ESTABLISHING MOBILE CONNECTIVITY IN REFUGEE CAMPS

HARVARD HUMANITARIAN INITIATIVE

MERCY CORPS

CONTENTS

Cite as: Caitlin N. Howarth, Adrienne Brooks, Danielle N. Poole, Robert Claro, John Traylor and Meghann Rhynard-Geil, "Establishing Mobile Connectivity in Refugee Camps," Mercy Corps and Harvard Humanitarian Initiative: Cambridge, MA (August 2020). Accessible at https://www.mercycorps.org/what-we-do/technology

This material is published under a Creative Commons Attribution-Noncommercial 4.0 International license.

Questions, collaboration and field enumerator contact requests can be directed to Adrienne Brooks (abrooks@mercycorps.org) or Dr. Danielle N. Poole dap355@mail.harvard.edu

WITH THANKS

The authors wish to thank Rahmani Abdulrahman, Farog Ali, Musa Drammah, Fode Mballo, and Syed Ahmad Ali Shah for their contributions as field interpreters and commitment to advancing refugee rights. This project would not have been possible without the leadership of Meghann Rhynard-Geil, Alexa Schmidt, Jesus Melendez Vicente and Susan Tannehill.

Special thanks also go to those building rights-based approachs and operational frameworks for humanitarian information activities and technology applications, including but not limited to Nathaniel A. Raymond, Stuart Campo, Jos Berens, Massimo Marelli, Christopher Kuner, Robert Reimann, and John Warnes. Their work and that of contributors to the OCHA Working Draft of Data Responsibility Guidelines, the ICRC Professional Standards for Protection Work, the ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, the Signal Code: A Human Rights Approach to Information During Crisis, NetHope, the Emergency Telecommunications Cluster, and UNHCR's Connectivity for Refugees can be seen throughout this guide.

This guide was conducted in a partnership between the Technology for Development (T4D) initiaitve of Mercy Corps and the Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative (HHI), and was funded by the Cisco-Mercy Corps Technology for Impact partnership.

USING THE GUIDE

This guide serves as a collected reference for establishing a rights-based approach to Internet connectivity as aid in refugee camps. The rapid evolution of technology, connectivity-oriented humanitarian resources, private-public partnerships, and affected population needs will require practitioners to update their minimum standards of good practice on at least an annual basis. This guide and related References offer an overview of key resources for routine updates collected by global experts in this field. The guide also offers a preliminary sample of what shared minimum standards for Internet connectivity as aid could require.

Connectivity as aid represents a response to shared infrastructure challenges in humanitarian settings. An agreed-upon set of shared standards will help the humanitarian sector organize its response to shared challenges and leverage its collective strength – including its financial investments – to benefit the safe, ethical and effective establishment of connectivity for affected populations.

This guide includes and adapts materials from several existing frameworks, including the OCHA Working Draft of Data Responsibility Guidelines, the ICRC Professional Standards for Protection Work, the ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, the Signal Code: A Human Rights Approach to Information During Crisis, and more. Cases are drawn from these resources as well as literature review conducted by the authors, including past and ongoing work by NetHope, the Emergency Telecommunications Cluster, UNHCR's Connectivity for Refugees, and CISCO Tactical Operations. A full reference set is available for this guide, providing essential orientation and updated good practice for humanitarian practitioners worldwide.

This guide focuses on **connectivity as aid**, specifically the objective to **provide mobile Internet access directly to affected populations in refugee camps via WiFi**. Related objectives, such as connectivity for aid (i.e., connectivity as an essential tool supporting humanitarian aid practitioners) and cellular network access for affected populations, can be informed by but are not fully addressed in this guide.

To better understand the current landscape of connectivity as aid, its challenges, and the insights provided by recent evidence collection among people on the move, some may wish to begin by reading "Connecting People on the Move: The Humanitarian's Duty of Care," which was developed alongside this guide.

RESPONSE	**ORIENTATION**
New response effort	Practitioners can establish safe, ethical and effective ICT infrastructure, private-public partnerships, and data management policies and practices from Day Zero of aid to an affected population. This effort starts with an orientation to the human rights at stake, the practitioner's obligations when establishing connectivity as aid, and the planning stages necessary to determine if connectivity as aid can be safely, ethically and effectively established as part of the overall response.
Existing response: no established measures for connectivity as aid	Some responses lack clear guidance to establish connectivity as aid. Practitioners can use this guide to establish a shared vocabulary, assess their operating environment, and launch a planning and budget process that incorporates the entire lifecycle of ICT and user data.
Existing response: some established measures for connectivity for and/or as aid	Due to years of dedicated work establishing connectivity for aid in both acute and protracted crises (see: Mercy Corps 'Technology for Good', NetHope, UNHCR Connectivity for Refugees), many new and ongoing responses have some operating principles and standard procedures in place. Practitioners working to extend or improve connectivity as aid can use this guide to assess assets, identify gaps and challenges, and review how they can deliver connectivity as aid without creating unacceptable levels of risk to the affected population. This guide may be helpful in coordinating a needs assessment and/or establishing advocacy objectives in environments where these benefits cannot be safely extended to affected populations due to ongoing protection threats. Practitioners may find it useful to start their work at a specific point of entry (e.g., Internet service provider contract renegotiation), leveraging that process to engage in planning process to improve and standardize their ongoing effort.
Organizations supporting connectivity as aid and conducting humanitarian information activities	Any organization can utilize this guide to better understand the challenges and benefits of connecting affected populations through WiFi. Organizations dedicated to protracted crises and long-term development objectives may find useful tools for planning multi-year ICT infrastructure efforts, as well as informing their awareness of policies and practices that could impact the safe and ethical delivery of connectivity as aid. This guide can also help establish an organizational commitment to data responsibility and affected population protection during information activities, using this specific implementation concept to orient their overall understanding of and standard response to the challenges involved. Some organizations may wish to adopt standards of good practice based on those set by similar organizations (see References), or draft policies specific to their organizational principles, needs and operating environments. Some organizations may determine, through their assessment of needs and organizational practices, that they should enter into strategic partnerships and/or join ongoing efforts to help inform and collectively negotiate terms for establishing Internet connectivity in their region.

