CONNECTIVITY AS AID

POSSIBLE USE

CHALLENGES

CHAPTER 16

CONNECTIVITY AS AID

Aaron Martin and John Warnes*

* The authors would like to thank Robert Riemann (European Data Protection Supervisor), Antonella Napolitano and Ed Geraghty (Privacy International) for their input and feedback on this chapter.

16.1 INTRODUCTION

In emergencies, staying connected can help affected persons get in touch with separated family members, plan safe routes, find shelter, engage with Humanitarian Organizations, and access humanitarian and other services. Yet after disasters, the telecommunications networks on which connectivity[1] relies frequently stop working, depriving affected people of the communication channels on which they increasingly rely. Similar situations arise in conflict settings where networks can become compromised or in other humanitarian situations where perhaps connectivity levels were low even prior to an emergency.

However, affected communities attach considerable importance to connectivity. In 2016, for instance, aid workers assisting migrants in Greece reported that they often asked for Internet access before food and water.[2] Humanitarian Organizations have recognized the importance of connectivity and developed a range of programmes accordingly.

It is important to differentiate between connectivity *as* aid and connectivity *for* aid. The latter refers to providing connectivity to aid workers so they can carry out their work, while the former relates to providing connectivity to affected people and offering related services as a form of aid in times of emergency or in protracted crises.[3]

This chapter focuses on data protection issues arising from connectivity *as* aid, and at two different levels: community and individual. At the community level, Humanitarian Organizations typically set up hot spots or provide connectivity at community centres. In such cases, organizations usually manage the "pipe" (that is, the physical infrastructure such as cables and fibre bundles needed to provide connectivity), which is shared among users. At the individual level, Humanitarian Organizations may support people in their dealings with connectivity providers, but individuals will have greater responsibility for their own access to connectivity.[4] The distinction between these two levels also has implications for the data protection responsibilities of Humanitarian Organizations.

1 For the purposes of this chapter, "connectivity" refers to access to mobile and Internet connections.

2 Lin Taylor, "Internet Is As Important As Food And Water To Refugees In Greece", Huffington Post, 22 July 2016: www.huffpost.com/entry/internet-is-as-important-as-food-and-water-to-refugees-in-greece_n_57928a22e4b02d5d5ed1ac5b.

3 For a longer discussion on the distinction and its implications, see: ICRC, "DigitHarium | Month #5: Connectivity as Aid, for Aid, Denial", International Committee of the Red Cross, Geneva, 9 July 2021: www.icrc.org/en/digitharium/digitharium-month-5.

4 See for example: UNHCR Innovation, "Connectivity for Refugees", UNHCR Innovation (blog), 2019: www.unhcr.org/innovation/connectivity-for-refugees.

16.1.1 OVERVIEW OF CONNECTIVITY AS AID INTERVENTIONS

Various initiatives and organizations are working to provide connectivity in emergencies and address connectivity black spots. Most recently, within the United Nations system specific efforts have been made to strengthen and systematize coordination and delivery of connectivity as aid interventions, notably the **UN Secretary General's Roadmap for Digital Cooperation,** an initiative aimed at mobilizing all stakeholders to play a role in advancing a safer, more equitable digital world. One of the key pillars of this initiative is the "Global Connectivity" pillar, with the objective of achieving universal connectivity by 2030, and action 5 within this pillar focusing on humanitarian situations.[5]

Operational initiatives to provide connectivity as aid include but are not limited to:

- The **Emergency Telecommunications Cluster (ETC)** is a global network of organizations that work together to provide shared communications services in humanitarian emergencies. The ETC is one of the 11 clusters designated by the Inter-Agency Standing Committee (IASC).[6]
- The UNHCR **Innovation Service's Digital Innovation programme** undertakes activities that innovate around connectivity solutions for forcibly displaced people and host communities, taking a rights-based approach that emphasizes inclusion in national systems. UNHCR's mandated role in coordinating refugee responses may also include coordination of refugee-facing connectivity interventions.
- A newly formed multi-stakeholder initiative on **Connectivity for Refugees**, supported by UNHCR, the ITU, GSMA and Government of Luxembourg seeks to advance connectivity for 20m forcibly displaced people and their hosts by 2030 by fostering deeper cooperation between states and private enterprise.
- **GIGA** is a programme set up by the International Telecommunication Union and UNICEF to "connect every school to the internet and every young person to information, opportunity and choice".[7]
- **NGOs such as NetHope,[8] its members,[9] Télécoms Sans Frontières[10] and many others** provide connectivity solutions in various emergency preparedness and response settings.

