GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Research on the Specific Risks or Constraints Associated with Data Sharing with Donors for Reporting Purposes in Humanitarian Operations

By FLORIAN WESTPHAL and CLAUDIA MEIER

SYNTHESIS REPORT
23 August 2020

gppi.net

COMMISSIONED BY THE INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) ON BEHALF OF THE HUMANITARIAN DATA & TRUST INITIATIVE (HDTI). THIS INDEPENDENT RESEARCH REFLECTS THE AUTHORS' VIEWS ONLY.

Contents

1 Introduction

Objectives. This research supports the ultimate objective of the Humanitarian Data and Trust Initiative (HDTI)[1] Wilton Park Dialogue: to allow government donors to request and humanitarian organizations to responsibly and safely share data on crisis-affected people with donors whilst doing no harm. It assesses whether and how the risks related to the sharing of data that were discussed at the Dialogue materialize in practice.[2] Separate research conducted by the University of Manchester is looking at how and why donor governments request data, and how they use it. Those findings, combined with the recommendations in this report, will inform the development of principles for safe and responsible data sharing by the HDTI Wilton Park Dialogue.

Methods. The analysis of the risks in this report is based on the observations of humanitarian and donor government staff working in or on the three countries examined as case studies: Bangladesh (response to the Rohingya refugee crisis), Nigeria, and Syria.[3] The research only looked at the past five years (2016-today), to account for the fact that data sharing risks and mitigation measures are changing rapidly. It draws on 35 confidential interviews with humanitarian staff, and ten with donor government agency representatives.[4] They included both field staff and staff at headquarters or regional offices. Depending on the structure of their organization and their role in it, the interviewees have different levels of exposure to data sharing with donors. A few primarily focus on data or information management, but most interviewees work in External Relations, Protection, Monitoring and Evaluation, and Programme Management. The organizations and donors selected for interviews were participants in the 2020 HDTI Wilton Park dialogue, or other international humanitarian organizations receiving direct government donor funding for their work in the three case study countries. Individual interviewees were identified thanks to recommendations by the

[1] For more information on the HDTI, see: https://centre.humdata.org/introducing-the-humanitarian-data-and-trust-initiative/

[2] This report uses mostly general terminology related to data to ensure that it is comprehensible to a non-expert audience. A set of full definitions of key terms used in this report can be found in Annex 1.

[3] The three contexts were suggested by the ICRC who commissioned the research on behalf of HDTI, and validated as relevant contexts by the Research Board in the inception phase.

[4] Six interviews were conducted during the inception phase of the research.

Research Board, personal contacts of the researchers, and suggestions by other interviewees. (See illustrations 1 and 2).

Illustration 1: Number of Interviews by Organization

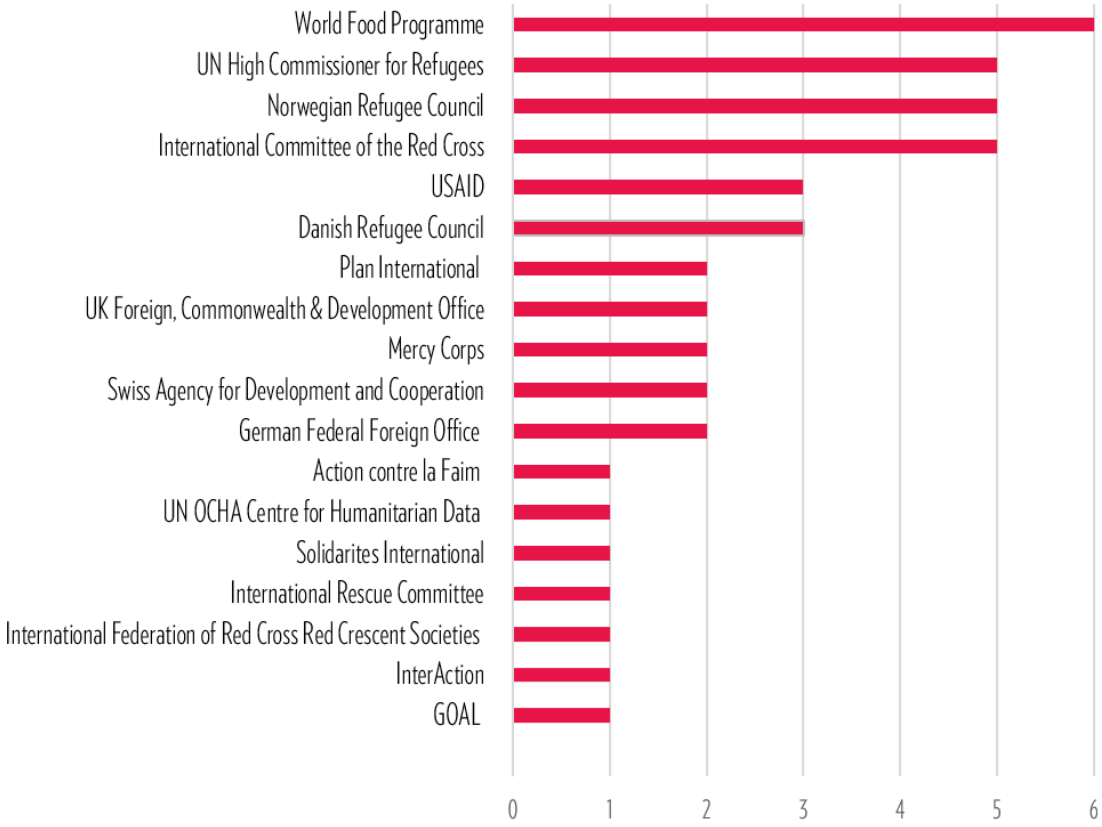
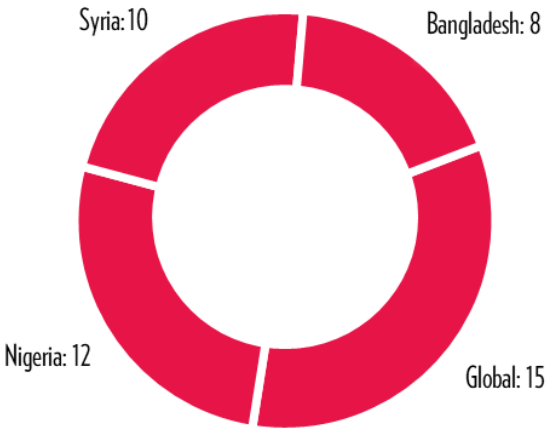


