether it leads directly to acts of sexual aggression is a hotly contested topic among researchers.

As a result of such subjectivities, **who is involved in the decision-making process about which risks should be attended to and which risks can be ignored will have an impact on the Internet policies that are ultimately adopted and shape how refugees experience the Internet.**

While the information available about these decision-making processes in connectivity for displacement projects is currently limited, what is available indicates that such decisions are likely predominantly made in a top-down fashion, often based primarily on technical concerns about network bandwidth or on well-intentioned beliefs about what is best for refugee users. However, the case of CTEN, the refugee-led organization in Uganda that runs a technology community centre, provides an important counterexample to this. In an article about CTEN's work, they wrote about the importance of working *with the affected community* itself to help inform decisions about what content should or should not be available in their centre.

> "**CTEN worked with the community to determine what online content should be available**, when the center should be open and what the terms of use should be. Humanitarian programming often derives from preconceived ideas of what type of content a community needs most. However, in this case, the community had free choice and decided it wanted, among other things, access to sports results – a type of content organizations might normally overlook." (Batali et al., 2019)

This is an important but rare example of refugees themselves participating in the Internet governance decision-making process. More research is needed to assess how effective this kind of policy-making is and could be at a larger scale in connectivity as aid work.

A comparative look at Internet governance decision-making

It is clear that those connecting refugees to the Internet face a complex and often contradictory array of factors to consider when making decisions about how that access should be managed and governed. As connectivity as aid projects are still relatively new, it can be immensely useful to look at how others in similar situations have balanced the need to protect users against the desire to provide access. In the section below, we look at three distinct contexts for lessons on how to navigate this balance: 1) earlier efforts to introduce communication technologies to refugee camps; 2) the provision of Wi-Fi in public libraries in the US; and 3) community-run Internet networks around the world. Unlike the commercial ISPs we looked at earlier, all of these initiatives are public or not-for-profit. So while they certainly factor in sustainability, cost and revenue generation metrics play a less central role in their decision-making process. What becomes apparent through these case studies is the profoundly influential role played by both local laws *and* deeply held beliefs. While local laws have an influence in every context, in some, Internet providers found ways to subvert these requirements or even to advocate for more open Internet policies.

Historic ICTs for refugees initiatives

The current trend in connectivity as aid – focusing on bringing 3G, 4G and Wi-Fi Internet connectivity to populations displaced by conflict has only taken off in the last few years; but there is a long history of work to make information communication technologies (ICTs) more broadly accessible to refugee populations. While the term "ICTs" is often replaced more recently with the terms "digital" or "technology", it still captures something they do not, namely the *purpose* people see behind the use of technology. In this case, the dual purpose of accessing information and communicating with others is embedded in the terminology. Crucially, there is ample research that shows how important both of these goals are to refugees living in often very uncertain circumstances, even if the evidence about how effective different technologies are in delivering this is mixed.

There is a great deal to learn from looking back on the successes and the challenges faced in prior endeavors to implement ICTs for refugees. In this section, we will do that with two cases. The first is the history of communication technologies in refugee camps in Germany starting in the 1940s; the second is the more recent work to set up Community Technology Access Centres (CTAs) by UNHCR starting in 2009. Ultimately, looking at these cases will demonstrate a few things:

1. That ICTs can indeed play an important role in connecting people and in accessing information but that we should not underestimate the value of offline communication tools as well;
2. That host country laws play an important role in shaping this access, but that when restrictions are too high people frequently find ways to circumvent them; and
3. That centres for technology access have a history of being used as a site for surveilling refugees' activities and that more transparency is needed around how refugees' activities with ICTs are monitored.

Pre-digital ICTs in German refugee camps

This case study comes primarily from a recent publication, called " 'We Demand Better Ways to Communicate': Pre-Digital Media Practices in Refugee Camps," from Philipp Seuferling, a media and communication scholar at Södertörn University in Sweden. Drawing on archival material, he looked in detail at historical media practices in refugee camps in German between 1945 and 2000 (Seuferling, 2019).

In it, he shows how refugees in these "pre-digital" times had the same "basic need for access to information and connectivity" (p. 211) as refugees today, but that they faced a much more "extreme situation of information scarcity" (p. 211). Seurling gives a number of examples in which camp administrators in the 40s and 50s provided, or advocated for the provision of, communication

technology in order to alleviate these concerns. In one example from several refugee camps in West Berlin in 1952, officials requested that radios – the only medium at the time that could receive live broadcasts across national borders – be supplied to refugees because "being cut off from the outside world hit the inmates of the camps especially hard" (Eichler, 1952, as cited in Seuferling, 2019, p. 211). "Radios," Seurling writes, were "one of the first things newcomers would buy or trade within the camps" (p. 211). In response, much like private sector ISPs setting up networks in refugee camps today, a public service broadcaster in Hamburg donated 65 radios. In another case, camp managers created "camp cinemas", which would show movies and newsreels, or rooms with TVs, radios, and newspapers that would double as social gathering spaces. As we will see, these kinds of common rooms for communication are echoed in UNHCR's later efforts to set up CTAs.

What these accounts also make clear is how camp management often put in place practices to either control the content refugees had access to or monitor their usage of communication tools. For example, in the case of some camp cinemas in Nuremberg, camp management "closely scrutinized the selection of films, as they wanted to boost morale and democratic education among the residents" (p. 211). While in others, media common rooms played a role in maintaining order because they "enabled full control and surveillance of where and when certain media practices could take place" (p. 211). These brief glimpses into the decisions made by early camp administrators give some indication of the kinds of policies in place regarding the limits of what was "acceptable" use of these communication tools and how such use should be monitored.

Some examples from camps in the 1980s and 1990s demonstrate how impactful host government politics can be. In the 1980s, the German Government implemented tighter laws that greatly restricted support for refugees, including the communication infrastructure available to them. "Media was no longer part of the basic provision and, in the case of camp telephones, the use of communication technology was often even explicitly forbidden, or only granted in emergencies" (p. 212). As a result, camps stopped offering cinemas or providing access to radios or newspapers. As in contemporary cases in which some governments have prohibited Internet access for refugees, host government legislation had a clear effect on the services offered by camp administrators.

However, it is also clear from Seurling's analysis that refugees desperate for information often found ways around these limits and many even engaged in activism to push for more access. For example, in one case, refugees came together with host community members and creased an 'info cafe' in a university dorm outside of the camp to enable access to information and speech in an environment free from camp surveillance (p. 212). In another case, when activists sent a letter to camp administrators asking for a "tea room" where information from home could be shared, the camp administrators responded with a long list of reasons why it would be impossible, but also advised the refugees to find facilities outside of the camp (p. 213). These brief insights illustrate the tension felt by many camp administrators between adhering with local laws and helping refugees to access the information for which they are desperate. It also provides some lessons about the likelihood that camp residents would engage in circumvention tactics or even advocacy when they feel cut off from vital information.

Community technology access centres

In 2009, UNHCR launched a project to provide "community technology access" (CTA) to refugees as part of its livelihood strategy. Shaped by a belief that "ICTs" were a "main source of knowledge and education" (UNHCR, n.d.), the primary goal of this initiative was to "enhance empowerment, self-reliance and employability of refugees and other UNHCR persons of concern through access to education, vocational training and livelihoods via technology" (Anderson, 2013). Like many of the current connectivity as aid projects, it involved a collaborative effort with private sector companies like Microsoft and Hewlett-Packard as well as local NGOs. The CTA centres were essentially computer centres or Internet cafes that hosted classes for children and training in computer skills, entrepreneurship, and language for adults. They initially piloted the initiative in Rwanda and Bangladesh; but by 2012, there were 56 CTAs set up around the world in refugee camps as well as urban, semi-urban, and rural communities in order to support local host communities as well as refugees.