5 United Nations, "Secretary-General's Roadmap for Digital Cooperation", United Nations, June 2020: www.un.org/en/content/digital-cooperation-roadmap.

6 "Emergency Telecommunications Cluster (ETC)", accessed 1 April 2022: www.etcluster.org.

7 UNICEF and ITU, "Giga – Connect Every School to the Internet", Giga Initiative, accessed 1 April 2022: https://gigaconnect.org.

8 NetHope, Inc, "Homepage", NetHope, 18 October 2021: https://nethope.org.

9 NetHope, Inc, "Our Members", NetHope, 2 November 2021: nethope.org/who-we-are/our-members.

10 Télécoms Sans Frontières (TSF), "Home", Télécoms Sans Frontières – ONG téléphonie humanitaire | Telecoms Sans Frontieres – NGO in Humanitarian calling, accessed 1 April 2022: www.tsfi.org/en.

Certain private-sector initiatives, beyond commercial connectivity services (cellular or otherwise) provided to the affected population, are also worth noting:

- **CISCO Crisis Response** (TacOps)[11] deploys a range of technologies and network equipment to provide free communication networks to both Humanitarian Organizations and beneficiaries after disasters. After the 8.1-magnitude earthquake in Nepal in 2015, for instance, Cisco Crisis Response was on the ground within 72 hours to restore communications.
- In many contexts, satellite companies[12] operate Corporate Social Responsibility (CSR) programmes that leverage their technology to facilitate connectivity for affected communities in humanitarian contexts, often in partnership with Humanitarian Organizations.
- **Before it was closed in December 2022, Meta Connectivity**[13] was also involved in a number of initiatives, including Free Basics, which aimed to provide free Internet access worldwide, and High Altitude Connectivity, which involved advancing the use of high-altitude platform station (HAPS) connectivity systems and satellite technology to bring connectivity to remote areas at lower costs.
- **Loon**[14] (now defunct) was an initiative initially led by Alphabet Inc. to connect people by deploying balloons containing the essential components of cell towers to bring Internet access to areas not covered by existing networks.

16.1.2 OPERATIONAL CONTEXT

When starting a connectivity as aid programme, it is important to remember that crises are complex situations, and that the circumstances and people affected will differ from one crisis to the next. Likewise, connectivity programmes will vary according to the context. For some, the emphasis will be on building existing network resilience to future natural disasters or emergencies. For others, the focus will be on establishing connectivity in areas where it has never existed. Although practical arrangements will inevitably differ, organizations will need to consider some common factors no matter what type of programme they are implementing. The first is the regulatory landscape, which will determine what the organization and potential service users (such as affected communities) can and cannot do. The second is the commercial and non-commercial organizations currently providing connectivity in the area. Indeed, Humanitarian Organizations often engage with private-sector

11 Cisco, "Incident Response – Connecting Communities in Crisis", Cisco, accessed 1 April 2022: www.cisco.com/c/en/us/about/csr/impact/cisco-crisis-response/incident-response.html.

12 Michael Oduor, "Boosting Self Reliance among Refugees through Satellite Connectivity", Africanews, 28 May 2021: www.africanews.com/2021/05/28/boosting-self-reliance-among-refugees-through-satellite-connectivity; SES, "SES Is Enabling Disaster Response and Connecting Affected Communities", Bloomberg.Com, 22 March 2017: www.bloomberg.com/press-releases/2017-03-22/ses-is-enabling-disaster-response-and-connecting-affected-communities; "Intelsat Customer UNHCR Wins Changing Lives Award at AfricaCom 2017", Intelsat (blog), 16 November 2017: www.intelsat.com/newsroom/intelsat-customer-unhcr-wins-changing-lives-award-at-africacom-2017.

13 Meta, "Meta Connectivity", accessed 1 April 2022: www.facebook.com/connectivity.

14 "Loon", X, the moonshot factory, accessed 1 April 2022: https://x.company/projects/loon.

entities throughout part or all of the connectivity chain and, as these partnerships have become increasingly common, organizations in both sectors have developed guidelines on how to cooperate with one another.[15]

When considering partnering with other entities (see Section 16.1.3 – Multiple stakeholders and partnerships, below), Humanitarian Organizations are always advised to assess the risks of such partnerships. One way to do so, at least in part, is through a Data Protection Impact Assessment (DPIA) – an exercise that can be designed to look beyond core data protection issues (see Section 16.2 – Data Protection Impact Assessments, below) and seeks to ensure that the partnership will follow "do no harm" principles and minimize and mitigate risks as far as reasonably possible.