Illustration 2: Number of Interviews by Location



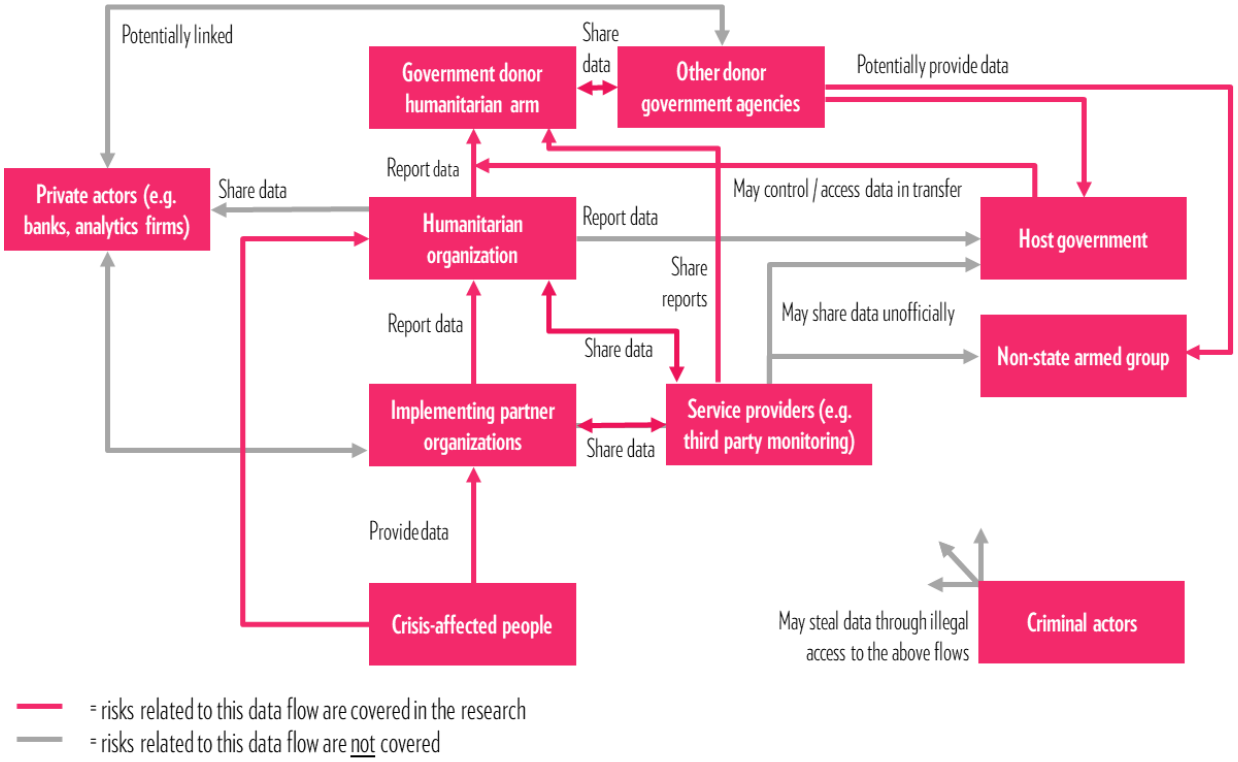
Limitations. The research process faced three important limitations:

- **Interview participation** was limited. The research team defined the participation of six different humanitarian organizations per context as the absolute minimum. The team managed to secure five per context. This limited diversity of humanitarian organizations did not make it possible to draw decisive conclusions about how risks materialize. However, the rich information from participating humanitarian organizations and donors provides a sufficient basis for identifying risks that should be considered when sharing data related to crisis-affected people.
- An important part of the proposed method was to conduct a **data stress test** to evaluate the re-identification risk in available data and donor reports. Unfortunately, the research team did not obtain enough suitable datasets to conduct the planned stress test. This report therefore only summarizes the qualitative interview data. We have indicated in the text below where we expect important insights from such a stress test.
- The **research into donor practices** by the University of Manchester follows a different timeline from this research. It was therefore not possible to take into account the findings and recommendations where the two efforts look at complementary aspects of the same issue.

2 The Complex Chain of Custody of Data Shared With Donors

Data sharing between humanitarian organizations and government donors is part of a broader ecosystem in which different stakeholders collect and share data for operational and reporting purposes in crisis settings. This research only focused on flows of data on crisis-affected people which are ultimately related to government donors (marked in red below).[5] They data flows in scope include, for example, any data on crisis-affected people which a humanitarian actor collects for upward reporting purposes (e.g. to international NGOs, UN organizations or donor governments.) While dataflows without a direct link to government donors (marked in grey below) fall outside the scope of this research, complexities related to the larger humanitarian data ecosystem emerged as important factors. Those are discussed in section 4.

Illustration 3: Data Flows in the Humanitarian System and Research Scope



In addition, this research found four important characteristics of the chain of custody as the data travels from crisis-affected people to government donors. These need to be understood before delving into the discussion of individual risks.

Organizations that collect data from crisis-affected populations are often not directly involved in sharing it with government donors. Especially in countries affected by conflict such as Syria and Nigeria, international humanitarian organizations funded by foreign governments often have limited or no direct access to the crisis-affected populations they seek to assist. Frequently, the data they end up sharing with donors is not collected by their own staff but by implementing

[5] This research focused exclusively on government donors funding humanitarian action abroad. It did not include host governments funding humanitarian action in their own countries, government donors' domestic interactions with humanitarian actors, or development banks.

organizations working on their behalf, typically local or national non-governmental organizations (NGOs) or Red Cross and Red Crescent societies. They obtain personal data of crisis-affected individuals such as names and contact details; they collect information on particularly vulnerable people such as internally displaced persons or refugees, survivors of sexual and gender-based violence, or unaccompanied minors. Implementing organizations are responsible for explaining to data subjects why their data is needed and how it will be processed, managed, and shared. They obtain the consent of data subjects to the use of their data.