Interestingly, while the primary goal of these CTAs was to further livelihood objectives like education and access to employment, a 2013 assessment found that the centres were in fact more useful in terms of supporting "the enjoyment of basic rights to freedom of expression and information" (Anderson 2013, p. 21) than in supporting the intended livelihood objectives. For example, evidence from one CTA in Georgia showed that people in a very remote location were "connected to the outside world" (Anderson 2013, p. 23) for the first time through their CTA. In another in Argentina, users were able to access a different perspective on local politics through Internet access available at their CTA centre than they were otherwise able to find on traditional local media outlets (Anderson 2013, p. 23). Others reported the centres helped with communication between refugee and host community populations. The experiences of CTA centres illustrate how technology facilities can often be used for a much wider range of purposes than originally intended by those implementing them.

Decisions about the particular training offered or access provided seems to have varied between CTA centres as they were often administered by local partner NGOs, though there is limited information available about what many of those decisions were. While across the board the primary focus was on the training offered to support refugee "self-reliance", many of the CTA centres also provided direct access to ICTs for more general purposes, including sometimes Internet access for accessing things beyond educational training, including social networking and accessing information online (UNHCR, n.d.). Policy documents often reference enabling "safe access" to technology (UNHCR, n.d.), but this raises the question of how they decided what kind of access to allow and how they ensured that technology access was "safe"? Did they have "fair" or "acceptable" use policies like the ISPs mentioned earlier? Was the usage of the technology and Internet access in these facilities monitored and regulated, to ensure users were only engaging with "safe" content? While these questions remain, what is clear is that those administering CTA projects worried about many of the same "governance" issues as connectivity as aid practitioners today. More work needs to be done to institutionalize how such decisions were made and by whom exactly so they can better inform future projects struggling with the same issues.

Finally, a 2011 report on UNHCR's response to the situation faced at the time by the Rohingya in Bangladesh provides another illustration of the role of host government policies, the capabilities of refugees to circumvent restrictions, and the challenges faced by humanitarian organizations as a result. While Bangladesh was one of the countries selected to pilot the CTA project, it was curtailed soon after because of "the refusal of the authorities to permit Internet access to the 1,200 CTA refugee students in Bangladesh" (Kiragu, Li Rosi, & Morris 2011, p. 18). The government insisted that training be confined exclusively to "Word, Excel and Publisher" (Kiragu et al. 2011 p. 18). It was clear from a subsequent UNHCR evaluation that this caused great frustration on the part of many of the refugees who felt cut off from resources that they knew were available. Despite these government restrictions, many of the refugees would leave camp illegally to go to Internet cafés in local communities or would access the Internet illegally from their mobiles (Kiragu et al., 2011, p. 18-19). Like the German camp administrators before them, the 2011 report indicates UNHCR's desire to advocate for the needs of refugees and find ways to support them as much as they could within the restrictions imposed on them. The report's section on the CTAs concludes that "UNHCR should explore the scope for providing the centres with a wider range of educational software, including English language, typing, mathematics and HTML instruction programs and should advocate for legalizing Internet access" (Kiragu et al. 2011, p. 19).

Wi-Fi in public libraries

Those providing Internet connectivity in refugee camps are far from the only ones wrestling with the complexities of providing Wi-Fi access directly in public settings. In many countries around the world, free Wi-Fi access is available in vastly different venues, from restaurants, shopping centres, and public libraries, to airports, schools, and public transport. It is worth looking in more detail at some of the challenges faced and decisions made in these contexts. One that provides a particularly illustrative example of how to balance the risks and benefits of Internet access is the case of public libraries. It is particularly interesting to see how important both laws and deeply held beliefs are in shaping the decisions made about how Internet access should be governed in these locations.

Public libraries, where they exist around the world, are often seen as important places where access to a wide variety of information can be democratized and made available regardless of the identity of the person visiting the library. In the US context, the primacy of this belief in the right to access information is fundamental to how public libraries adapted to the increasing availability of Internet access and the introduction of new federal laws to regulate it.

Since the 1990s, seeing the Internet as an important new source of information to add to their collection, libraries in the US began adding computer terminals that visitors could use to access the Internet, later introducing Wi-Fi through which people could access it on their own devices. But in 2000, the federal Government introduced a new law, called the Children's Internet Protection Act (CIPA), that required libraries to filter Internet access if they wanted to receive E-rate funding, the only federal government assistance available to support ICT infrastructure in libraries (Jaeger, Bertot, McClure, & Langa, 2006, p. 132). The purpose of this law was to prevent minors from accessing potentially harmful content, but the law required content to be filtered for everyone on all devices in the library with the filters only being disabled if an adult patron requested it (Jaeger

et al. 2006, p. 132). This law created ideological dilemmas for a number of libraries as the need and desire to protect children came up against a particularly fundamental belief on the part of many librarians about the right to access information. A wide scale study of public libraries in the US conducted in 2008 found that only 50% of all libraries across the country had applied for E-rate funding. While some said they hadn't applied because the application process was cumbersome, others said it was because "compliance with the filtering requirements of the Children's Internet Protection Act (CIPA)" had been deemed "unacceptable" (Bertot, McClure, & Jaeger 2008, p. 293). In other words, those libraries believed so strongly in the role of their institutions in providing free and unfettered access to information that they had rejected funding because of filtering requirements it had imposed.

A similar result emerged after the US Government passed the PATRIOT Act in 2001. Among many other things, this new law, which followed quickly after the 9-11 terrorist attack, required libraries to monitor their visitors' behavior, and particularly what they did online (Jaeger et al., 2006). Strong beliefs in personal and intellectual freedoms again informed how many libraries responded to these new surveillance demands. As a result, many libraries actually stopped collecting certain information from their patrons – including items checked out, the nature of library fines, searches on public access databases, and web browsing activities – so they would not have to make them available to the authorities (Jaeger et al. 2006, p. 135). Some libraries, for example, would set the public computer terminals to wipe the browsing history whenever a user logged off. (Dosono 2016, p. 4) But as remote technology advances, particularly remote tracking software, the ability of libraries to protect the privacy of their visitors becomes increasingly difficult. Despite these challenges, the belief in the fundamental importance of access to information has led many US libraries to continue providing Internet access regardless and to add in clear disclosure information about their Internet policies and the kinds of privacy risks users face online when users sign into their network (Dosono 2016, p. 4). Furthermore, libraries have even taken a more active approach to changing the law and have been central to the move to challenge the PATRIOT Act in court (Jaeger et al. 2006, p. 135).

The importance of these deeply held beliefs for decision-making becomes more apparent when we look at American librarians in comparison to others. For example, one study that looked at attitudes towards filtering online content at American university campuses found a marked difference between the views of the librarians and other stakeholders, like university administrators, faculty, and IT professionals (Orenstein & Stoll-Ron 2014, p. 62). It found that a full 100% of university librarians believed that filtering was censorship, while other groups accepted varying levels of filtering. Even though universities are protected by academic freedom and there are no laws in the USA, like CIPA, that require filtering at universities, many in university administration still do decide to filter Internet access. This case also helps illustrate the complex matrix of authority when it comes to decision-making about Internet access standards as librarians, IT professionals, and university administrators all play a role in shaping access at universities.