1. A RIGHTS-BASED APPROACH

This guide uses a rights-based approach to design, implement and assess connectivity in a migrant and refugee context. A rights-based approach is constructed to position the core rights of the affected person – the migrant or refugee – as the primary objectives. Used by the Sphere Standards, Professional Standards of Protection Work, and other essential guidelines for humanitarian practice, the rights-based approach articulates the ultimate human rights at stake in order to ensure that practitioners understand how the implementation of these minimum technical standards works to achieve a broader impact. Executed well, a rights-based approach should also fundamentally center the people – both individual and collective – whose rights are at stake.

Across the various handbooks and standards of practice for humanitarian organizations, multiple human rights and organizational operating principles are established. Any organization attempting a rights-based approach to connectivity as aid should first examine this landscape against its own principles. When informed by a diverse and inclusive set of local actors, including representatives of the affected population itself, an organization can then define the principles, objectives, priorities and phases of its effort to establish Internet connectivity as aid.

This guide utilizes the Signal Code, which gathers input from across the humanitarian sector to articulate five interrelated human rights:

- **The Right to Information**
- **The Right to Protection**
- **The Right to Privacy and Security**
- **The Right to Data Agency**
- **The Right to Rectification and Redress**

These rights are interrelated because a failure to fulfill any one of these rights will undermine the success of the others. For example: If refugees are provided with open Internet access (i.e., access to information) but that access requires the refugee to surrender all privacy, then the humanitarian cannot claim that the refugee's right to information has been fully realized. Yes, the refugee may have access to the Internet – but without privacy, that access is neither free nor uncompromised. It could even produce a protection threat. Privacy, protection and access must all exist if the right to information is to be considered real and meaningfully upheld.

The Signal Code

The Right to Information

Access to information during crisis, as well as the means to communicate it, is a basic humanitarian need. Thus, all people and populations have a fundamental right to generate, access, acquire, transmit, and benefit from information during crisis. The right to information during crisis exists at every phase of a crisis, regardless of the geographic location, political, cultural, or operational context or its severity.

The Right to Protection

All people have a right to protection of their life, liberty, and security of person from potential threats and harms resulting directly or indirectly from the use of ICTs or data that may pertain to them. These harms and threats include factors and instances that impact or may impact a person's safety, social status, and respect for their human rights. Populations affected by crises, in particular armed conflict and other violent situations, are fundamentally vulnerable. HIAs have the potential to cause and magnify unique types of risks and harms that increase the vulnerability of these at-risk populations, especially by the mishandling of sensitive data.

The Right to Privacy and Security

All people have a right to have their personal information treated in ways consistent with internationally accepted legal, ethical, and technical standards of individual privacy and data protection. Any exception to data privacy and protection during crises exercised by humanitarian actors must be applied in ways consistent with international human rights and humanitarian law and standards.

The Right to Data Agency

Everyone has the right to agency over the collection, use, and disclosure of their personally identifiable information (PII) and aggregate data that includes their personal information, such as demographically identifiable information (DII). Populations have the right to be reasonably informed about information activities during all phases of information acquisition and use.

The Right to Rectification and Redress

All people have the right to rectification of demonstrably false, inaccurate, or incomplete data collected about them. As part of this right, individuals and communities have a right to establish the existence of and access to personal data collected about themselves. All people have a right to redress from relevant parties when harm was caused as a result of either data collected about them or the way in which data pertaining to them were collected, processed, or used.

HARVARD
HUMANITARIAN
INITIATIVE

Signal
Human Security
+ Technology

2. ORIENTATION, PLANNING & DESIGN

When designing an Internet connectivity as aid program, humanitarian organizations and practitioners first orient themselves to the needs of the affected population, the challenges and opportunities of the operational environment, and the principles, goals and objectives specific to their organization or scope. A global or country-wide effort may begin at the rights-based principles stage, first establishing its overarching objectives and legal parameters; local practitioners often begin with an understanding of affected population needs and gaps in aid. Regardless of how an Internet connectivity as aid effort is initiated, all practitioners should ensure that their work is grounded by clear understanding of affected population needs, the operational environment, and the principles they seek to achieve. Defining these three dimensions orients the overall effort and will determine relevant costs, phases, legal requirements, implementation standards, partnerships, and much more. Practitioners can also use this orientation and planning phase to position themselves as part of shared efforts to build Internet connectivity across all populations in their region, establishing their seat at the public infrastructure negotiation table as representatives of often underserved or intentionally excluded people on the move. The sooner practitioners join collective efforts to establish secure, equitable Internet connectivity, the more effective and cost-efficient their implementation plans can be.[1]

2.1.1. OPERATIONAL CONTEXT

Prior to launching any Internet connectivity as aid effort, whether for the first time or as part of ongoing humanitarian activities, practitioners must have a clear understanding of their operating environment. Achieving this requires a combination of activities to determine the existing landscape of ICT infrastructure assets and actors, applicable laws, operational context, and requisite expertise to establish connectivity safely, ethically and effectively.

Efforts to establish Internet connectivity as aid vary widely based on timing and operational context, as surrounding conditions of conflict, extreme weather, political change, and economic upheaval will significantly impact everything from the availability of existing ICT infrastructure to the risk assessment for using it. Humanitarians benefit from learning about their operational context from a wide range of local and global actors with verifiable insights into ICT business investments, civil rights and liberties, security conditions, ICT access regulations, and local media. Local actors can best orient practitioners to both challenges and opportunities to overcome or circumvent connectivity barriers, and it is essential to learn directly from affected populations. Populations on the move face unique barriers to Internet connectivity – particularly via mobile devices, e.g., phones – that longtime residents may not experience.