16.1.3 MULTIPLE STAKEHOLDERS AND PARTNERSHIPS

Humanitarian Organizations may not have the necessary expertise, technology or equipment to implement a connectivity programme alone. This means that they may have to partner with one or more connectivity or technology providers in order to achieve their objectives. These can include non-profit organizations, private enterprises (such as telecommunications providers and technology companies), and NGOs providing connectivity solutions in emergencies.

Aside from considering the other parties involved, it is also important to understand that providing connectivity may be a layered process. As mentioned above, there are two different levels: community and individual. At the individual level, beneficiaries bear a greater responsibility for their own connectivity, since connectivity operators may collect data directly from them.

Once connectivity is established, there are additional (so-called "over-the-top") services, such as social media services running on top of a mobile service contract, mobile wallets or mobile money. Some providers of these services may offer their products directly to affected persons receiving aid. Here, although affected persons are technically acting as consumers, they are in fact more vulnerable than the average consumer. There are also less visible parties involved in connectivity programmes, such as infrastructure providers and those working on the backhaul to bring connectivity to Humanitarian Organizations or service providers (such as bandwidth providers). Providers can also add deep package inspection (DPI)[16] to the network as an added layer of protection. DPI involves filtering unwanted packets (units of data sent from an origin to a destination over the Internet) such as viruses or

15 See for example: GSMA, "Humanitarian Connectivity Charter", Mobile for Development (blog), accessed 1 April 2022: www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charter.

16 For more on deep package inspection, see: Rahul Awati and Jessica Scarpati, "What Is Deep Packet Inspection (DPI)?", Tech Target – Search Networking (blog), September 2021: www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI.

malware. Importantly, however, DPI makes it possible to identify the originator or recipient of content containing specific packets, meaning it can also be used for monitoring and surveillance purposes.

All these organizations and entities operating at different layers of the connectivity programme – backhaul, pipe, over-the-top and last-mile access – may collect or have access to users' data. This is because additional data and metadata are generated and processed at every layer of connectivity. This Processing by different entities is technically necessary, since sending a message from one location to another usually requires multiple entities knowing its source and destination.[17] These metadata (such as connection end points, "likes" and visits) may be accessible to some or all entities in the connectivity chain, which may be able to extract knowledge about humanitarian emergencies and the individuals involved in ways that are difficult for both beneficiaries and Humanitarian Organizations to anticipate.[18]

EXAMPLE OF CONNECTIVITY OPERATORS COLLECTING DATA DIRECTLY FROM AFFECTED PERSONS:

A domestic mobile network operator usually has access to the following information for billing purposes: unique identifiers for the SIM card and device (IMSI and IMEI numbers); time and location of transactions, such as calls and messages; and data obtained during SIM card registration.[19] The data obtained during SIM card registration may vary considerably from one country to another and according to the type of SIM card purchased (pre-paid or post-paid). Nevertheless, there has been a general tendency towards mandatory registration for all types of card, requiring users to provide Personal Data[20] such as a copy of their ID, their national identification number and their date of birth. In some cases, the individual is also cross-checked against a national ID database (India and Pakistan) or has their fingerprints and photograph taken (Nigeria, for instance).[21] Research[22] has found that, in most cases, refugees and other forcibly displaced people struggle to obtain SIM cards through standard legal channels and resort instead to both formal and informal workarounds that both introduce additional risks to affected people and present challenges for Humanitarian Organizations in terms of mapping relevant data flows.

17 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 22–23.

18 Ibid., 23.

19 Ibid., 71.

20 Donovan and Martin, "The rise of African SIM registration". See also the European Court of Human Rights (ECHR) judgment in the case of *Breyer v. Germany* (application no. 50001/12), 30 January 2020.

21 GSMA, "Mandatory Registration of Prepaid SIM Cards".

22 UNHCR Innovation, "Displaced and Disconnected", UNHCR Innovation (blog), 2019: www.unhcr.org/innovation/displaced-and-disconnected.