Another useful point of comparison is libraries in the UK where national law requires similar protections for children as CIPA but where the country is also a signatory of the legally binding European Convention on Human Rights, including the freedom to impart and receive information (Spacey et al., 2017). In contrast to many American libraries, the vast majority of libraries in the UK

do impose filters on available content. According to a 2013 survey of Scottish libraries, for example, fully 31 or 32 libraries had them (Brown & McMenemy, 2013; Spacey et al., 2017). In this case, "the obligation of public libraries to protect children and to be a safe place for them effectively overrides the right of adults to access lawful information without undue hindrance" (Spacey et al. 2017, p. 22).

One way in which libraries have made this decision-making process particularly clear is in the creation of a number of public documents that lay out their policies and offer guidelines for other libraries seeking to create them. For example, the American Library Association (ALA) even has a Library Bill of Rights, in which it "affirms that all libraries are forums for information and ideas," (American Library Association, 2006) and asserts that "libraries should challenge censorship in the fulfilment of their responsibility to provide information and enlightenment" (American Library Association, 2006). The ALA outlines that it views "the use of filtering software by libraries to block access to constitutionally protected speech" to be a violation of the Library Bill of Rights. The ALA also offers a toolkit for helping libraries across the country create their own "Internet use policies", including acceptable use policies and disclosure documents for library patrons about their rights and the library's Internet policies. This approach of offering professional guidelines and toolkits has made it incredibly easy for different libraries to navigate the complex decision-making process around balancing the risks and the rights when it comes to Internet access.

Community Internet networks

One final case provides additional insights into how others setting up Internet connections have navigated the challenges around Internet governance: community networks (CNs). CNs differ from other approaches to Internet connectivity in that the local communities are directly involved in owning and operating the physical infrastructure of connectivity. Many such networks are deployed in very remote rural locations, making them useful points of comparison for those setting up networks in remote refugee camps. Moreover, in the case of AirJaldi Networks, there is at least one case of a community network being deployed specifically for a refugee community, in this case the Bylakuppe Tibetan settlements in India (AirJaldi Networks, 2017).

Precisely because they are more locally-rooted than other approaches to connectivity, community networks around the world vary considerably in their structures, motivations, and approaches, reflecting the different characteristics of the communities they represent. But like their counterparts in refugee contexts, they are often set up through collaborations between different organizations, only in this case the organizations tend to be local non-profits, cooperatives, small businesses, local governments, and universities. Due to their local grounding, such organizations are often willing to invest the time and effort necessary to build sustainable infrastructure and the training necessary to maintain them. This same requirement for "local" investment may appear to create problems for displacement contexts due to the transience of many refugees, who may be unlikely to feel a "sense of investment" in setting up or maintaining an Internet infrastructure for a place in which they do not intend to stay. Nonetheless, though it is rarely the intention, many refugees end up staying in places far longer than they had intended, as is the case in some refugee camps like Dadaab where many Somali refugees have lived for decades. As a result, it may still be beneficial to offer refugees opportunities to have a stake in building or maintaining their own Internet network.

The investment from local organizations inherent in the community network approach has a number of other important outcomes.

First, it increases the "potential to foster a sense of agency and empowerment among users and those involved in the network" (Bidwell & Jensen 2019, p. 10). In fact, in many instances this has actually led to some of the livelihood outcomes that were intended with UNHCR's CTA project. In what many CNs refer to as "capacity building", members of the local community are often directly involved in the construction of the necessary infrastructure, and those who are interested but lack the skills receive training in how to manage networks. For example, in the Red Hook Initiative, high school students in Brooklyn were trained in how to manage the community network (Red Hook Initiative, 2019). In some cases, this has led to community members building their own small businesses around the networks. In NetHope's evaluation of its work to set up Wi-Fi for Syrian refugees, they anecdotally observed a similar sense of investment and pride on the part of the few refugees with engineering skills who were able to participate in the network set-up.

Second, it enables "more local control over how the network is used and the content that is provided over the networks" (Bidwell & Jensen 2019, p. 9). While the main motivation of most community networks is the desire to "help meet needs for better and more affordable communication infrastructure" (Bidwell & Jensen 2019, p. 15) many also do so for more ideological reasons, like "supporting aspirations of building the autonomy of their community" (Bidwell & Jensen 2019, p. 16). In fact, community autonomy over Internet governance decision-making is a key by-product of the community network model. By contrast, with the exception of refugee-led initiatives like CTEN, refugees rarely are so directly involved in Internet governance decisions for Internet networks in displacement contexts.

As a result of their autonomy, Internet governance decisions in CNs can vary widely, reflecting the desires, underlying beliefs, and cultural norms of the people they are serving. For many CNs the desire for autonomy is as important to them as the belief in the free flow of information is to many American librarians. And like the librarians, these beliefs and motivations shape how they choose to approach Internet governance. As a result, many CNs choose to adopt extremely liberal approaches to content moderation. For example, in contrast to many other public Wi-Fi setups, many CNs do not adopt any filtering to protect children, instead leaving this decision-making power with the parents (Bidwell & Jensen 2019, p. 135). However, while not imposing filters, some CNs do create time limits on the use of their networks at certain hours of the day to discourage children from seeking out "negative" content (Bidwell & Jensen 2019, p. 135). Similarly, in contrast to most private sector ISPs, most CNs do not impose any caps on users' data allowances. Instead, they often allow unlimited data usage and charge users per week or per month, though some CNs restrict access to streaming content at high-traffic times to alleviate network congestion that could result from unlimited access (Bidwell & Jensen 2019, p. 75). The point is that when you build a network from the ground up, all of the decisions, including those about how to store and manage personal data, are made within the community, which is especially empowering when marginalized communities normally have previously limited autonomy over their data.

As in all of the cases we have examined, the legal and regulatory environments shaped the creation and management of these networks. In many contexts, regulations – particularly those that dictate

how spectrum should be allocated and how much it costs – present particular challenges to community networks because the existing rules have been written for large, commercial ISPs. As a result, many CN members – and organizations that advocate for their adoption like the Internet Society and the Association for Progressive Communication – have become vocal advocates for regulatory reform, at the local and even international level. Community networks members have even advocated for change at the International Telecommunication Union.

However, there are contexts in which government regulations have actually encouraged the growth of community networks. For example, in one case in Indonesia, the government went beyond financial incentives for universal access and required local village authorities to have their own websites and "Village Information System" that was intended not only to ease community access to government but also to preserve cultural heritage and promote local businesses (Bidwell & Jensen 2019, p. 86). The community network model that encourages local autonomy and the creation of local content was particularly well-suited to meet these government objectives. Similarly, in Mexico the spectrum license has a special provision to protect "social use" that supports community networks (Hinojosa, 2016), while South Africa regulation now has a provision for the establishment of non-profit telecoms (APC & IDRC, 2018).

Together, these diverse cases – CNs, public libraries, CTAs centres, and historic pre-digital media practices in refugee camps – provide a picture of the complex matrix of factors involved in Internet (or technology) governance decision-making and how diverse actors have chosen to address them. In all cases, laws and regulations clearly played a part in shaping what restrictions were imposed, but in some cases (particularly with community networks and libraries) organizations involved in providing access began to play a role in advocating for change when they believed regulations were too restrictive or when they believed the communities they served deserved greater access. Similarly, all cases depict the important role played by the particular beliefs and world views of those making Internet or technology governance decisions. Librarians' views about the importance of the right to privacy and unfettered access to information, for example, even led them to reject or circumvent government restrictions they did not agree with. This leaves us with a clear indication of just how variable Internet governance decisions can be depending on who is involved in the process.