2.1.2. NATURAL DISASTERS

Practitioners working in natural disaster-prone regions (and/or those experiencing upticks in extreme weather events) will need to assess their context and planning based on the resilience of existing ICT infrastructure, connectivity blackout patterns from previous crises (including those exacerbated or determined by energy utilities and Internet service providers), and investments in redundant (fail-over) systems. When orienting for connectivity as aid objectives, it is important to note that natural disaster response contexts tend to favor 'mission critical' actors over the affected population. Humanitarian first responders have established increasingly sophisticated, resilient systems for Internet connectivity during these crises that support their own operation, but connectivity for suddenly displaced populations often remains a secondary or tertiary priority assigned primarily to commercial ICT service providers.

Ensuring ongoing connectivity as aid objectives in such conditions requires humanitarians to assess:

- Opportunities to pre-position communal information sharing channels in the event of sustained Internet connectivity blackout;
- Alternative digital and analog technologies and strategies for information sharing;
- Information ecosystems and trusted amplifiers;
- Protection concerns and data management policies related to these alternatives; and
- Expectations for Internet connectivity resumption based on prior disasters.

Although this guide does not examine alternative digital and analog technologies, these resources are crucial redundancy measures. Local communities and affected persons are often the best source of information about these alternatives and successful communication strategies, particularly civil society organizers with a track record of successful word-of-mouth campaigns. Mapping existing information ecosystems, including amplifiers (i.e., locally trusted sources of information, persons with particular influence among specific communities), will help those in disaster-prone areas best anticipate how to work when Internet connectivity is suspended – as well as how to maximize its efficacy when operational. There are no 'one source serves all' solutions; when it comes to information sharing during crises, humanitarians must anticipate diverse needs and include trusted amplifiers to underserved communities in order to design a full and equitable response plan.

2.1.3. CONFLICT ZONES

Those operating in conflict environments will face targeted, pervasive threats to ICT infrastructure and the data lifecycle it supports. Communications infrastructure is often one of the first targets for destruction during conflict, as opposing forces seek to limit each other's operational capacity or force the use of communication channels vulnerable to surveillance, interception, and manipulation. Humanitarians establishing Internet connectivity in these conditions must frequently do so independent of terrestrial infrastructure, using high-cost satellite technology to establish and secure connectivity for limited mission critical use. Even when Internet infrastructure is available, humanitarians seeking to establish connectivity as aid must be aware of significantly increased threats to affected populations who may use it and evaluate whether connectivity as aid under such conditions can even be ethical, let alone effective.

For more on network security and humanitarian protection measures, explore the ICRC Handbook on Data Protection in Humanitarian Action.

2.1.4. IDP CAMPS

Like refugee camps, internally displaced persons (IDP) camps run by humanitarian organizations already maintain rights-based standards of operation with implementation, accountability and learning mechanisms. However, their relative position vis-à-vis the source of their displacement – particularly when displaced due to conflict or if subject to targeted action by the state – requires a unique protection risk analysis when evaluating the potential and design of Internet connectivity as aid on-site. This is not to indicate that such aid cannot be provided, only to note that the needs assessment and vulnerabilities of the affected population may vary, including among subgroups within a camp. Ethical consideration of how to equitably provide connectivity as aid under such conditions may alter the "go/no go" decision to implement access.

2.1.5. REFUGEE CAMPS

The refugee camp environment, somewhat removed from the immediate source of the refugee's crisis, provides a structured context for Internet connectivity as aid efforts where it may be possible to achieve safe, ethical and effective access. From UNHCR's Connectivity for Refugees initiative to the Mercy Corps technology work that inspired this guide, refugee camps already operate with accepted, shared standards for design, implementation, monitoring and accountability. These shared expectations, defined by managing agencies and the Sphere Standards, create an operational scaffold within which to shape Internet connectivity as aid to their residents. The refugee camp context will be the primary focus of this guide, establishing a standard duty of care that can be utilized in other contexts for contrast and project viability assessment.

2.2. REGULATORY AND INFRASTRUCTURE MAPPING

2.2.1. ICT INFRASTRUCTURE LANDSCAPE

Mapping existing ICT infrastructure, service providers, and last-mile solutions is an essential phase of establishing Internet connectivity as aid in refugee camps. Unlike humanitarian innovation efforts that have been able to produce sustainable solutions for shelter, WASH facilities, food and medical aid in resource-limited environments, Internet connectivity can be prohibitively expensive to generate at the scale necessary for quality connectivity as aid absent significant investments in terrestrial networks and the active participation of multiple government and private sector partners. Aid efforts have tended to prioritize mission critical ICT connectivity for humanitarian professionals in refugee and IDP camp settings, using satellite systems independent of local ICT networks.

Longstanding practitioner reliance upon VSAT solutions may produce a tendency to overlook the importance of ICT infrastructure mapping when negotiating camp locations with host governments. But unlike providing shelter and medical aid, the international humanitarian organization tendency to parachute in solutions cannot suffice for connectivity - despite the fact that access to information during crises is a human right, and that Internet connectivity is increasingly recognized worldwide as a critical necessity for daily life. Organizations must recognize that in order to realize Internet connectivity as aid with the urgency required in emergencies, they will need to dedicate more resources to collaborative efforts that aggregate demand, negotiate terms consistent with humanitarian obligations, and invest in infrastructure protected to outlast even a protracted crisis. Such a challenge may be best suited to a triple nexus approach blending expertise and strategic planning by humanitarian, development, and peace actors to create sustainable solutions with protected status (particularly during present or future conflict).[2]

As noted by Schmitt et al (2018), established refugee camps tend to sit in ICT infrastructure-poor environments where connectivity of any kind is limited or non-existent. This contributes to a unique information ecosystem for refugees, who may become more reliant upon limited sources and generate more word-of-mouth information networks than they would use in a non-camp setting.[3] (For more information on refugee information networks and related protection concerns, see “Connecting People on the Move” and related references.) Humanitarians should note that studies report information access conditions in camps that tends to be poorer than in surrounding communities and more vulnerable to misinformation[4] and rumor - conditions that should concern anyone at a time when information manipulation and misinformation have compromised aid worker safety and aid access.[5] Ensuring more, consistent and independent access to verified, up-to-date and relevant resources like Refugee.Info should be a priority for any camp management team attempting to combat distrust and misinformation.