In this context, Humanitarian Organizations will not have control over the whole connectivity chain and, therefore, cannot guarantee to protect individuals against having their data and metadata misused. The risks that may arise from this lack of control should be evaluated through Data Protection Impact Assessments (see Section 16.2 – Data Protection Impact Assessments, below) whenever Humanitarian Organizations and their partners play an active role in improving connectivity for affected communities. As a mitigating measure, some Humanitarian Organizations provide affected people with information and guidance on digital security.[23] While Humanitarian Organizations may opt to not provide connectivity when the risks prove high through a Data Protection Impact Assessment, the alternative options that might be pursued by communities through the open and black market could present even greater risk. Humanitarian Organizations should consider these risks holistically and take appropriate action that minimizes risk in the connectivity ecosystem.

16.2 DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA)[24] is carried out to identify, evaluate and address the risks posed to Data Subjects by the Processing of their Personal Data in connection with a project, policy, programme or other initiative. It should ultimately lead to measures promoting the avoidance, minimization, transfer or sharing of data protection risks. Before launching technology programmes that involve the Processing of Personal Data, Humanitarian Organizations should conduct a DPIA to assess the possible consequences, which could include unlawful use of beneficiaries' data by partners and government interference with the network.

Before entering into a partnership for a connectivity programme, a Humanitarian Organization should assess potential partners and their data protection policies, as well as the legal obligations to which they are subject or any Privileges and Immunities they may hold, in order to fully understand how they process people's data. In some cases, in the absence of ownership of the specific infrastructure needed or local assets required to provide connectivity, it may be very difficult to fully understand and control data flows. Where the organization is able to glean a clear picture of the connectivity landscape, the parties involved and the services they provide, it may be in a position to draft standard guidelines or requirements explaining the services it needs, including technical specifications and data protection requirements. This could help organizations engage with partners and shorten the time between engagement and agreement in times of emergency.

23 For more on data security, see Section 2.8 – Data security and Processing security.

24 See Chapter 5: Data Protection Impact Assessments (DPIAs).

It is also important to remember that, in the humanitarian sector, affected persons are especially vulnerable and the risk of harm is high. For these reasons, the DPIA should give due consideration to Data Subjects' other fundamental rights.[25] Since Humanitarian Organizations operate in accordance with humanitarian principles, it may also be appropriate to consider the rights and freedoms of all members of a given group or community when setting up connectivity programmes, including non-data related rights. In parallel to application of other appropriate risk assessment frameworks, a DPIA could, for instance, be designed to also identify issues around unequal access to the network[26] and the potential exclusion of certain groups that are not digitally literate. It is also important to consider that some of the partners with which Humanitarian Organizations work have business models that are based on the monetization of data, which may be incompatible with humanitarian principles. Organizations may also be unwilling to engage with some private-sector partners because of inadequate findings of human rights due diligence processes and the reputational risk that doing so can carry. If the DPIA indicates that a connectivity programme could create more problems than can be adequately mitigated, it may be appropriate to decide not to move forward with the programme.

16.3 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

A Data Controller is the person or organization who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. A Data Processor, meanwhile, is the person or organization who processes Personal Data on behalf of the Data Controller. These concepts are defined and discussed at greater length in Chapter 2: Basic principles of data protection.

25 See: EU Article 29 Working Party, Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, October, 2017; Raphaël Gellert, "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review*, Vol. 34, No. 2, 1 April 2018, pp. 279–288: https://doi.org/10.1016/J.CLSR.2017.12.003.

26 For example, young children and elderly people might not be able to benefit from connectivity programmes or access services that require connectivity as they may lack computer literacy. In addition, "[w]omen in low- and middle-income countries are 10% less likely to own a mobile phone, and are considerably less likely than men to use more transformative services. For example, women in low- and middle- income countries are 26% less likely than men to use mobile internet, and 33% less likely to use mobile money." Source: GSMA, *Connected Women: The Gender Analysis & Identification Toolkit. Estimating subscriber gender using machine learning*, GSMA, 2018, p. 6: www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/08/GSMA-Gender-Analysis-and-Identification-Report-August-2018.pdf.

When Humanitarian Organizations set up and operate connectivity programmes, they can act as either Data Controllers or Data Processors, depending on the role that they and other partners play in a programme. This distinction is important when attributing responsibilities for data Processing.