While the factors involved in these cases all differ in various ways from those that must be considered in contemporary connectivity as aid initiatives, the comparisons are nonetheless fruitful. They all share a common desire to provide access to technology or the Internet for reasons beyond revenue generation and typically target a particular population that is less likely to be able to get access through more conventional commercial means. For example, public libraries are often a primary source of Internet access for homeless communities in the US while community networks connect villages that are disconnected from private sector networks. What is a particularly pertinent takeaway for those working to connect displaced communities is how clearly diverse world views can influence the Internet governance decisions that are eventually taken. With very diverse beliefs and priorities, ISPs, humanitarian organizations, and the refugees themselves are likely to all make very different decisions about how Internet networks should be governed.

Conclusion

Around the world, Internet access is simultaneously connecting people with loved ones, new friends, vital information, and employment prospects, while also fomenting loneliness, societal divisions, political conflict, and in some cases even genocide. It is overflowing with important resources and information but also new technologies like deep fakes that make reliable information more difficult to identify. As with many of the methods of communication that preceded it, the Internet is a reflection of society and the inherent contradictions within it, but because of the speed of Internet communication these contradictions tend to accelerate. How then should this tension affect decisions about whether to connect a particular community to the Internet and how to manage that access and the risks it might bring once installed? How should the potential risks be balanced against the benefits of access? These are the kinds of questions confronting most stakeholders involved in Internet governance, from State governments and commercial ISPs to community networks and social media companies. They are also the kinds of questions that anyone involved in setting up Internet access for displaced populations must be particularly careful to address.

Those who have been forced to flee conflict, disasters, or persecution, are often more in need of accurate information and communication tools like the Internet than the rest of us. They are also often less able to access them themselves through normal commercial means and at greater risk from things like fraud, misinformation, and hate speech. Environments with ongoing conflict or hosting populations displaced by conflict may present particularly delicate information environments more vulnerable to the risks of spreading hate speech and disinformation than most; while environments that have historically welcomed refugees are more susceptible to the spread of misinformation and anti-refugee and immigrant rhetoric online than before.

The Universal Declaration of Human Rights includes a fundamental right to "seek and impart information", while international refugee law creates a specific obligation to "protect" refugees. Both of these apply regardless of the national laws in which a particular intervention is operating. Such rights and protections need to extend to the digital. How then can Internet access be provided safely? And whose responsibility is it to make these decisions? The current legal landscape that governs the Internet in displacement contexts is decidedly plural and complex, with States changing their individual Internet regulations around things like hate speech, surveillance, and cybersecurity frequently. While it may be difficult to discern which actors should be responsible for safety and security online at any one time or in any one location, when dealing with refugee populations, there is clearly a greater responsibility to ensure their online protection than even for the general public. As a result, those working in connectivity for displaced populations should be clear about the policies they are putting in place to ensure that protection.

However, as we have seen in this report, the current landscape of governance of Internet networks for refugees and other displaced populations is opaque. A dizzying array of actors are often involved, from local commercial MNOs to massive international Internet companies, from governments to humanitarian organizations and local community-based NGOs. Each brings their own values, beliefs, and objectives into this process, often varying depending on the industry they work in, the country they are from, their religion, or any number of other characteristics and deeply held beliefs about the world. For example, there is an underlying tension between actors – like

commercial MNOs or private social media companies – that may be motivated in part, or primarily, by financial incentives, and others – like humanitarian organizations or local NGOs – that may be motivated more by humanitarian or human rights-based objectives or by beliefs about certain rights online. What difference does it ultimately make to the Internet that refugees have access to whether it is provided directly by a commercial ISPs or in collaboration with humanitarian or other non-profit actors? As this report outlined, humanitarian initiatives like NetHope, ETC, and UNHCR's own connectivity initiatives tend to involve more value-driven decision-making, but there is a need for more transparency and reflexivity about how these beliefs and values shape decisions about where to set-up a new Internet network, what that network should look like, and how to manage it.

In addition, there is a lack of Internet policy documents publicly available from those who work in displacement contexts, documents that clearly state what content or online behavior is restricted and explain why and how such policies were decided upon, both of which could help refugees and the wider public assess how stakeholders' beliefs and priorities influence Internet decisions that affects them. Refugees, like everyone, should have access to information about how and why their online behavior is being enabled, restricted, or tracked. And there should be mechanisms in place for them to appeal when they believe their rights have been infringed by things like filtering decisions. For the most part, users anywhere in the world face an immense challenge sifting through what information is provided. Dense and ambiguously written privacy policies or community standards and frequent changes in government regulation make it difficult for the public to know what their rights are online and how countless actors – from Internet providers, websites, and social media companies, to governments, hackers, stalkers and others – are tracking or manipulating what they can access or communicate online. By putting the rights of the displaced front and centre, those involved in connectivity as aid initiatives, have the opportunity to set an example about how open and transparent Internet governance practices can be.

Many of the commercial ISPs that get involved in connectivity for refugee projects like to focus on the technical side, on things like how to maintain the best network coverage for the most number of users. But many also already have their own policy documents, like privacy or fair use policies, and sometimes even acceptable use policies. MNOs that provide access directly to their network for refugees through new cell towers should review these policies to evaluate if they make sense or if they need to be adapted in some way to support the protection of refugees and IDPs, and evaluate whether they can be presented in a clearer way.

For connectivity initiatives propelled more by humanitarian actors, there is a need for better, more transparent, and more standardized practices around how communal Internet facilities are set up and managed. While the contexts are quite different, humanitarian organizations could take a cue from the American Libraries Association, which publishes a clear Libraries Bill of Rights on its website and makes Internet policy templates available for libraries around the country. Such policy documents are also easily accessible on most library websites and content filtering and surveillance provisions laid out clearly and in detail when patrons log on. Organizations working to support displaced communities operate under much more varied legal and logistical contexts than domestic American libraries. Nonetheless, similar documents could be produced to help standardize some of the decision-making around Internet access in displacement while also leaving space for adaptation to the often very different demands of each displaced community or host environment. The recent work to develop standards around data collection and privacy rights, like ICRC's Handbook on Data Protection in Humanitarian Action, are important examples of what this could look like in practice.

Finally, what also became clear during the research produced for this report was how little Internet governance decision-making usually involves end-users, refugees or otherwise. Initiatives like community networks provide important examples of how this can be different and how end-users can be involved in both the construction of networks and in the decision-making process around maintaining and governing them. But for the moment, most community networks are small scale endeavors, focused on individual communities or clusters of communities, and often face an uphill battle with legal systems that have been built around commercial models. A lot of work still needs to be done to see whether they can scale more widely or could be viable in unique displacement contexts. Initiatives like UNHCR's recent work to explore the viability of the community network model in its connectivity for refugees work are important steps towards assessing how refugees could be involved more in Internet governance decision-making in practice.

Overall, important work is currently being done to improve the landscape of Internet access available to those displaced by violence and disaster. As a result, the current moment is a particularly important one in which to incorporate more of this kind of reflection and transparency into how decisions are made that affect what that access looks like and how it is experienced by vulnerable populations.

Projects like the Global Broadband Plan for Refugees could be good starting points but they need more involvement and buy-in from practitioners working in displacement and displaced communities and they need to go beyond calling for greater inclusion and access and to set up plans for protection as well.

Margin space

This Margin Space builds on the overview in the primary Internet Governance in Displacement research brief. First, it provides suggestions on how to use the findings in that report to move forward productively; and second, it identifies new areas of potential research that emerge as a result and lays out new questions that have emerged as a result of this study. In many ways, in putting together this research brief what became most clear was *how much we don't know* about how decisions are currently being made about Internet access in connectivity as aid projects, by whom, and in many cases, what those decisions even are. The suggested ways forward provided below are an attempt to address this gap.