DadaabNet

When natural and human-driven emergencies forced over 500,000 people to a camp originally designed for 90,000 in Kenya, multiple agencies combined efforts to expand the camp’s core infrastructure - including its Internet architecture.

This two-fold exercise in connectivity for aid and connectivity as aid illustrates the range of technical and organizational options for operations at this scale and complexity, while also demonstrating the limits of humanitarian design to date. To learn more, view the reports by NetHope, Inveneo, and others available at: https://solutionscenter.nethope.org/implementation-guides/dadaabnet

2.2.2. REGULATORY LANDSCAPE & PUBLIC-PRIVATE PARTNERSHIPS

Understanding the full regulatory landscape that governs an innately international resource like Internet connectivity requires dedicated expertise that few local aid efforts can support. Collective efforts like NetHope and the Emergency Telecommunications Cluster pool coordination alongside service provider networks and technical expertise to help ensure that humanitarian organizations remain consistently up to date on the daily evolutions in regulations, infrastructure capacity and connectivity threats worldwide. Private-public partnerships are the norm as aid providers develop their capacities; to that end, organizations like NetHope help establish shared legal standards for service provider contracts, as well as access to preferential terms as a result of collective bargaining via their Demand Aggregation initiative. Efforts to synchronize legal terms and procurement policies for ICT connectivity can improve not only the quality of service provided to affected populations, but the systems interoperability between humanitarian organizations working to securely share sensitive information and facilitate rapid, effective aid delivery. Guidelines for partnerships specific to ICT connectivity already exist, including the Humanitarian Connectivity Charter and OCHA guidance on data responsibility in public-private partnerships.

As noted in the Handbook on Data Protection in Humanitarian Action, affected populations may be discussed as if they are typical 'consumers' of ICT service; however, they are uniquely and significantly vulnerable to protection threats as a result of their status. Simply connecting to an open WiFi network established at a refugee camp may be sufficient to attract the interest of actors interested in the identity, location, activity and movement of whoever holds the connected mobile device. When examining the regulatory landscape, humanitarians must carefully assess local laws requiring third party disclosure of metadata that can readily identify individuals and specific communities (e.g., women, LGBTQ+). As it is virtually impossible to establish Internet connectivity as aid at scale without multiple third party involvement - involvement often well behind the scenes and not apparent to non-experts - humanitarian organizations have a clear duty to invest in training and expert support that will help detect and explain the implications of metadata sharing in the local environment.[6] To offer Internet connectivity as aid without such awareness and corresponding mitigation strategies would be to endanger affected populations and compromise the core humanitarian principle to protect.

Information Ecosystems

The concept of information ecosystems exists across various sciences, and the understanding of how information flows between people during crisis continues to evolve. In **Digital Lifeline? ICTs for Refugees and Displaced Persons**, Carleen Maitland et al explore the ways in which being on the move and in camp settings creates unique information ecosystems that shape actions, risk perceptions, routes, and more. Instead of accepting the common trope of the refugee as lacking resources, Maitland et al study how agency flows from and among those on the move. Those attempting to center the people in the design of humantiarian practice will find these studies useful when challenging assumptions about whose partnership should be primary.

WHO HAS ACCESS TO BENEFICIARY DATA?

BACKHAUL NETWORKS

PIPE OPERATORS

LAST-MILE SERVICE

TRAFFIC MONITORS

3RD PARTY COMPANIES

GOVERNMENTS

HUMANITARIAN ORGANIZATIONS

2.2.3. INDIVIDUAL MOBILE DEVICES ON COMMUNAL WIFI NETWORKS

Although this guide primarily focuses on the provision of and challenges associated with communal humanitarian Internet connectivity, WiFi networks necessary to establish connectivity as aid at scale in a refugee camp setting require knowledge of the regulations for mobile ICT devices. Mobile phones represent an essential lifeline for refugees on the move and at points of arrival, leaving metadata footprints across countries and regulatory frameworks. Registration for SIM cards often requires users to provide such personal information as their name, national identification, and date of birth - information that humanitarians will recognize as sensitive and vulnerable for use as targeting data when associated with the user's location. A user's IMSI (unique SIM number) and IMEI (unique device number) are logged by service providers to facilitate billing, along with time and location of transactions (e.g., calls and messages) and information associated with SIM card registration (with variation by country regulations and SIM type, such as pre- or post-paid accounts).

Refugees face a multitude of challenges related to identification and registration, often generating informal workarounds to obtain SIM cards along the journey and at points of arrival.[7] From a protection perspective, humanitarian objectives are best served by minimizing data collection and organizations should resist efforts to establish SIM card registration as a feature of refugee or IDP aid provision. To learn more about digital identification protection concerns and their relationship to ICT technologies, see Chapter 12 of the Handbook on Data Protection in Humanitarian Action.

Even without formal registration linking a user's unique mobile device to a WiFi network, metadata collected by third party service providers can generate digital identities based on behavioral attributes. Activity patterns of purchases, social media use, call detail records, etc. can be collected and amalgamated using machine learning to generate 'algorithmic identification' and link the user's digital footprint to their offline identity.[8] Studies of behavior patterns utilizing consumer data have already demonstrated high consistency of rapid re-identification based on only a handful of metadata points.[9] Interested actors with access to third party service provider user records and/or commercial databases can leverage these tools to identify, track, and surveil the activities of those they consider persons of interest. Even when mobile devices are shared among users, distinct activity patterns can still be detected. Such network analysis can generate risks to beneficiaries profiled as or linked secondarily to persons of interest by counterterrorism and national security agencies.[10]

Humanitarian Internet connectivity providers, particularly those leveraging WiFi networks to achieve scale, should be aware of the potential for harm to affected populations and design mitigation techniques consistent with both local laws and their humanitarian obligation to protect. If connectivity cannot be achieved without meaningful protection from surveillance, humanitarians need to assess whether or not providing a shared point of access for affected populations presents a greater threat than potential benefit. Protection by network design and default should be a standard any connectivity as aid activity is measured against.