The same data often serves multiple purposes, but these purposes are not always known. In addition to optimizing their own operations, humanitarian organizations use data to apply for donor funding; to report to donors on results achieved with their funding; to enhance the donor's overall understanding of a particular crisis and its impact on the most vulnerable; to convince the donor to support a humanitarian organization's advocacy objective; to support the donor's public communication; or to respond to specific requests by donors. In turn, humanitarian organizations say they know little about what donors do with the data once it has been shared. This lack of insight influences the perceptions of risk described in the next section.

Data shared between the organizations and donors consulted is primarily disaggregated group data, with some exceptions and doubts. Most organizations consulted for this report said that they primarily share data disaggregated according to gender, age, location, and – frequently – disability. The level of disaggregation varies in line with the type of activity supported: for example, reporting on a nutrition program will include more detailed data of the children assisted, disaggregated according to relatively narrow age cohorts. Occasionally, agencies provide data related to specific, clearly defined groups of people considered to be particularly vulnerable, such as returnees in parts of Northeast Nigeria.

Most organizations and government donors interviewed stressed that they do not share between them data that directly identifies individual data subjects such as names, phone numbers, or precise information about their location. However, there are exceptions:

- Humanitarian organizations do share data including pictures of particular individuals to support the public communication of donors.
- One donor also said that humanitarian organizations it funds are obliged to indicate suspected cases of individuals trying to obtain more assistance than they are entitled to. They have to report such cases to another agency in its government with the donor agency in copy. Said reports may contain data related to individuals.
- In Bangladesh, one donor requested details of a sample of crisis-affected individuals supported by humanitarian organizations it funds to contact them for post-distribution spot checks. In Syria and Nigeria, some donors interviewed outsource such tasks to Third-Party Monitors who check whether and how the activities they support have reached the intended objectives and whether humanitarian organizations have managed donor funds well. Humanitarian organizations commonly provide contact details of a sample of crisis-affected individuals and of implementing organizations on the ground to Third-Party Monitors, who interview them on behalf of the government donor. While these external service providers report their findings to donors that commissioned their services, the donors consulted said that they never receive data from Third-Party Monitors that would allow them to identify the individuals interviewed.
- There were some examples related to requests to screen individuals considered for assistance, in order to exclude links to organizations designated as terrorist (see counter-terrorism further below).

Formal reporting is only one among several channels. Apart from formal reporting channels, data related to crisis-affected populations is also shared between humanitarian organizations and donor representatives during informal, unregulated contacts and during meetings of humanitarian coordination platforms attended by donors.

The risks discussed below occur at different stages of the data chain of custody. They also need to be viewed in relation to the interests and actions of other stakeholders in the broader data ecosystem, which are discussed in section 4.

3 Country-Level Insights on Risks and How They Materialize

This section presents the reflections by interviewees on two categories of assumed risks: risks that may impact individuals and groups supported by humanitarian organizations, and risks that may affect stakeholders' perceptions of humanitarian organizations, thereby restricting their ability to operate. Interviews only revealed one concrete example of data sharing with donors resulting in harm to crisis-affected people. However, they pointed to clear weaknesses related to each risk that ought to be addressed to prevent harm.

Re-Identification

What is the risk? If not adequately protected, disaggregated data shared with donors could be manipulated to identify individual data subjects or to gain further insights about them. For example, such data may make it possible to discover a new characteristic of an individual, or to add more detail to information about someone's identity. Donors may also end up holding multiple disaggregated datasets related to the same crisis-affected population, which can be linked in a way that reveals new information about individuals or groups.[6]

How does it materialize? Interviewees generally acknowledged that re-identification, especially of vulnerable individuals, for example victims of human rights abuses or crimes such as trafficking, could expose them to significant harm. However, they assumed that the risk this would happen through data shared with donors was minimal, primarily because they felt that the data shared was aggregated at a high-enough level. This remains an unproven assumption, a data stress test would be necessary to evaluate the re-identification risk in available data and donor reports.

Violations of the Rights to Privacy and Data Protection

What is the risk? The rights to privacy and data protection of individuals are defined and protected by laws and regulations. While UN agencies and the International Committee of the Red Cross (ICRC) enjoy privileges and immunities, most international humanitarian actors considered here are NGOs and therefore bound by relevant legislation of the country where they operate, as well as data protection legislation of the country where they are headquartered. If the transfer of data and the way it is subsequently managed by donors violates applicable legislation, the NGOs in question may be legally liable since their responsibility for the data continues to apply even after transferral.

[6] For more information on this risk see: UN OCHA Centre for Humanitarian Data. "Guidance Note Series Data Responsibility in Humanitarian Action, Note #1: statistical disclosure control" n.d.

How does it materialize? Interview partners mentioned one concrete instance where the right to privacy of crisis-affected individuals had been violated because humanitarian organizations shared data with donors. In this case, the family of a woman had to be moved to a different refugee camp in Bangladesh after a donor agency had revealed sensitive details of her situation, including her location, on Twitter. This measure was taken because of concern that authorities in Bangladesh may be able to identify the woman based on the tweet. While this was the only example interviewees mentioned, there is a related risk that should be looked at in more detail. As noted above, humanitarian actors regularly share personal data of crisis-affected individuals with Third-Party Monitors that report to donors. They know little about how these entities process the data, whether it is immediately destroyed after use, or whether it may be shared with third parties such as host governments or commercial companies.[7]

Military and Intelligence Use of Data

What is the risk? A donor involved in an armed conflict or closely allied to a conflict party may use humanitarian data for intelligence or military purposes. Such data may be used for targeted violence against individuals or groups of people, or discrimination or stigmatization by government service providers or businesses. It could also be used to identify the location of services and institutions critical to the survival of vulnerable individuals and groups, such as health clinics or food distribution sites, with a view to harming their operations.