Recommendations for moving forward

Suggestions for improving how Internet governance decisions in displacement are *made*:

1. More evidence is needed about the real effects of Internet access in these unique contexts, including potential unintended consequences;
2. More clarity is needed about which stakeholders are responsible for making which Internet governance decisions;
3. More reflexivity and documentation is needed about what risks (and to whom) are being, and should be, considered, and what informs those decisions;
4. A better record is needed of how decisions are currently made. Even if only done internally, this could help those setting up Internet networks in the future anticipate challenges;
5. More effort should be made to integrate end-users – displaced populations themselves – into the decision-making process, through things like feedback mechanisms, involvement in the construction and maintenance of backend hardware, and the management of community Wi-Fi hotspots.

Suggestions for improving how Internet governance decisions in displacement are *communicated*:

1. Clear guidelines for Internet governance in displacement should be created. They could be modelled off of the ICRC Handbook on Data Protection in Humanitarian Action, with guidelines on how to ethically navigate the different specific decisions that need to be made when setting up and managing Internet networks. They should be flexible enough that fieldworkers could adapt them to the specifics of the context in which they are working. The Libraries and Internet Toolkit produced by the American Libraries Association provides a very useful example of the kinds of guidelines for Internet policy documents that retain such flexibility.
2. For each individual Internet network set up in displacement contexts, clear privacy, fair, and acceptable use policies should be written and made publicly available. These can build on the flexible guidelines above. They should be available succinctly on landing pages when displaced users first log onto the network, but also made available on the websites of the organizations managing them for greater transparency.
3. A mechanism should be put in place to enable users, including displaced populations, to appeal, or otherwise voice dissatisfaction, with content filters or other Internet governance decisions. For example, Facebook has a policy where users can appeal if they believe a post has been taken down in error, while some ISPs have mechanisms where users can appeal if they believe their bandwidth has been restricted unfairly. The ways in which these companies approach such processes can be quite controversial and not always transparent. Given the ethical grounding with which the humanitarian sector approaches its work, there is potential for it to set a model for more progressive transparency between Internet providers and users.

Future avenues for research

1. Some Internet governance decisions for displaced populations – particularly those that lead to some kind of censorship or restriction – are based on assumptions that often have little evidentiary basis. This is particularly true for things like exposure to pornography (which some believe leads to offline violence) or exposure to terrorist propaganda (which some believe leads to radicalization). While in both cases there is limited research of the effects of these things on the general population, there is virtually no research on their effect on displaced populations. Similarly, there is almost no research on the mental health effects of Internet access for refugees. While there is some evidence that the Internet can cause mental health problems in the general population, due to their unique circumstances, this may be vastly different for the displaced.
2. More research is needed into cases where decisions were made to NOT provide access. At times, these kinds of inaction are harder to observe but the decision-making process can still be examined and can be very fruitful for future planning.
3. There is also a need for more research into the real impact of humanitarian actors partnering with private sector actors with vastly different guiding values and objectives in Internet connectivity work. In many cases, the private sector can be a valuable and even necessary ally, but little is known publicly about the impact these divergent ethical codes have on decisions that are ultimately made. In particular, for partners like Facebook and Google, which are deeply steeped in global debates around the most contentious Internet governance issues, we should ask: To what extent are their agendas seeping into any Internet governance decisions that might affect the safety and privacy of displaced communities? For example, do humanitarian organizations partner with Facebook to set up Free Basic in refugee camps? If so, do concerns about a "two-tier internet" factor-in? How are decisions made about what is available on Free Basics and what is not? Where does the decision-making power of Facebook and its humanitarian partners diverge? Where does it overlap?
4. What efforts have been made in the past to incorporate displaced populations into decision-making processes (beyond Internet governance) that affect their lives and experiences in humanitarian relief? Have feedback mechanisms been successfully (or unsuccessfully) deployed? Why and how did they succeed or fail? Can efforts to create fair Internet governance decisions in displacement learn from any of these past projects? The research for this report raised important related questions about how displaced populations can be more involved in the construction and management of

Internet networks, while the example of CTEN demonstrates that is it possible for them to have an element of autonomy over public Wi-Fi network governance decisions.

5. While this report talked exclusively about Internet access, including its role as a source of connection or information, the Internet represents only a small portion of how displaced populations (as well as the general population) get information important to them. More research is needed that looks at the role of the Internet within the wider *media ecology* of refugees and other displaced groups. We need to look holistically to better understand where the Internet fits within this ecology of where and how these communities access information, including through word of mouth, posters, radio and television stations, local host communities, smugglers, and rumours. Doing so will help us understand what benefits the Internet really poses compared to other sources of information. For example, are false rumours about migration routes and ongoing conflict more readily available online or through word of mouth communication?
6. Finally, more research is needed about how displaced populations themselves perceive the risks and benefits of going online. This report showed evidence that some were worried about being surveilled online, while others were aware of the spread of misinformation online. Where do those beliefs come from? What decisions do they make as a result? Do they limit their usage? Use only particular platforms? Like the general populations, in many ways displaced individuals make their own "Internet governance" decisions daily about what they do or do not want to access. They may be tired of the negative effects of social media or they may decide that getting online is worth even the risk of leaving a safe location. What differs from the broader population is often their capacity to enact those decisions. More research is needed to understand how they work with or overcome such barriers.

Lingering questions

1. While the report talked about potential risks of connecting to the Internet, it did not cover much about the potential risks of *not* connecting. This raises further questions, like: Where there are no specific efforts to connect displaced populations to the Internet, are they finding ways to get online anyway? For example, are they leaving refugee camps to get access? Are they putting themselves at additional risk through doing so? In general, how, specifically, do refugees or asylum-seekers access the Internet?
2. A recent submission to the UN Human Rights Council draws attention to the overlooked environmental cost associated with connecting more people to the Internet. To what extent, if at all, is the environmental impact of extending Internet networks being considered in displacement contexts? Should it be? How do you balance the environmental impact against the potential good you believe Internet access will do for these particularly vulnerable populations?
3. Where those involved in managing Internet networks for displacement choose to implement certain content filters, how do they do that from a technological perspective? What software is used? With whom is the data collected through this process shared? What role, if any, do software companies play in deciding the details of the filtering adopted? For example, many public Wi-Fi hotspots in the UK managed by major telecom companies, will have the specifics of the filtering outsources to a third party company, and often with it many of the most detailed filtering decisions. Is this happening in displacement contexts as well? What risks, if any, does this outsourcing create?
4. The task of deciding what are the risks and benefits to users of accessing the Internet is, in many ways, quite a paternalistic one. Those involved in such Internet governance processes are essentially deciding what is good and what is not *for other people*. Facebook does it all the time on their platforms; so do governments. While the founding ethic of the Internet envisioned a network where information could travel freely, the trend recently is towards greater restrictions and control. While humanitarian organizations are motivated by a desire to support and help displaced populations, this report raises important ethical questions about the extent to which humanitarian organizations want to get involved in making these decisions for other people, and what is a "fair" way of doing so. Is it better to limit restrictions and let refugees and IDPs make their own decisions?
5. How, if at all, are Internet filtering decisions for humanitarian staff different from filtering decisions for displaced populations? Internet access has been made available for staff for longer than for affected populations; what can be learned from that earlier experience? Are there any institutionalized practices, even internal ones, put in place that can help guide new connectivity efforts?
6. In contexts where governments have made decisions to heavily restrict Internet access for displaced populations, do humanitarian organizations have a role to play in advocating for change? What might be the risks in doing so?

References

AirJaldi Networks. (2017). Bylakuppe Network. Retrieved December 12, 2019, from AirJaldi Networks Retrieved from: https://airjaldi.com/networks/byalkuppe/

Alencar, A., Kondova, K., & Ribbens, W. (2019). The smartphone as a lifeline: An exploration of refugees' use of mobile communication technologies during their flight. *Media, Culture & Society*, *41*(6), 828–844.