2.2.4. COMMUNAL DEVICES ON COMMUNAL WIFI NETWORKS

One possible alternative to those providing Internet connectivity as aid is to follow the model established by public libraries.[11] By providing communal access to shared devices connected at a single location, humanitarians can systematically improve hardware security, ensure that encryption measures are in place, and maintain an information ecosystem that supports individual use while providing a layer of collective anonymity. Unique user activity will still generate digital footprints that can be analysed to reverse engineer personally identifiable information; however, legal means of obfuscation (e.g., virtual private networks and onion routing) can be deployed to disconnect these footprints from the physical location of the refugee camp, further separating the location and time stamps from specific users. Digitally savvy users, particularly those who have grown up with Internet connectivity access, can be expected to have some familiarity with these tools simply to pursue recreational activities, such as music and video entertainment via often-restricted torrent services.

2.2.5. EQUITABLE CONNECTIVITY AND DATA MINIMIZATION

As illustrated in "Connecting People on the Move," torrent activity and high-bandwidth Internet use can quickly exhaust a refugee camp's limited resources and exponentially increase costs. Finding technical solutions to limit such activity - to preserve access equity for all users - while minimizing activity surveillance is an essential activity for aid providers. Network activity management technologies provided by companies like CISCO can help maintain high quality, equitable Internet connectivity for users. These tools and their aid provision benefits must also be counterbalanced by data collection minimization, secure and limited access archival, and routine destruction. As with all data records, aid providers must be aware of any archival requirements mandated by local law and organizational policy, ensuring compliance while remaining consistent with humanitarian obligations to the affected data subject. Humanitarians act as data controllers in this capacity, a status which carries specific legal and operational requirements.[12]

3. DESIGNING INCLUSIVE CONNECTIVITY

The humanitarian's objective is to provide meaningful Internet access consistent with the rights and dignity of every member of the target affected population. For Internet access and use to be meaningful, it should be possible for any user to achieve high-speed, consistent connection and functionality (non-inclusive of functions deemed illegal or otherwise disallowed through the organization's equitable access policy, e.g., torrenting). This relies upon at least four key factors:

- Signal Strength
- Location
- Bandwidth
- Time

3.1.1. SIGNAL STRENGTH

Signal strength is measured by the consistency of high-speed access suitable to meet beneficiary needs. Definitions of "high-speed" will vary based on a combination of regional Internet infrastructure and applications prioritized by beneficiaries. Beneficiary expectations for signal strength and speed are often established through consumer behavior prior to arrival in camp settings, whether in their home countries or along the journey. Benchmarking facilitated by organizations like GSMA therefore plays an important role in establishing metrics for humanitarian connectivity as aid.

WiFi Network Strength

WiFi signal should be available throughout the area where humanitarian aid recipients are gathered.

Signal strength should be at least 66 percent to be considered meaningful, as measured by a user's mobile device (e.g., phone).

Any beneficiary should be able to easily and frequently access areas with connectivity as part of their daily routine. If communal devices are provided, beneficiaries should be able to easily and equitably access these resources without compromising other forms of aid

Sub-Optimal	Minimum	Optimal
Signal strength is less than 66% in the majority of common areas; users must congregate close to a single or small set of connectivity areas in order to gain Internet access. Users may not have routine daily access to areas with connectivity.	Signal strength is at least 66% in primary common areas (excluding areas deemed sensitive for protection purposes, e.g., bathrooms). All affected population users have meaningful access to primary common areas at least once per day.	Signal strength is 100% in primary common areas and at least 66% in private spaces. All affected population users have meaningful access to primary common areas and secure access to private spaces throughout the day and evening.

Humanitarianism for Who?

In many histories of humanitarian aid, the central figure who summons the will to act decisively is typically cisgendered male, white, from the Global North, socioeconomically advantaged, Christian, and heterosexual. Their movement into emergencies is a sudden twist while pursuing a different profession for their primary income. Their path remains celebrated as a classic narrative: the Hero's Journey, a maverick mobilizing against the tides for those too vulnerable to withstand them.

This narrative deserves more skepticism, as do its implications for the systems - reinforced by billions of dollars - both in humanitarianism and technology-centered solutions. Reimagining the future of these fields, Aarathi Krishnan, Evgeny Morozov and others offer tech-savvy perspectives on how to realign decisions about risk and protection with those who bear their consequences. Exploring ways to make aid more inclusive - and ceasing to excuse inequities and discrimination in aid organizations - should center any effort to connect us all.

Communal Network Strength

Internet access through communal devices (e.g., desktop computers and kiosks at static locations) is a) predictable and b) available at least 75% of the time that stations are open to beneficiaries.

Sub-Optimal	Minimum	Optimal
Internet connectivity is unpredictable and available less than 75% of the time that stations are open to beneficiaries.	Internet connectivity is predictable and available at least 75% of the time that stations are open to beneficiaries.	Internet connectivity is predictable and available more than 75% of the time that stations are open to beneficiaries.

3.1.2. LOCATION & ACCESSIBILITY

Whether delivered through communal stations or WiFi networks, equitable and inclusive delivery of connectivity as aid in camp settings must be assessed by whether all potential users are able to benefit from Internet access. Not all spaces within a camp are equally accessible to all residents: women, families, unaccompanied minors, the elderly and those with disabilities or certain health conditions may each have designated quarters in which to sleep, play, socialize, eat, and conduct other routine activities as part of life in the camp. Some of these differentiations are by design, built and enforced by humanitarians to ensure specific protection outcomes for particularly vulnerable populations (including those with 'invisible' vulnerabilities, such as identifying as LGBTQ+). Other differentiations are defined and enforced through social and cultural norms among the camp population.

An Internet connectivity needs assessment should be designed to detect and measure the range of social and physical factors that can influence access to both the Internet and the devices necessary to connect to it. Reports on digital gender and disability gaps[13] can help humanitarians establish shared metrics for consistent longitudinal evaluation. Specific investments should be made to build relationships with trusted sub-group interlocutors, as illustrated in "Connecting People on the Move." Mapping connectivity infrastructure throughout a camp, assessing signal strength and device access for especially vulnerable persons in spaces and at times during which they can safely, securely and effectively go online, is an essential asset to design and implement an inclusive and equitable connectivity as aid program.