How does it materialize? Several governments who fund humanitarian assistance also provide political and military support to governments and other conflict parties in Nigeria and Syria. Some interviewees therefore expressed concern that the data shared with government donors by humanitarian organizations may end up also being used for military or intelligence purposes, whether intentionally or by accident. However, no interviewee mentioned a concrete example of data shared with government donor agencies being used for military and intelligence purposes, and therefore resulting in harm for crisis-affected individuals and communities. Interviewees pointed to the confidential character of the issue, which implies that they would usually not know whether this happens – or would not be at liberty to disclose it. The fact that humanitarian organizations generally say they do not know much about what donor agencies do with the data shared with them leaves some room for speculation on their part. Some interviewees assumed that the government entities dealing with humanitarian funding would simply not have the power to stop military and intelligence actors from accessing the data they hold. One specific concern mentioned was that military and intelligence agencies could obtain, and share with conflict parties on the ground, data indicating the location of vulnerable individuals and groups or of services and institutions critical to their survival, such as health clinics or food distribution sites, exposing them to the risk of attacks. One humanitarian organization reported that because of this risk they avoided sharing GPS data with donors (and other third parties).

Donor representatives, on the other hand, considered the risk to be limited. Several reported that their agencies have put in place measures to prevent data shared with them from being used for unintended purposes, and that if information is shared with security or military entities of their governments, it never contains data that would permit the identification of vulnerable individuals or groups. However, several donor representatives did not exclude the possibility of data reaching military and intelligence agencies through informal channels, for example when humanitarian and military officials share the same office space. In general though, they assumed that military and

[7] The research conducted by the University of Manchester may provide additional information about the data-processing requirements that donors impose on the Third-Party Monitors they hire.

intelligence agencies had access to their own sources of relevant data and therefore little interest in data held by donor agencies.

Use of Data for Other Non-Humanitarian Objectives

What is the risk? Governments may use data shared by humanitarians for **counter-terrorism activities**, an issue that has sparked some debate, especially when humanitarian organizations have been asked to screen individuals before they receive assistance. There is also a risk that this data is used to manage **migration flows** across borders and along important migration routes, for example across the Sahel. Finally, there is a risk that commercial companies involved in the data chain of custody may market the data of crisis-affected people for **commercial gain**.

How does it materialize? Interview partners reflected on two distinct questions to unpack how the risk of shared data being used for **counter-terrorism activities** could materialize.

First, donors may request data to screen individuals considered for assistance for possible links with groups they consider to be terrorist entities. Two humanitarian organizations reported that they had refused requests from donors to provide data related to individual crisis-affected people to enable such screening.[8, 9] One donor representative reported hearing that other donors had asked humanitarian organizations to provide names of individuals to be assisted to be able to check whether they are involved in terrorist organizations banned by the donor government. The donor representatives consulted for this research, however, said that they never request personal data for this purpose. Several organizations explained that while they do not get requests to screen individuals considered for assistance, data of staff members of local and national partner organizations they work with is shared with donors for screening purposes.

The second question is whether the disaggregated data of the type commonly shared with donors permits the re-identification of individuals, thereby allowing the possibility of them being screened for possible connections to suspected terrorist entities. The research team hopes that a stress test of datasets can be conducted at a later stage to provide some insight in this respect.

Regarding **migration flows**, several humanitarian organizations expressed concern that the data they provide to donors may be instrumentalized by political forces in donor countries advocating for a more restrictive approach towards migrants, as it enables assessment of migration flows. However, none provided a specific example.

The interviews did not produce any concrete example of Third-Party Monitors and auditors commissioned by donors using data related to vulnerable individuals for **commercial purposes**.

---

[8] For more insights on screening dynamics (not involving data sharing), see: The New Humanitarian, 5.11.2019, "Aid workers question USAID counter-terror clause in Nigeria", https://www.thenewhumanitarian.org/news-feature/2019/11/05/USAID-counter-terror-Nigeria-Boko-Haram; and Charny, Joel, "Counter-Terrorism and Humanitarian Action: The Perils of Zero Tolerance", https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/.

[9] Since the 2019 report by The New Humanitarian on USAID's counter-terror clause in USAID grant contracts for Nigeria was widely discussed, it is worth pointing out that the clause reproduced in the article specifies that recipients of USAID funding are not expected to share any individual or personalized data with the US government. See: The New Humanitarian, "Aid workers question USAID counter-terror clause in Nigeria".

Perceptions and Reputational Risks

What is the risk? The transfer of data to donors may also damage the reputation of humanitarian organizations as neutral, independent, and impartial entities. Crisis-affected communities, host governments, or non-state armed groups may perceive actual or suspected data transfers as a sign that humanitarian organizations support non-humanitarian goals. As a result, they may decide to restrict the access of humanitarian organizations to crisis-affected people. In the most extreme cases, misperceptions around the transfer of data to donors may even result in physical harm to humanitarian staff.

If a donor government is perceived to be allied to a party in an armed conflict, any transfer of data may be suspected of being part of an intelligence operation. Even if data were transferred for strictly humanitarian purposes and all the technical safeguards were observed, the mere suspicion of a link with intelligence operations could compromise an organization's reputation. Host governments may also question the neutrality and independence of humanitarian organizations when they suspect that a donor has used data shared by humanitarian actors to criticize or pressure the host government.

How does it materialize? In the three contexts studied, interviewees felt that host governments perceive many humanitarian organizations as acting in the interests of the donor governments that fund them rather than remaining independent, especially if they work in areas controlled by groups opposed to the host government. In Syria, several donor governments support anti-government forces and some have directly intervened in the conflict. Data sharing with donors was not seen as a decisive factor explaining the tension in what was often described as a difficult relationship with authorities in the three countries. Interviewees did, however, point to two examples of suspicions about data sharing contributing to host government mistrust towards humanitarian organizations and the governments that fund them:

- In two instances, organizations said they had been questioned by host governments as to why they were sharing data related to their own citizens with foreign governments but not with the host government.
- One humanitarian organization expressed concern about donor governments using data provided by humanitarian organizations in confidence to criticize host governments for human rights violations. Another organization said that even when donors do not mention the source of their information, host governments may well be able to deduce which humanitarian organization provided relevant data, thereby raising further doubts about their independence.