American Library Association. (2006, June 30). Library Bill of Rights. Retrieved December 9, 2019, from American Library Association: Advocacy, Legislation & Issues website: http://www.ala.org/advocacy/intfreedom/librarybill

Anderson, J. (2013). Policy Report on UNHCR's Community Technology Access Program: Best Practices and Lessons Learned.*Refuge: Canada's Journal on Refugees*, *29*(1), 21–30.

APC, & IDRC. (2018). *Global Information Watch 2018: Community Networks*. Retrieved from Association for Progressive Communications & International Development Research Centre website: https://giswatch.org/sites/default/files/gw2018_south_africa.pdf

Article 19. (2018, May 17). Kenya: Censorship by film classification board limiting free expression. Retrieved December 9, 2019, from ARTICLE 19 website: https://www.article19.org/resources/kenya-censorship-by-film-classification-board-limiting-free-expression/

Batali, Peter, Christopher, A., & Drew, K. (2019, October 2). Five Ethical Principles for Humanitarian Innovation (SSIR). Retrieved December 10, 2019, from Stanford Social Innovation Review website: https://ssir.org/articles/entry/five_ethical_principles_for_humanitarian_innovation

Batali, Peter. (2019, April 12). Why community-led innovation is fueled by risk, ambition, and experimentation. Retrieved December 12, 2019, from Medium website: https://medium.com/unhcr-innovation-service/why-community-led-innovation-is-fuelled-by-risk-ambition-and-experimentation-e8e58555e49f

Batha, E. (2018, November 20). This mobile app is paying refugees to train artificial intelligence. Retrieved December 9, 2019, from World Economic Forum website: https://www.weforum.org/agenda/2018/11/mobile-app-pays-refugees-to-boost-artificial-intelligence/

BBC. (2010, July 1). Broadband "legal right" for Finns. *BBC News*. Retrieved from https://www.bbc.com/news/10461048

Bertot, J. C., McClure, C. R., & Jaeger, P. T. (2008). The Impacts of Free Public Internet Access on Public Library Patrons and Communities. *The Library Quarterly: Information, Community, Policy*, *78*(3), 285–301.

Bidwell, N. J., & Jensen, M. (2019). *Bottom-up Connectivity Strategies: Community-led small-scale telecommunication infrastructure networks in the global South*. Retrieved from APC website: https://www.apc.org/en/pubs/bottom-connectivity-strategies-community-led-small-scale-telecommunication-infrastructure

Bletscher, C. G. (2019). Communication Technology and Social Integration: Access and Use of Communication Technologies Among Floridian Resettled Refugees. *Journal of International Migration and Integration*, 1–21.

Borg Psaila, S. (2011, May 2). Right to access the Internet: The countries and the laws that proclaim it. Retrieved December 12, 2019, from DiploFoundation website: https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it

Brown, G., & McMenemy, D. (2013). The implementation of internet filtering in Scottish public libraries. *Aslib Proceedings*, *65*, 182–202. Emerald Group Publishing Limited.

Counter Extremism Project. (2018). *OK Google, Show Me Extremism: Analysis of YouTube's Extremist Video Takedown Policy and Counter-Narrative Program*. Retrieved from Counter Extremism Project website: https://www.counterextremism.com/ok-google

Dark, S. (2018, July 6). Strict new internet laws in Tanzania and Uganda are driving content creators offline. Retrieved December 9, 2019, from The Verge website: https://www.theverge.com/2018/7/6/17536686/tanzania-internet-laws-censorship-uganda-social-media-tax

Dekker, R., Engbersen, G., Klaver, J., & Vonk, H. (2018). Smart refugees: How Syrian asylum migrants use social media information in migration decision-making. *Social Media+ Society*, *4*(1).
Dosono, B. (2016). *Patron privacy: A luxury concern for marginalized internet users*. https://doi.org/10.9776/16285

Ericsson Response. (2018, April 20). Ericsson Response Mission Timeline. Retrieved December 9, 2019, from Ericsson.com website: https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/technology-for-good/humanitarian-response/ericsson-response

ETC. (2019). ETC Operations | Emergency Telecommunications Cluster (ETC) [Organization]. Retrieved December 10, 2019, from ETC website: https://www.etcluster.org/etc-operations

Etherington, D. (2019, July 2). Alphabet's Loon balloons will get their first commercial trial in Kenya | TechCrunch. *Tech Crunch*. Retrieved from https://techcrunch.com/2019/07/02/alphabets-loon-balloons-get-their-first-commercial-trial-in-kenya/

Farrell, T. (2017). *Reconnecting Refugees: A Case Study on the Impact of Wi-Fi Technology on Refugee Communities*. Retrieved from NetHope website: http://www.thepattersonfoundation.org/blog/net-hope/reconnecting-refugees-a-case-study-on-the-impact-of-wi-fi-on-refugee-communities.html

Georgia Tech School of Public Policy. (2019). What Is Internet Governance? Retrieved December 13, 2019, from Internet Governance Project website: https://www.internetgovernance.org/what-is-internet-governance/

Ghelli, T. (2017, March 14). Connectivity brightening future of refugees in Malawi. Retrieved December 10, 2019, from UNHCR USA website: https://www.unhcr.org/news/latest/2017/3/58c7aa054/connectivity-brightening-future-of-refugees-in-malawi.html

Gillespie, M., Osseiran, S., & Cheesman, M. (2018). Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social Media+ Society*, *4*(1).

Global Business Coalition for Education. (2019, January 14). REACT in Action: Broadband for Refugees in Uganda. Retrieved December 9, 2019, from Global Business Coalition for Education website: https://gbc-education.org/react-in-action-avanti-communications-to-deliver-free-broadband-connectivity-to-social-innovation-academy-in-uganda/

Government of the Republic of Kenya. (2013). *The National Broadband Strategy: A Vision 2030 Flagship Project*. Retrieved from http://icta.go.ke/pdf/The_National_Broadband_Strategy.pdf

GSMA. (2017a). *Mobile is a Lifeline: Research from Nyarugusu Refugee Camp, Tanzania*. Retrieved from GSMA website: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/07/mobile-is-a-life-line.pdf

GSMA. (2017b). *The Importance of Mobile for Refugees: A Landscape of New Services and Approaches*. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/02/The-Importance-of-mobile-for-refugees_a-landscape-of-new-services-and-approaches.pdf

GSMA. (2017c, February 24). Zain's initiatives to assist refugees and internally displaced people. Retrieved December 9, 2019, from Refugees and Connectivity website: https://www.gsma.com/refugee-connectivity/zain-case-study/

GSMA. (2019). *The digital lives of refugees: How displaced populations use mobile phones and what gets in the way*. Retrieved from GSMA website: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/The-Digital-Lives-of-Refugees.pdf

Heaphy, E. (2018, July 30). The unique legal concept that led to Germany's weird wifi laws. Retrieved December 9, 2019, from Quartz website: https://qz.com/1343460/the-unique-legal-concept-that-led-to-germanys-weird-wifi-laws/

HIF, elrha, & Samuel Hall. (2018). *Innovating mobile solutions for refugees in East Africa: Opportunities and barrier to using mobile technology and the internet in Kakuma refugee camp and Nakivale refugee settlement*. Retrieved from https://www.elrha.org/wp-content/uploads/2018/02/Innovating_mobile_soultions_Report.pdf

Hinojosa, D. P. (2016, September 1). First telecommunications licenses for social indigenous use in Mexico – Observacom. Retrieved December 12, 2019, from Observacom website: https://www.observacom.org/first-telecommunications-licenses-for-social-indigenous-use-in-mexico/

Indeje, D. (2019, September). Kenya's Proposed Law Requiring Clearance of WhatsApp, Facebook Admins Raises Concerns. Retrieved December 9, 2019, from Khusoko website: https://khusoko.com/2019/09/25/kenyas-proposed-law-requiring-clearance-of-whatsapp-facebook-admins-raises-concerns/

Internet World Stats. (2019, June 30). Africa Internet Users, 2019 Population and Facebook Statistics. Retrieved December 10, 2019, from Internet World Stats website: https://www.internetworldstats.com/stats1.htm

Isaac, M. (2019, March 30). Mark Zuckerberg's Call to Regulate Facebook, Explained. *The New York Times*. Retrieved from https://www.nytimes.com/2019/03/30/technology/mark-zuckerberg-facebook-regulation-explained.html

Jaeger, P. T., Bertot, J. C., McClure, C. R., & Langa, L. A. (2006). The Policy Implications of Internet Connectivity in Public Libraries. *Government Information Quarterly*, *23*(1), 123–141.