Assessing Equity and Inclusion for Connectivity as Aid

Sub-Optimal	Minimum	Optimal
Especially vulnerable populations (e.g., women, unaccompanied minors, those with disabilities, LGBTQ+ persons) can only access the Internet in communal spaces dominated by other groups. Internet access for these persons is persistently mediated through social norms and physical features that restrict access to Internet-connected devices. Signal strength is less than 75% in sub-group locations and private spaces.	Especially vulnerable populations (e.g., women, unaccompanied minors, those with disabilities, LGBTQ+ persons) can access the Internet in camp-wide communal spaces, in sub-group specific locations (e.g., housing designated for women and families), and in private spaces (i.e., individual shelters). Signal strength is at least 75% or greater in sub-group locations and private spaces. Internet access for these persons is facilitated through programming and device provision specific to the needs of each group.	All especially vulnerable persons can access the Internet safely and effectively without constraints or negative consequences due to device ownership, social norms, or lack of privacy. Those with conditions requiring accommodation (e.g., hearing or sight impaired, low digital and/or reading literacy) have access to tools and support specific to their conditions.

3.1.3. BANDWIDTH

Bandwidth refers to the amount of information a user can transmit in a given unit of time, as well as the range of frequencies used to transmit the data. Many non-expert users experience this as the capacity of an Internet network to support total user traffic at the same rate at any given time using standardized, independently verifiable measures of upload and download speeds. Expectations of what constitutes high-speed bandwidth is typically set through regional consumer experience (see above), and through humanitarian negotiations with Internet Service Providers (ISPs). Depending on local regulations and available ICT infrastructure (i.e., backhaul, pipe, over the top and last-mile access), service provider rates will vary to establish consistent user access to high-speed Internet at the scale required by a camp's population size.

To achieve humanitarian objectives for connectivity as aid, practitioners should assess:

- Whether the ratio of WiFi bandwidth and/or shared access stations to user base (i.e., affected population size) supports meaningful access for most users most of the time. Bandwidth is sufficient to conduct basic activities, which may or may not include video streaming as resources allow.

- Meaningful access is defined as being able to connect to the Internet and conduct basic activities, such as:
  - Sending and receiving text messages and emails;
  - Making VOIP audio calls;
  - Accessing non-limited Internet sites and services (e.g., non-inclusive of audio-visual torrenting);
  - Accessing standard support services and information via Refugee.info; and
  - Sending or receiving money, and conducting online banking.

- Depending on available resources, meaningful and equitable access may not include the ability to stream or download all audio-visual files during certain hours of the day.

- WiFi network(s) provided by humanitarian actors should provide sufficient bandwidth to meet affected population needs as assessed through evidence-based survey methods. Members of the affected population should not need to rely upon self-funded data plans in order to conduct routine, basic functions as described above.

Assessing Bandwidth for Internet Connectivity as Aid

Sub-Optimal	Minimum	Optimal
Most users cannot conduct basic Internet activities during most of the day due to insufficient bandwidth. Attempts to access basic services time-out and fail more than 25% of the time.	Most users can send and receive text messages, make VOIP audio calls, access most websites*, and send and receive money during most of the time available for network access. Attempts to use basic services time-out and fail less than 25% of the time. *Does not include video streaming or large file downloads	All users can send and receive text messages, make VOIP audio calls, access most websites*, send and receive money, and download and use mobile apps throughout the day. Attempts to use basic services time-out and fail less than 5% of the time. *May include sites that include video streaming, such as Facebook and YouTube, throughout the day or during designated periods

3.1.4. TIME

In addition to the speeds associated with network bandwidth, beneficiary time is a critical metric of success or failure for connectivity as aid programs. Humanitarian standards of care should reflect the ubiquity of Internet access for beneficiaries in ways comparable to standards for accessing shelter, food, medical care, and WASH facilities. When installation or other constraints limit user access to Internet networks, the need to achieve high-quality connectivity is increasingly concentrated in the time allowed per user. Time limitations and variations may also, along with other factors, impact equitable and inclusive access to Internet connectivity.

To assess beneficiary time as a metric for connectivity as aid, humanitarians may find the following definitions helpful:

- Most users can achieve meaningful WiFi or fixed Internet connectivity when they need it, including during hours that support social connection, legal aid, education, financial inclusion, and access to other forms of humanitarian aid.

- Depending on humanitarian resources and available bandwidth, user access restrictions may vary throughout the day. These restrictions should not generate inequitable access to Internet networks among beneficiaries.

Sub-Optimal	**Minimum**	**Optimal**
Most users cannot achieve meaningful WiFi Internet connectivity for basic activities for more than 2 hours in each 24-hour period. Users cannot access, generate, or receive information or services related to education, employment, financial inclusion, legal aid or familial connection during the hours those resources are available.	Most users can achieve meaningful WiFi Internet connectivity for basic activities for more than 2 hours in each 24-hour period. Users can regularly generate and receive information or services related to education, employment, financial inclusion, legal aid, and familial connection during some hours in which those resources are online and available.	All users can achieve meaningful WiFi Internet connectivity for basic activities whenever they need it, day or night. Users can regularly generate and receive information or services related to education, employment, legal aid, financial inclusion, and familial connection during the hours most optimal for those activities.

3.1.5. INTERDEPENDENT RIGHTS AND STANDARDS

Just as the human rights realized through connectivity as aid are interdependent upon one another, the design and standards of Internet networks in humanitarian settings require holistic, inclusive efforts to achieve meaningful, equitable, safe and effective benefits for all. No single technology or access point supports the entire range of needs expressed by vulnerable populations. Humanitarians must include diverse perspectives to inform needs assessment, infrastructure and information ecosystem mapping, protection threat assessment, and evaluation indicators. Bias toward dominant groups in information access will only continue or be exacerbated by humanitarian aid unless inclusive, specific efforts are made to achieve connectivity equity.