Several humanitarian organizations interviewed assume that many affected people in Syria also link humanitarian organizations with a European and North American political agenda. Again, data sharing with donors is unlikely to significantly alter these existing critical perceptions. However, they stressed that if it were widely known that the data of conflict-affected people is shared with these donors, it would further increase suspicions of the donors and the organizations they fund. In response, some donors have adopted a zero-branding approach: aid organizations on the ground do not have to use stickers on cars or billboards outside NGO offices to show which donor funds their work. Especially in government-controlled areas of Syria, some humanitarian organizations do not disclose donor governments to national organizations that implement programs on their behalf. This creates a tension between the need to mitigate perception risk, and the ambition for transparency regarding the source of funding to secure the informed consent of crisis-affected people to their data being shared with donors, as is explained in detail below.

4 Factors Complicating Data-Sharing Risks with Donors

The discussion of risk revealed seven factors that either amplify data-sharing risks, or complicate them.

Power Dynamics Around Data Sharing

The HDTI Wilton Park Dialogue drew attention to power dynamics between humanitarian organizations and government donors as a potential amplifier of the risks described above.[10] It highlighted the potential risk of humanitarian organizations sharing more data with donors than required because they believe it will improve their chances of obtaining funding. There are indeed indications that humanitarian organizations report and share data in a way that they believe will help them to secure donor support. However, no interviewee mentioned that this leads them to deliberately collect and share more data than required.

Perceived power relations also play a part in how humanitarian organizations tackle disagreements with donors over data sharing. Do they feel they can refuse donor requests for data because of concerns about the risks described above? To an extent, the answer depends on just how important a specific donor is for a humanitarian organization and on the sensitivity of data requests. Several NGOs said they had little choice but to comply with donor requests because of concerns that they may lose their funding. Some even felt that simply to raise questions about why donors wanted particular data would jeopardize their chances of future support. There was concern that by refusing to share certain data, organizations would signal to donors that they were not prepared to be held accountable for their operations and had "something to hide." Again, the complaint was raised that humanitarian organizations simply do not know why donors need certain data, and therefore struggle to assess the potential risks of sharing it. The pressure is particularly felt by staff handling donor contacts at field level, who may not have the option of referring difficult data requests to headquarters for decisions.

However, this is only one side of the coin. Humanitarian organizations, including some NGOs, shared several examples where they refused specific data requests because of concerns about associated risks or because they did not understand why the donor needed the data. Some organizations have foregone funding by specific donors because of strings attached – those related to data sharing but also to donor demands that organizations screen the individuals they plan to assist. Again, the extent to which an organization depends on a particular donor is important, as is the nature of the data. In some cases a compromise was found whereby donors agreed to fund an activity while reducing their initial request for data.

A lot depends on the quality and depth of the relationship between individuals on both sides. This sense of mutual trust also increases the likelihood of data being shared informally, outside the usual reporting channels. These informal channels can be beneficial for both sides: humanitarians use them to seek donor support, for example during disagreements with host governments, while donors see them as a way to enrich their understanding of humanitarian challenges. However,

[10] See Belina, Jonas et al., "Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Humanitarian Action", Wilton Park 1777V, 2020, https://www.wiltonpark.org.uk/event/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action-wp1777/

interviewees pointed to instances of donors using informal contacts with humanitarian staff to push for data that their organizations were not prepared to share through regular channels. There is a risk that humanitarian staff unaware of the potential risks may end up sharing data in a way that breaches their organization's internal regulations.

The interviews unearthed some details of the power dynamics between Third-Party Monitors commissioned by donors, on the one hand, and implementing humanitarian organizations on the other hand. One interviewee suggested that Syrian NGOs may be inclined to comply with any data request because they feel it may give them an advantage over competitors. This part of the data chain of custody merits being explored more with the stakeholders directly involved.

Multiple Overlapping Regulatory Frameworks

The HDTI Wilton Park Dialogue also highlighted the lack of a regulatory framework governing the sharing of group data across the humanitarian sector as a factor that could amplify the risks discussed above.[11] The lack of a regulatory framework does indeed present the risk that potentially contradictory measures are applied at different stages of the data chain of custody, weakening the protection of data. Both donors and humanitarian organizations interviewed for this research rely on their own internal regulations as a basis for managing data of crisis-affected populations:

- All NGO interviewees were aware of data protection legislation in the country where their organizations were headquartered. Most of them mentioned the European Union's General Data Protection Regulation as the legal framework applicable for processing personal data.
- There was limited awareness of the applicability of national laws or regulations for the processing of personal data in Bangladesh, Nigeria, and Syria. That implies that these organizations also know little about the legal obligations applying to national NGOs that collect data from crisis-affected individuals on their behalf. With the volume of global data flows increasing, countries worldwide have been developing national legislation on data protection.[12] The lack of awareness on the part of NGOs increases the risk that their management of data, and that of their local partners, does not fully comply with applicable law in countries of operation.
- The donor representatives interviewed provided few details of the legal framework their agencies apply to protect data shared with them by humanitarian organizations. Yet this information is key.[13] Humanitarian organizations and their local partners need to be fully informed about the legal framework applied during all stages of the data chain of custody, including after data has been shared with donors, so they can provide comprehensive information to crisis-affected individuals about what happens with their data.

Difficulties With Consent

According to the humanitarian organizations consulted, the consent[14] of crisis-affected people provides an important basis for the processing and sharing of their data. While the specific consent

[11] Belina et al., "Responsible Data Sharing with Donors," p. 4.

[12] World Bank. 2021. "World Development Report 2021: Data for Better Lives." Chapter 6. World Bank, Washington, DC. Accessed via https://wdr2021.worldbank.org/the-report/#download

[13] It may be addressed in more detail in the donor documentation reviewed by the University of Manchester.