Since data are collected at different layers of a connectivity programme, it is important to map, as much as possible and based on information that can be made available or acquired from the providers, data flows at each layer, identifying who is collecting them, what the purposes are, how long the data are retained and with whom they are shared. This mapping exercise will help to identify what role each party, including the Humanitarian Organization, plays in deciding how data are processed – and, therefore, whether each one is acting as a Data Controller or a Data Processor.

If a Humanitarian Organization determines the final objective (purpose) of the programme (such as establishing connectivity) and chooses a specific partner to implement it (means), it qualifies as a Data Controller. This means that the organization has a range of obligations, including responding to requests from Data Subjects wishing to exercise their rights.[27] In some cases, Humanitarian Organizations and partners from other sectors will determine the purpose and means of the programme together and, therefore, act as joint controllers. In such situations, the joint controllers must set out their respective responsibilities, including the handling of Data Subjects' requests, in a written agreement.

16.4 BASIC DATA PROTECTION PRINCIPLES

16.4.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

When Personal Data are required to access connectivity services, or generated in the process, an appropriate legal basis for the Processing of these data is necessary. Such legal bases are listed in Chapter 3: Legal bases for Personal Data Processing, which also explains the challenges associated with using Consent as a legal basis in humanitarian settings. Consent in humanitarian contexts may not always be considered freely given, since beneficiaries may feel compelled to Consent when that is the only way to receive a specific service (in this case, connectivity). Moreover, the complexity surrounding connectivity as aid might make it difficult to rely on a properly informed Consent, since Data Subjects with lower levels of digital literacy might not be able to understand all aspects of the Processing. Here, Humanitarian Organizations and service providers should seek a different legal basis for data collection and Processing, such as those listed below:

27 See Section 2.11 – Rights of Data Subjects.

- **Public interest**: This may be an option for an organization that has a specific mandate to facilitate access to connectivity, or for a Data Processor operating under instruction of an organization with such a mandate.[28]
- **Legitimate interest of the Humanitarian Organization**: This basis could also be considered where establishing or re-establishing connectivity is in line with the organization's mission, and where doing so could help beneficiaries access other essential services and improve coordination of the humanitarian response. This basis would only apply, however, if the interest(s) pursued by the organization and the anticipated benefits of the Processing are not outweighed by the rights and freedoms of the individuals in question.[29]
- **Performance of a contract**: Private companies providing connectivity services to affected communities on a commercial basis under applicable contract law may utilize performance of a contract as the legal basis for data Processing.[30]
- **Legal obligation**: Some jurisdictions may require connectivity service users to be registered. Here, the legal basis for Processing users' data for registration would be compliance with a legal obligation.[31]

16.4.2 DATA SECURITY

Mobile network operators play an important role as providers of critical connectivity infrastructure. In emergencies, for instance, being able to communicate with ambulances and other health-care providers is vital to effective incident response. These operators are required, depending on the specific telecommunications regulations in a country of operation, to implement technical and organizational security measures in order to protect communication networks and keep the data they carry secure. These measures, which will depend on the degree of risk, include encryption and other technical ways of ensuring the confidentiality, integrity and availability of collected data, as well as the overall resilience of Processing systems and services.[32]

Some metadata stored on individual devices, however, may not be encrypted and may require alternative security measures.[33] Wherever possible, Humanitarian Organizations and individuals should routinely review and update the measures they take, in order to account for the development of new security technologies, and to ensure a level of data protection and security that is appropriate to the degree of risk involved in the Processing of Personal Data. It is important to remain mindful that some entities or organizations may have an interest in accessing the data and

28 See Chapter 3: Legal bases for Personal Data Processing.
29 See Section 3.5 – Legitimate interest.
30 See Section 3.6 – Performance of a contract.
31 See Section 3.7 – Compliance with a legal obligation.
32 For more on data security, see Section 2.8 – Data security and Processing security.
33 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018, 25.

metadata generated in connectivity programmes for non-humanitarian purposes, such as commercial targeting and exploitation, or surveillance.

EXAMPLE:
Germany and Denmark have passed laws that allow the authorities to carry out a detailed forensic analysis of asylum seekers' smartphones. The data and metadata extracted from their devices can be used "to verify claims made in their asylum applications or to obtain new information about their identity, their story, the route they took, etc.".[34] Similar legislation has been passed in Belgium, Switzerland[35] and Austria.[36] In practice, such laws could mean that data generated through connectivity programmes end up being used for purposes that, even if legitimate, may not be compatible with the principles by which Humanitarian Organizations abide.