Inclusive Needs Assessment - Sample

	One Size Fits Some	**Bias-Adjusted**
Enumerator Recruitment	Recruit based on number of enumerators needed, with preference for necessary local languages. Recruitment may take place immediately prior to the beginning of the survey.	Identify range of enumerators needed based on preliminary population demographic analysis; include at least one woman. Recruitment planning should begin with potential enumerators being identified during the pre-assessment stage.
Participant Recruitment: Census	Enumerators canvass population at large without resources dedicated to a specific area.	Dedicated enumerator(s) canvass specific parts of a camp designated for certain groups (e.g., women and families), maintaining a consistent presence in physical space and building rapport over the course of the study.
Interlocutors & Amplifiers	Obtain necessary permissions to enter camp and conduct assessment among participants, consistent with local laws, ethical guidelines and humanitarian requirements.	In addition to standard permissions and review, conduct pre-assessment to identify local interlocutors with established relationships among the affected population, including those who may be under-represented at a particular site (e.g., women, LGBTQ+). Incorporate interlocutor feedback into survey design and facilitate follow-up that meets both specific populations' needs and study requirements.
Time	Planned based on necessary n population size to generate statistically meaningful results* (*Or meaningful results defined by on study methodology)	Additional time allotted to ensure sufficient interaction with underrepresented populations. When possible, document the relative length of time necessary to recruit participants; this will inform future good practice.

4. CENTERING SUPPORT & CONSENT

Once Internet connectivity has been planned, data access negotiatied, infrastructure established, and powered on, humanitarians have at least two major tasks in their next phase: 1) establish meaningful and informed consent to the terms under which this aid is provided, and 2) centering the needs of those on the move in their online experience.

4.1. ESTABLISHING CONSENT

To determine whether an Internet network's user has consented to the terms and conditions of use, volumes of references would be necessary. Establishing consent in aid environments carries specific difficulties, given the potential perception that only when terms are accepted will aid be rendered - a perception that defines 'coercion.' Beyond the refugee camp environment, the issue of meaningful and informed consent in the use of everyday digital technology applications and data transfer has been increasingly examined. Many doubt how informed a user can be when asked to download a mobile app for immediate use, only to see a dense array of legal jargon end with the options "Do Not Accept" and "Accept". The situation is made clearer when "Do Not Accept" simply deletes the app altogether, leaving the user with fewer options than they had before.

As humanitarians navigate the complex web of third party metadata collection and data transfers (see Section 2.2.3 above), a few steps may help provide meaningful opportunities for informed consent and improved beneficiary protection:

Accessible descriptions of how the network functions | Illustrating key concepts like metadata, identification, and government access through visual imagery and relevant language translation helps demonstrate that warnings are present, and that the beneficiary can take simple actions to limit their exposure using tools like VPNs and privacy-enhancing software. Materials and guides in local languages already exist through human rights organizations dedicated to supporting safe, sensitive information sharing around the world.

Illustrate how to avoid detection | To avoid coercive effects on beneficiaries seeking connectivity as aid, humanitarians can provide illustrated, accessible guides for how to access WiFi without detection. Establishing HTTPS Everywhere protocol by default, as well as advertising free and non-exploitative virtual private network (VPN) tools, can help ensure that no user must submit to data surveillance as a condition of their connection.

Identify what data is collected, for which specific purposes, and how to submit requests for redress. | Any beneficiary should receive a clear, concise overview of what metadata may be collected while using the local WiFi network, as well as what that data may be used for, who can access it, and who the relevant Data Protection Officer is at the camp.

Powering Access

The most basic requirement for Internet access may also be a key to centering support and consent among beneficiaries: electrical power. Establishing charging areas throughout a camp provides hubs for offline information distribution, both verbal through camp personnel and visual through posters. Where possible, shade and seating help establish a social area to facilitate informal information exchange.

Simple kiosks with permanently-installed charging cords can further support beneficiaries who may not otherwise be able to use their mobile device at the time or to the extent they require.

By providing social- and technology-specific support areas, camp managers can help establish hubs for information exchange that may prove crucial when attempting to dispel rumor or promote aid.

These steps are extensively outlined in the Handbook on Data Protection in Humanitarian Activities.

Describe how different types of use impact others - and offer alternatives. | Most restrictions on humanitarian WiFi or fixed broadband use reflect bandwidth issues, limiting the amount and types of audiovisual content that can be streamed or downloaded. To ensure that beneficiaries support a strong local network, while respecting their dignity and choices, humanitarians may design alternative hubs for music and video downloading and sharing.

Through the camp registration process, posters in common areas, and periodic digital security workshops for camp residents, this information can be made accessible and appropriate to beneficiary needs.

4.2. PROMOTING INFORMATION AS AID: Refugee.Info

A simple step in supporting Internet connectivity as aid: facilitate access to up-to-date, refugee-specific information and resources. Posted signs and a simple country-specific splash page directing WiFi users to the resources at **Refugee.Info** can help beneficiaries better understand the information available to them. Leveraging the existing Refugee.Info investments through advanced user interaction analytics can help push improvements in user-centered design and offline support to camps where re-alignment of information and aid can support safer, more effective interventions.

Sub-Optimal	Minimum	Optimal
Information about how metadata is collected through WiFi use is difficult to find or is not offered to beneficiaries. Alternative ways to safely access the Internet using the WiFi are not illustrated. A clear majority of beneficiaries report no awareness that metadata is being collected and/or that this data can be used to track their activities and movements in the host country.	Information about how metadata is collected through WiFi use is clear and easy to find when the beneficiary first joins the WiFi network. Alternative ways to safely access the Internet while still using the WiFi are illustrated. Some beneficiaries report using these tools. A clear majority of beneficiaries report some awareness that metadata is being collected and/or that this data can be used to track their activities and movements in the host country.	Information about how metadata is collected through WiFi use is clear and easy to find when the beneficiary joins the WiFi network. Alternative ways to safely access the Internet while still using the WiFi are illustrated. Some beneficiaries report using these tools. A clear majority of beneficiaries report some awareness that metadata is being collected and/or that this data can be used to track their activities and movements in the host country. Time spent in the camp correlates with increased awareness of these risks and ways to mitigate them.