Kaufmann, K. (2018). Navigating a new life: Syrian refugees and their smartphones in Vienna. *Information, Communication & Society*, *21*(6), 882–898.

KC. (2019, May 9). These 16 U.S. States Passed Resolutions Recognizing Porn as a Public Health Issue. Retrieved December 9, 2019, from Fight the New Drug website: https://fightthenewdrug.org/here-are-the-states-that-have-passed-resolutions/

Kiragu, E., Li Rosi, A., & Morris, T. (2011). *State of denial: A review of UNHCR's response to the protracted situation of stateless Rohingya refugees in Bangladesh*. Retrieved from UNHCR Policy Development and Evaluation Service website: https://www.unhcr.org/4ee754c19.pdf

Klompmaker, N. (2019). Censor Them at Any Cost: A Social and Legal Assessment of Enhanced Action against Terrorist Content Online Scientific. *Amsterdam Law Forum*, (3), 3–29.

Lambropoulos, C. (2019, August 3). 5 Days in Kakuma Refugee Camp: Retrieved December 12, 2019, from Medium website: https://medium.com/swlh/5-days-in-kakuma-refugee-camp-11279ab3bf57

Levin, B., & de Sa, P. (2019). *Global Broadband Plan for Refugee Inclusion* (p. 367). Retrieved from The World Bank; USA for UNHCR, Tent.Org website: https://static1.squarespace.com/static/5a0f82f67131a5ac3ca77f03/t/5c9cd941ee6eb02afe82469a/1553783109805/GBP4RI+March+FINAL_For+Posting.pdf

Levin, S. (2018, July 3). Is Facebook a publisher? In public it says no, but in court it says yes. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit

Long, J. (2016, May 27). Opinion | Pornography is more than just sexual fantasy. It's cultural violence. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/in-theory/wp/2016/05/27/pornography-is-more-than-just-sexual-fantasy-its-cultural-violence/

MacRitchie, K. (2013, June 20). DadaabNet: Delivering Sustainable Internet to the World's Largest Refugee Camp – NetHope. Retrieved December 9, 2019, from NetHope website: https://nethope.org/2013/06/20/dadaabnet-delivering-sustainable-internet-to-the-worlds-largest-refugee-camp/

Madianou, M. (2019). Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media + Society*, *5*(3).

Maganza, F. (2017, June 20). Standing with refugees and nonprofits that serve them on World Refugee Day. Retrieved December 9, 2019, from Google.org: The Keyword website: https://blog.google/outreach-initiatives/google-org/standing-refugees-and-nonprofits-serve-them-world-refugee-day/

Mandic, D. (2017). Trafficking and Syrian Refugee Smuggling: Evidence from the Balkan Route. *Social Inclusion*. https://doi.org/10.17645/si.v5i2.917

Marlowe, J. (2019). *Refugee resettlement, social media and the social organization of difference*. Retrieved from Global Networks Partnership & John Wiley & Sons Ltd. website: https://onlinelibrary.wiley.com/doi/abs/10.1111/glob.12233

Mastercard Foundation. (2019). About the Smart Communities Coalition. Retrieved December 9, 2019, from Smart Communities Coalition website: https://www.mastercard.us/en-us/governments/find-solutions/smart-communities.html

Mozur, P. (2018, October 15). A Genocide Incited on Facebook, With Posts From Myanmar's Military. *The New York Times*. Retrieved from https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

NetHope. (2019a). DadaabNet: Part 1: Overview of Project. Retrieved December 9, 2019, from NetHope Solutions Center website: https://solutionscenter.nethope.org/implementation-guides/dadaabnet/Overview

NetHope. (2019b). Our Mission – NetHope. Retrieved December 9, 2019, from NetHope website: https://nethope.org/our-mission/

NetHope. (2019c, April 24). Connectivity for humanity: Efforts aid Venezuelan migrants in Colombia – NetHope. Retrieved December 12, 2019, from NetHope blog website: https://nethope.org/2019/04/24/connectivity-for-humanity-efforts-aid-venezuelan-migrants-in-colombia/

NetHope. (2019d, June 12). IOM and RIS to assume maintenance of NetHope networks for refugees in Greece – NetHope. Retrieved December 12, 2019, from NetHope blog website: https://nethope.org/2019/12/06/iom-and-greek-government-to-assume-maintenance-of-nethope-networks-for-refugees/

NetHope. (2019e, October 14). Greek engineers work to continue connectivity for Syrian refugees—Greece. Retrieved December 9, 2019, from ReliefWeb website: https://reliefweb.int/report/greece/greek-engineers-work-continue-connectivity-syrian-refugees

Omori, K., Zhang, Y. B., Allen, M., Ota, H., & Imamura, M. (2011). Japanese college students' media exposure to sexually explicit materials, perceptions of women, and sexually permissive attitudes. *Journal of Intercultural Communication Research*, *40*(2), 93–110.

Orenstein, D. I., & Stoll-Ron, L. (2014). Internet Filters and Academic Freedom: Librarian and Stakeholder Perceptions and Their Impact on Access to Information. *LIBRES: Library and Information Science Research Electronic Journal*, *24*(2), 62.

Otuki, N. (2017, January 3). Safaricom paid Sh7.5 billion for Nairobi security network. *Business Daily*. Retrieved from https://www.businessdailyafrica.com/corporate/Safaricom-paid-Sh7-5-billion-for-security-network-contract/539550-3505148-10lgf3b/index.html

Panova, T., & Lleras, A. (2016). Avoidance or boredom: Negative mental health outcomes associated with use of Information and Communication Technologies depend on users' motivations. *Computers in Human Behavior*, *58*, 249–258.

Poole, D., Latonero, M., & Berens, J. (2018). *Refugee Connectivity: A Survey of Mobile Phones, Mental Health, and Privacy at a Syrian Refugee Camp in Greece*. Retrieved from Harvard Humanitarian Initiative; Data & Society Institute; Centre for Innovation, Leiden University website: https://datasociety.net/wp-content/uploads/2018/04/Refugee_Connectivity_Web.MB4_.8-2.pdf

Porter, J. (2019, March 21). Here's how the EU plans to fight online terrorism content. Retrieved December 10, 2019, from The Verge website: https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu

Radu, R. (2019). *Negotiating Internet Governance*. Oxford University Press.