[14] This report deliberately draws on the notion of "consent" as communicated to us during the interviews to ensure that it reflects as much as possible interviewees' understanding of this concept. Note that consent is not the only legal basis for holding personal data.

of data subjects is not necessarily required for their personal data to be used as part of aggregate datasets or statistics [15], most humanitarian organizations described it as the main justification they draw on for processing data. Interviewees stressed that they aim for transparency to ensure that crisis-affected individuals are aware of what will happen with their data and therefore seek consent of individuals before using their name, photographs or video footage publicly or before sharing it with donors for their public communication. Some organizations said they would contact individual data subjects to seek their consent again if their data were to be used for a different purpose to that originally intended. And two humanitarian organizations mentioned that they ask for the consent of individual data subjects before sharing their contact details with Third-Party Monitors.

Although clear in theory, it is difficult to ensure in practice that consent is unambiguous, explicit, free and informed. People affected by crisis that rely on humanitarian aid are unlikely to refuse to consent to the use of their data if they fear that will leave them ineligible to receive aid. Furthermore, the organizations collecting the data do not always have all the necessary information to comprehensively inform data subjects about what will happen with their data after it has been shared with donors or with Third-Party Monitors commissioned by donors. In Syria, implementing organizations may not even know which donors fund the activities they are involved in. Keeping the identity of foreign donor governments confidential may make sense to enhance the acceptance of humanitarian actors in conflict zones, but it also means crisis-affected people are not fully informed about what may happen with their data.

Weak Overall Data Security

When data subjects consent to the use of their data they should expect that every entity processing the data will do its utmost to reduce the risks of accidental leaks and intentional hacking. That implies that everyone, starting with staff in direct contact with crisis-affected communities, has to have the know-how and equipment needed to protect their data. No concrete examples were mentioned of data of crisis-affected people being illegally accessed in transfer between humanitarian organizations and donors. However, several interviewees expressed concern about the overall risk of hacking, and doubts about their organization's ability to protect the data entrusted to it. Some interviewees remarked that their organizations do not always store and protect data sufficiently and share it through unsafe channels. One interviewee described data security in their organization as "pre-historic" while another said that staff members regularly store data related to crisis-affected people on their personal computers. This also raises the question of the extent to which the many local organizations involved in the data chain of custody – who often do not get overhead funding that would allow them to invest in infrastructure – are equipped to prevent accidental data leaks.

Limited Staff Sensibility About Data Sharing Risks and Related Policies

Many interviewees expressed serious concerns about the risks of accidental data leaks due to a lack of awareness of the sensitivity of data. Field staff are often not fully aware of data protection policies and specific agreements on data sharing. Interviewees pointed to instances where details of individual protection cases had been discussed in meetings with many organizations present, and suspected that this lack of awareness would also lead to sensitive data being shared with donors. In

A more comprehensive discussion of consent can be found in Kuner, Christopher and Marelli, Massimo, eds., *Handbook on Data Protection in Humanitarian Action*, Second Edition, Geneva: ICRC, 2020, pp. 58

[15] Kuner, Christopher and Marelli, Massimo, eds., *Handbook on Data Protection in Humanitarian Action*, p. 71

one example, field-based staff of an NGO shared personal data of individuals with a UN agency acting as a donor despite an agreement at HQ level that this would not happen.

The Central Role of Host Governments

Host governments are not part of the data chain of custody between humanitarian organizations and donors examined here, but they were frequently mentioned as the primary risk factor. Authorities in the countries concerned are exerting increasing pressure on humanitarian organizations to share data of crisis-affected people. To what extent they have already managed to obtain it remains unclear. However, in some countries, commercial companies supporting humanitarian operations, such as cash or e-voucher distributions, are legally obliged to share data of assisted individuals with host governments. And while no examples were provided of host governments obtaining data through hacking, it was raised as a potential risk – especially in Syria, where some organizations avoid sending data through channels that they believe may be at risk of government interference.

The risk of host governments obtaining data and potentially using it for non-humanitarian purposes was reported as a major source of concern for crisis-affected people in the three countries studied. Organizations active in Syria report that many men who have left government-controlled areas to avoid military conscription are worried that their data will end up with the government. Authorities in Bangladesh reportedly used data of assisted refugees that was accidentally shared with them to select Rohingya refugees to be resettled on Bhasan Char island. In Nigeria, there are concerns that the data of children released after their abduction by non-state armed groups may end up with these groups or with the authorities, thereby exposing them to scrutiny against their will. Organizations and donors also mentioned instances where authorities pressured national staff members to share data related to vulnerable individuals. No concrete examples were mentioned of data shared with donor governments making its way to host governments. However, given that interviewees voiced such strong concerns about host governments, it is important that humanitarian organizations and donor governments put special safeguards in place towards them, especially in countries where governments are parties to armed conflict.

UN Agencies as Donors

Government donors are not the only significant source of funding for international NGOs in the three countries studied. Several NGOs interviewed mentioned that UN agencies are both operational partners and important donors for them. In the former role, NGOs occasionally give these UN agencies access to personal data of individual beneficiaries, including details of individuals considered to be particularly vulnerable. This is the type of data generally not shared with government donors.

NGO observations regarding the role of UN agencies as donors to an extent mirror those related to government donors. There were some complaints that UN agencies use their power as a source of needed funding to exert pressure on their NGO partners to share data. Several interviewees expressed concern that because of the UN's perceived proximity to host governments, UN agencies may be more prepared to share data with them. This report did not set out to examine potential risks of data sharing with UN agencies or any other international organizations acting as donors. However, the fact that many humanitarian interviewees chose to discuss the issue without being prompted to do so indicates that it merits further attention.

5 Conclusion and Recommendations

In the 45 interviews conducted for this research, we found few concrete examples that the sharing of data with donors has exposed crisis-affected individuals and communities to harm or, on its own, impeded the ability of humanitarian organizations to access people in need in the three contexts studied. However, especially in view of the limited scope of the research, there is no room for complacency. Many interviewees pointed out possible risks in other areas of the complex data ecosystem that were not considered in detail by this research. Furthermore, the volume of data shared is steadily increasing. Many humanitarian organizations and donors plan to make more use of the data of crisis-affected people to optimize operations. Meanwhile, other actors also see benefits in getting hold of the data at stake here. Host governments may consider it a strategic asset in political or military conflicts. And private companies involved in humanitarian aid activities may well be interested in exploiting the potential commercial benefits of the data they handle. In light of these developments, humanitarian organizations and government donors should not wait for further proof of harm to individuals before taking action. It is incumbent on humanitarian organizations to mitigate existing risks whenever they process the data of crisis-affected people, and to anticipate and prevent future risks from materializing. To be able to do so, they will need to work with the donors that support them. As a first step, they should cooperate to conduct a stress test of the risk of the re-identification of individual data subjects from disaggregated datasets and reports.