5. MEASURING AND EVALUATING CONNECTIVITY

Practitioners seeking to establish connectivity as aid have a range of options available and should exploit the opportunity to more accurately measure the potential positive impact of connectivity on psychosocial wellbeing, among other metrics. Beginning with a **pre-installation assessment** among current or probable beneficiaries, a baseline study can establish levels of depression and anxiety, mobile device and Internet access, and relative levels of digital security awareness pre-intervention. These baselines can provide an essential evidence foundation for future iteration and improvements, as well as a sound basis for ongoing investment in connectivity as aid.

Some evaluations, such as one establishing a baseline for beneficiary behavior and ICT access, require survey methods. Other forms of monitoring and evaluation can be conducted through rigorous tracking of **WiFi network use** and **user interface analysis of Refugee.Info**. It is essential that such monitoring and evaluation be coupled with ongoing, digital and analog efforts to support meaningful informed consent among beneficiaries.

Humanitarians supporting connectivity as aid have a further duty to establish a **Data Protection Officer** trained in digital network protection, beneficiary rights, and local challenges to beneficiary protection and privacy. This role should be established before any network is put online, or as an immediate step for programs without one. Full details of a Data Protection Officer's role, responsibilities, and resources can be found in the ICRC Handbook for Data Protection in Humanitarian Activities. In emergencies, including crisis-compounding events like natural disasters, humanitarians should have a **designated point of contact for the Emergency Telecommunications Cluster**. It is important that this person not be solely responsible for both emergency connectivity and data protection during a crisis; supplemental training for other camp managers should be sufficient to orient them to the responsible data guidelines they all must follow as part of daily operations, and this orientation should provide sufficient personnel coverage in acute emergencies to ensure that any critical incidents do not go missed.

5.1. CRITICAL INCIDENTS

At any time during a connectivity as aid program, a critical incident may occur in which a humanitarian WiFi network's security, users, and/or data are compromised. Individual users may also experience critical incidents, such as hacking or the spread of malware, that can indicate a potential digital threat to the broader camp population. The Data Protection Officer is responsible for collecting, documenting and reporting these incidents, ideally as part of a humanitarian collective effort to identify digital threats to beneficiaries. Mitigation steps should be taken to the furthest extent possible immediately upon the Data Protection Officer's verification of a critical incident report.

Critical Incidents

Critical incidents are events that compromise a user's or community's rights to access to information, creating a threat to their protection, privacy, and ability to access and/or use and share information. Shared learning and mitigation techniques remain in their infancy among humanitarian organizations, as recent critical incident investigations by The New Humanitarian have demonstrated. OCHA provides helpful guidance on identifying and managing these events.

ENDNOTES

1. NetHope, "Demand Aggregation for Improved Connectivity." Accessed 20 August 2020 at https://solutionscenter.nethope.org/program-areas/connectivity-infrastructure/demand-aggregation-for-improved-connectivity.

2. Redvers, Louise and Ben Parker. "Searching for the nexus: Give peace a chance." *The New Humanitarian*, 13 May 2020. Accessed 20 August 2020 at https://www.thenewhumanitarian.org/analysis/2020/05/13/triple-nexus-peace-development-security-humanitarian-policy.

3. Schmitt, Paul, Daniel Iland, Elizabeth Belding, and Mariya Zheleva. "Cellular and Internet Connectivity for Displaced Persons," in *Digital Lifeline? ICTs for Refugees and Displaced Persons* (ed: Carleen F. Maitland), MIT Press: Cambridge, MA (2018), 115-119.

4. Carlson, Melissa, Laura Jakli, Katerina Linos, "Rumors and Refugees: How Government-Created Information Vacuums Undermine Effective Crisis Management," *International Studies Quarterly*, Volume 62, Issue 3, September 2018, Pages 671–685, https://doiorg.ezp-prod1.hul.harvard.edu/10.1093/isq/sqy018

5. Russell Hargrave, "Aid groups targeted by fake news, report says," *The New Humanitarian*, 14 February 2018. Accessed 20 August 2020 at https://www.devex.com/news/aid-groups-targeted-by-fake-news-report-says-92096

6. ICRC, "International Data Sharing," *Handbook on Data Protection in Humanitarian Action* (2nd edition), Geneva: 2020, 68-81 https://www.icrc.org/en/data-protection-humanitarian-action-handbook

7. Ibid, ""Digital Identity," 206-221.

8. Ibid, Chapter 6, "Data Analytics and Big Data." ; Mittelstadt et al, "The ethics of algorithms: Mapping the debate," Big *Data & Society* 3:2 (1 December 2016), accessible via https://doi.org/10.1177/2053951716679679.

9. Centre for Humanitarian Data, "Statistical Disclosure Control," Guidance Note Series: Data Responsibility in Humanitarian Action, OCHA (7 August 2019). Available at https://centre.humdata.org/guidance-note-statistical-disclosure-control/

10. Albader, Fatemah. "The Digital War on Human Rights: Guilty until Proven Innocent: In Light of the Counter-Terrorism and Border Security Act of 2019," *Minnesota Journal of International Law*: 29:2 (2020), 21-42.

11. Nijboer, Jelke. "Big Brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11," *New Libary World* 105:7, 256-261. Available at https://doi.org/10.1108/03074800410551002

12. ICRC Handbook on Data Protection for Humanitarian Action, 80.

13. Robinson, Alex et al, "Gap Analysis: The Inclusion of People with Disability and Older People in Humanitarian Response," Elhra (7 August 2020), available at https://www.elrha.org/researchdatabase/gap-analysis-humanitarian-inclusion-disabilities-older-people-literature-review/; GSMA. "The Mobile Gender Gap Report 2019," London, UK: GSM Association, September 2019. Available at https://www.gsma.com/mobilefordevelopment/resources/mobile-gender-gap-report-2019/