RCRWireless News. (2016, January 21). Wi-Fi for emerging markets: Connecting the next billion - Wi-Fi Now Episode 21. Retrieved December 10, 2019, from RCR Wireless News website: https://www.rcrwireless.com/rcrtv/wi-fi-for-emerging-markets-connecting-the-next-billion-wi-fi-now-episode-21

Red Hook Initiative. (2019). Who We Are [Organization]. Retrieved December 12, 2019, from Red Hook Initiative website: https://rhicenter.org/

Reglitz, M. (2019). The Human Right to Free Internet Access. *Journal of Applied Philosophy*, *n/a*(n/a). https://doi.org/10.1111/japp.12395

Riemens, P. (2011, August 31). *[Wsfii-discuss] [Fwd: Himalayan Effort AirJaldi is connecting rural communities through wifi and innovation. HIMANSHU KAKKAR (Outlook Business)]*. Retrieved from https://lists.okfn.org/pipermail/wsfii-discuss/2011-August/002155.html

Romm, T. (2019, April 9). A flood online of hate speech greets lawmakers probing Facebook and Google about white nationalism. Retrieved December 9, 2019, from Washington Post website: https://www.washingtonpost.com/technology/2019/04/09/flood-online-hate-speech-greets-lawmakers-probing-facebook-google-about-white-nationalism/

Safaricom. (2015). *Terms and Conditions for Safaricom Internet at Home (Fibre to the Home) Service*. Retrieved from https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/terms_and_conditions_for_safaricom_internet_at_home_service.pdf

Safaricom. (2019). *Safaricom Data Privacy Statement*. Retrieved from https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/C1_Safaricom_Data_Privacy_Statement.pdf

Schlindwein, S. (2019, July 20). Uganda: One year of social media tax. Retrieved December 12, 2019, from DW.COM website: https://www.dw.com/en/uganda-one-year-of-social-media-tax/a-49672632

Seacom. (2019). Seacom Acceptable Use Policy. Retrieved December 9, 2019, from Seacom website: https://seacom.com/legal-acceptable-use-policy

SES. (2019a). Networks in Africa: Bridging the digital divide [Corporate]. Retrieved December 12, 2019, from SES website: https://www.ses.com/africa/networks-africa

SES. (2019b). SES Fair Usage Policy. Retrieved December 9, 2019, from Bigblu website: https://bigblu.co.uk/ses-fair-usage-policy/

Seuferling, P. (2019). "We Demand Better Ways to Communicate": Pre-Digital Media Practices in Refugee Camps. *Media and Communication*, *7*(2), 207–217.

Shapshak, T. (2019, July 3). Google And Facebook To Build Own Undersea Cables Around Africa. *Forbes*. Retrieved from https://www.forbes.com/sites/tobyshapshak/2019/07/03/google-and-facebook-to-build-own-undersea-cables-around-africa/

Shieber, J. (2019, April 4). Amazon joins SpaceX, OneWeb and Facebook in the race to create space-based internet services. *TechCrunch*. Retrieved from http://social.techcrunch.com/2019/04/04/amazon-joins-spacex-one-web-and-facebook-in-the-race-to-create-space-based-internet-services/

Solon, O. (2019, September 20). Six months after Christchurch shootings, videos of attack are still on Facebook [News]. Retrieved December 12, 2019, from NBC News website: https://www.nbcnews.com/tech/tech-news/six-months-after-christchurch-shootings-videos-attack-are-still-facebook-n1056691

Spacey, R., Muir, A., Cooke, L., Creaser, C., & Spezi, V. (2017). Filtering wireless (Wi-Fi) Internet access in public places. *Journal of Librarianship and Information Science*, *49*(1), 15–25.

Suardiaz, G. (2019, April 5). A Personal Account of a Tech Partner in Colombia – NetHope. Retrieved December 9, 2019, from NetHope website: https://nethope.org/2019/03/05/i-am-nethope-a-personal-account-of-a-tech-partner-in-colombia%ef%bb%bf/

UN General Assembly. (1948). *Universal Declaration of Human Rights*. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

UN General Assembly. (2016, June 27). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. A/HRC/32/L.20*. Retrieved from https://digitallibrary.un.org/record/845728?ln=en#record-files-collapse-header

UN Sustainable Development Goals. (2019). Sustainable Development Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization. Retrieved December 9, 2019, from UN Sustainable Development Goals Knowledge Platform website: https://sustainabledevelopment.un.org/sdg9

UNHCR. (2017, May 30). UNHCR refers Kenya staff to police after internal investigation finds fraud at Kakuma camp. Retrieved December 10, 2019, from UNHCR website: https://www.unhcr.org/news/press/2017/5/592dcf644/unhcr-refers-kenya-staff-police-internal-investigation-finds-fraud-kakuma.html

UNHCR. (2019). *Displaced & Disconnected: Connectivity for Refugees*. Retrieved from UNHCR website: https://www.unhcr.org/innovation/wp-content/uploads/2019/02/Displaced-Disconnected-WEB.pdf

UNHCR. (n.d.). *Community Technology Access (CTA) programme: "Empowerment through Technology": ANNEX VI*. Presented at the UNHCR. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjh2fGq0KnmAhUEoVwKHbCWDjMQFjADegQIBBAC&url=https%3A%2F%2Fwww.ungm.org%2FUNUser%2FDocuments%2FDownloadPublicDocument%3FdocId%3D47157&usg=AOvVaw1PEzUQyi87vZLEJuyRY4wX

UNHCR Innovation Service. (2018, July 3). Connectivity for Refugees: Where are we two years later. Retrieved December 9, 2019, from UNHCR Innovation Service website: https://www.unhcr.org/innovation/cfr-two-years-in/

UNHCR Innovation Service. (2019). Connectivity for Refugees: Introduction. Retrieved December 12, 2019, from UNHCR Innovation website: https://www.unhcr.org/innovation/connectivity-for-refugees/

UNHCR Kenya. (2019). Dadaab Refugee Complex—UNHCR Kenya. Retrieved December 12, 2019, from UNHCR Kenya website: https://www.unhcr.org/ke/dadaab-refugee-complex

UNHCR South Africa. (2019, October 18). It has been brought to our attention that the following FRAUDULENT notice is being circulated on social media. [Social Media]. Retrieved December 10, 2019, from Facebook website: https://www.facebook.com/UNHCRSouthernAfrica/posts/1443937112441682

United Nations, General Assembly. (2018, September 13). *Report of the United Nations High Commissioner for Refugees: Part II Global compact on refugees, A/73/12*. Retrieved from https://www.unhcr.org/gcr/GCR_English.pdf

Von Behr, I. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*.

Wright, P. J., & Tokunaga, R. S. (2016). Men's objectifying media consumption, objectification of women, and attitudes supportive of violence against women. *Archives of Sexual Behavior*, *45*(4), 955–964.

Xu, Y., & Maitland, C. (2016). Communication behaviors when displaced: A case study of Za'atari Syrian refugee camp. *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, 58. ACM.

Yafi, E., Yefimova, K., & Fisher, K. E. (2018). Young Hackers: Hacking Technology at Za'atari Syrian Refugee Camp. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, CS21. ACM.

YouTube. (2019). Violent or graphic content policies—YouTube Help. Retrieved December 10, 2019, from YouTube Help—YouTube policies—Violent of graphic content policies website: https://support.google.com/youtube/answer/2802008?hl=en

Zimmerman, J. (2019, August 16). RidgeBuilder™ 2019 Challenge: People on the Move—Kakuma Connected. Retrieved December 12, 2019, from OpenIDEO website: https://challenges.openideo.com/challenge/2019-bridgebuilder-challenge/ideas/building-the-internet-infrastructure-in-kakuma-refugee-camp-facilitating-learning-and-information-exchange-amongst-community-members

UNHCR Innovation Service

unhcr.org/innovation | @unhcrinnovation