The issues that currently complicate the sharing of data between humanitarian organizations and donors do not appear to be insurmountable. Mutual trust and transparency are key. More information is needed to ensure that humanitarian organizations understand why donors require certain data, what type of data they need, how they process it, and whether and how they share it with other government agencies. They also require more details of how Third-Party Monitors working for donors handle the data entrusted to them. Donors and humanitarian organizations need to ensure that informal data exchanges between their staff do not result in additional risks for data subjects.

The research also shows that humanitarian organizations involved in the data chain of custody face different challenges: there are differences in legal status and hence obligations under data protection legislation; different levels of maturity of data processing and data sharing; different abilities to withstand donor pressure to provide data; and different levels of resilience when faced by host government pressure to release data. To effectively address the risks identified during the HDTI Wilton Park Dialogue means identifying and supporting the weakest links in the data chain of custody. Arguably, the humanitarian organizations participating in the Dialogue were among those best equipped to handle the risks. However, the picture is not complete unless the Dialogue also considers the specific challenges facing local organizations collecting the data of crisis-affected communities.

Recommendations

The recommendations below are to an extent derived from best practices mentioned by individual organizations and donors, meaning some of them are already being implemented. They will eventually have to be harmonized with the recommendations derived from the parallel research looking at donors to ensure that the requirements and ideas of both humanitarian organizations and donors are adequately reflected:

1. Any principles applicable to government donors agreed by the HDTI Wilton Park Dialogue should also **apply to UN agencies** or other international organizations when they act as donors to implementing partners unless the data shared with them is required to allow them to directly deliver assistance to crisis-affected people.

2. Humanitarian organizations and donors should **provide maximum clarity to crisis-affected individuals and communities** about what will happen with their data. Data subjects are entitled to be told who will have access to their data and how it will be protected. This requires both sides to be transparent about why they need certain types of data and how they will process and protect it. The acid test is whether the organizations in touch with vulnerable people are able to give them assurances about what will definitely NOT happen with their data. Data subjects should be given the possibility to exercise their right to object to specific uses of their data or to withdraw their consent to it being used.

3. In situations of armed conflict or other crises presenting significant protection concerns, there should be a default agreement that **no data allowing the identification of crisis-affected individuals or of specific groups exposed to a risk of persecution is shared with donors**. Any exceptions should be regulated through a specific agreement between humanitarian organizations and donors that details for what specific purpose such data needs to be shared.

4. **Any sharing of personal data with Third-Party Monitors commissioned by donors needs to be based on an agreement** that stipulates why data is shared and how it will be processed up to the point of destruction once it has served its purpose. Donors should commit to not obtaining personal data of individuals from Third-Party Monitors. Donors need to inform the humanitarian organizations they fund about what data is shared with Third-Party Monitors.

5. **Any agreement on data sharing needs to be based on an explicit analysis of relevant applicable legal frameworks**. Where the legal obligations of different actors in the data chain of custody differ, this needs to be acknowledged and addressed. In particular, local organizations involved in data collection should receive the necessary support to avoid ending up in situations where they contravene national data protection legislation to fulfil their obligations to partners.

6. Donors and humanitarian organizations should **prioritize the general issue of processing the data of crisis-affected people** and the specific risks associated with sharing data along the chain of custody described in this report. These questions should be covered in audits commissioned by donors so that risks can be identified and mitigated. This may require additional funding.

7. Humanitarian organizations must **ensure that agreements with donors about data sharing are known to their own staff and to implementing organizations** involved in the data chain of custody. They should provide implementing organizations with the know-

how and means needed to apply the agreement on the ground. Donors should be prepared to fund these efforts.

8. Humanitarian organizations should consider reassigning the **final responsibility for decisions on sharing data with donors to a single official or team** in order to maintain a consistent approach to managing risks and to promote organization-wide learning.

9. Humanitarian organizations and donors should develop a **joint approach to host governments and other relevant parties** in situations of armed conflict or in crises presenting significant protection concerns, to agree on clear rules that avoid the data of crisis-affected populations being used for non-humanitarian purposes.

10. **Further research should be conducted into other risks** related to the data chain of custody in particular and the data ecosystem as a whole that were beyond the scope of this assignment. However, we believe that even without further research this report provides sufficient grounds for initiating some of the actions foreseen in recommendations 1. to 9.

Annex 1: Definitions

This report used the definitions of key terms elaborated by the HDTI Wilton Park Dialogue in 2020:[16]

Anonymisation is defined as encompassing techniques that can be used to ensure that datasets containing Personal Data are fully and irreversibly anonymised so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.

Demographically Identifiable Information (DII) as well referred to as **Group Data**: Data points that enable the identification, classification, and tracking of individuals, groups, or multiple groups of individuals by demographically defining factors. These may include ethnicity, gender, age, occupation, and religion. This may also be referred to as Community Identifiable Information that specifically identifies certain groups or communities. [Source: OCHA Centre for Humanitarian Data Glossary: https://centre.humdata.org/glossary/]

Personal Data means any information relating to an identified or identifiable natural person. This covers personally identifiable information (PII) but it is not limited to it. Non-PII, such as cookies, may also be considered personal data since the traces it leaves, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them.

Personally Identifiable Information (PII), also called "direct identifiers", are variables that reveal directly and unambiguously the identity of a respondent, (e.g. names, social identity numbers). [Source: OCHA Centre for Humanitarian Data Glossary: https://centre.humdata.org/glossary/]

Re-identification describes the process of turning allegedly anonymised data back into Personal Data through the use of data matching or similar techniques. If the risk of re-identification is deemed to be reasonably likely, the information should be considered to be Personal Data and subject to all the Data Protection principles. It can be very difficult to assess the risk of re-identification with absolute certainty.