Current surveillance methods can be quite sophisticated and obtain substantial amounts of data and metadata about users of a given network.[37] This is particularly concerning, since metadata can be used to infer information that an individual has not agreed to share, and make predictions about their behaviour, which would mean that data generated in the process of humanitarian services could end up being used as highly valuable information in conflict.

In some cases, a Humanitarian Organization – depending on its mandate and status – may need to cooperate with national or foreign government authorities on a given connectivity programme. This type of cooperation can be in the interest of affected persons, such as when medical data are shared with health authorities to facilitate the provision of medical aid and public health. Humanitarian Organizations should be transparent with affected persons about any such cooperation arrangements, and make clear that their data may be shared with national or foreign authorities.

Where possible, Humanitarian Organizations should negotiate security measures with their partners to ensure the highest level of security throughout the entire connectivity chain – including those parts of the chain outside the organization's control.

34 Ibid., 62.

35 See Secrétariat d'État aux migrations, "Mise en œuvre de la révision de la loi sur l'asile (LAsi): accélération des procédures d'asile", Governmental website, Confédération Suisse, 12 May 2018: www.sem.admin.ch/sem/fr/home/sem/rechtsetzung/archiv/aend-asylg-neustruktur.html.

36 ICRC and Privacy International, *The Humanitarian Metadata Problem*, October 2018. See also Parlament Österreich. "Fremdenrechtsänderungsgesetz 2018 – FrÄG 2018", Governmental website, 13 June 2018: www.parlament.gv.at/gegenstand/XXVI/I/189.

37 See for example: Bruce Schneier, "China Isn't the Only Problem with 5G", Foreign Policy (blog), 10 January 2020, https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance.

16.4.3 DATA RETENTION

Personal Data must not be kept for longer than is necessary to fulfil the purposes for which they were collected or to comply with applicable legal obligations.[38] This means that Personal Data should always be deleted or anonymized as soon as they are no longer needed. In connectivity programmes, however, the various partners may have different roles, policies and needs that could impact how they Process data, including how long they retain them for. Again, it is important at the outset to establish a written agreement setting out each party's responsibilities and data retention policies. This will ensure that Humanitarian Organizations fully understand what data are being held by each partner at a certain point in time, and where they are being stored.

Beyond retention required for fulfilment of a contract for connectivity services with the Data Subject, mobile network operators are also required to retain data about users for periods specified in national law. Requirements such as these are intended, for instance, to give law enforcement authorities access to data in case a crime is committed. Humanitarian Organizations should therefore analyse which data are actually needed to deploy the programme and, as far as they can, avoid the collection of any unnecessary data. If only a minimum amount of data is collected, then only a minimum amount can be retained.

16.4.4 INFORMATION

In connectivity programmes, Data Subjects should be informed in clear and plain language about what data relating to them are being collected, for what purpose and through which means. This is especially important in situations where it may not be obvious to Data Subjects that their data are being collected, such as when metadata are generated or when the data collected are inferred data (information that can be deduced from data explicitly given by the Data Subject or from other observations). Individuals should also be told whom they can contact to exercise their rights. This information will enable them to make informed decisions about whether or not to use a specific service, and to understand how to proceed when they wish to exercise their rights.

In the interest of transparency and full disclosure, Humanitarian Organizations are advised to inform Data Subjects about the Third Parties involved in the programme, which activities they are responsible for and how to contact them. They should also be informed about the actual and potential negative consequences and risks associated with receiving and using connectivity services, and with connectivity programmes in general. The example set by UNHCR, which informs individuals of the privacy risks associated with the El Jaguar campaign, is a helpful model to follow.[39]

38 See Section 2.7 – Data retention.

39 See El Jaguar, "Privacidad En Facebook". This campaign video provides tips on privacy and profile safety on social media.

16.5 INTERNATIONAL DATA SHARING

Data processed online routinely flow across national borders. This raises Personal Data protection concerns in relation to connectivity programmes. Although recognized legal mechanisms exist, such as the use of contractual clauses, it can be difficult for Humanitarian Organizations to implement them effectively, especially since connectivity solutions are often outside their control. That said, organizations should undertake due diligence to ensure that the provider has implemented the necessary data transfer arrangements.[40]

40 See Chapter 4: International Data Sharing.