Sensitive data is data that, if disclosed or accessed without proper authorisation, is likely to cause harm to any person, including the source of the data or other identifiable persons or groups, or a negative impact on an organisation's capacity to carry out its activities or on public perceptions of that organisation. [Source: OCHA Data Responsibility Guidelines: https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf]

[16] For the comprehensive glossary (including the ones not used in this report, see Belina, Jonas et al., "Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Humanitarian Action", Wilton Park 1777V, 2020, pp. 8-9. https://www.wiltonpark.org.uk/event/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action-wp1777/

Annex 2: Literature List

Belina, Jonas; Campo, Stuart; Cassard, Vincent; Rogenaes-Panxha, Cecilie; Silverman, Mark and Weicherding, Fanny. "Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Humanitarian Action (WP1777)." Wilton Park. Accessed January 6, 2021. https://www.wiltonpark.org.uk/event/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action-wp1777/.

Berens, Jos. "Data Responsibility in Humanitarian Action: From Principle to Practice WP 1688," 2019

Bouffet, Tina, and Massimo Marelli. "The Price of Virtual Proximity: How Humanitarian Organizations' Digital Trails Can Put People at Risk." Humanitarian Law & Policy Blog, December 7, 2018. https://blogs.icrc.org/law-and-policy/2018/12/07/price-virtual-proximity-how-humanitarian-organizations-digital-trails-put-people-risk/.

Bryant, John; Holloway, Kerry; Lough, Oliver; Willitts-King, Barnaby . "Bridging Humanitarian Digital Divides during Covid-19." ODI. Accessed February 9, 2021. https://www.odi.org/publications/17580-bridging-humanitarian-digital-divides-during-covid-19.

Capotosto, Jill. "The Mosaic Effect: The Revelation Risks of Combining Humanitarian and Social Protection Data." Humanitarian Law & Policy Blog, February 9, 2021. https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/.

Carroll, Joshua. "Violence Stalks UN's Identity Card Scheme in Rohingya Camps." Accessed February 9, 2021. https://www.aljazeera.com/news/2018/11/23/violence-stalks-uns-identity-card-scheme-in-rohingya-camps.

Chaney, Joel. "Counter-Terrorism and Humanitarian Action: The Perils of Zero Tolerance." War on the Rocks, March 20, 2019. https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/.

Cilem, Natalie, and McKenzie, Ann-Marie. "Digital Dignity in Armed Conflict: A Roadmap for Principled Humanitarian Action in the Age of Digital Transformation," 2019.

Corbett, Jessica. "'Breathtaking and Terrifying': UN Food Relief Agency Partners With CIA-Funded Software Firm Palantir." Common Dreams. Accessed February 9, 2021. https://www.commondreams.org/news/2019/02/06/breathtaking-and-terrifying-un-food-relief-agency-partners-cia-funded-software-firm.

Cornish, Lisa. "New Security Concerns Raised for RedRose Digital Payment Systems." Devex, November 28, 2017. https://www.devex.com/news/sponsored/new-security-concerns-raised-for-redrose-digital-payment-systems-91619.

Fast, Larissa, and Lindskov Jacobsen, Katja. "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care." *Disasters, 2019* 43(S2), pages 151-168.

Hayes, Ben, and Marelli, Massimo. "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy." Humanitarian Law & Policy Blog, October 18, 2019. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.

Hosein, Gus, and Nyst, Carly. "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, September 1, 2013. https://doi.org/10.2139/ssrn.2326229.

Htet, Arkar. "Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps." Radio Free Asia. Accessed January 18, 2021. https://www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html.

Inter-Agency Standing Committee. "Operational Guidance - Data Responsibility in Humanitarian Action," 2021. https://interagencystandingcommittee.org/system/files/2021-02/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action-%20February%202021.pdf.

INGO Forum. "Sharing Beneficiary Lists – Guidelines for Humanitarian Actors in Yemen," 2017. https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/annex_5_beneficiary_lists_guidelines_for_humanitarian_actors_final_0.pdf.

Kaurin, Dragana. “Data Protection and Digital Agency for Refugees,” May 15, 2019. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

Koenig, Bryan. “USAID Finalizes Vetting System For Assistance Recipients - Law360.” Accessed February 18, 2021. https://www.law360.com/articles/673070/usaid-finalizes-vetting-system-for-assistance-recipients.

Kuner, Christopher. “Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action.” *EJIL: Talk!* (blog), July 13, 2017. https://www.ejiltalk.org/creating-international-frameworks-for-data-protection-the-icrcbrussels-privacy-hub-handbook-on-data-protection-in-humanitarian-action/.

Kuner, Christopher, and Marelli, Massimo. “Handbook on Data Protection in Humanitarian Action”, Second Edition, 2020

Latonero, Mark. “Opinion | Stop Surveillance Humanitarianism.” *The New York Times*, July 12, 2019. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

Madianou, Mirca. “Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises.” *Social Media + Society* 5, no. 3 (April 1, 2019) https://doi.org/10.1177/2056305119863146.

McDonald, Sean. “Ebola: A Big Data Disaster — The Centre for Internet and Society.” Accessed February 8, 2021. https://cis-india.org/papers/ebola-a-big-data-disaster.

Office of the Inspector General. Internal Audit Report AR/17/17. “WFP Internal Audit of Beneficiary Management,” 2017.

OXFAM, and Engine Room. “Biometrics in the Humanitarian Sector,” 2018. https://policy-practice.oxfam.org/resources/biometrics-in-the-humanitarian-sector-620454/

Privacy International. “Palantir and the UN’s World Food Programme Are Partnering for a Reported $45 Million.” Medium, February 6, 2019. https://medium.com/@privacyint/palantir-and-the-uns-world-food-programme-are-partnering-for-a-reported-45-million-a6a5e811c78a.

———. “Privacy International’s Contribution to Global Virtual Summit on Digital Identity,” 2019.

Privacy International, and ICRC. “The Humanitarian Metadata Problem - Doing No Harm in the Digital Era.” Accessed February 9, 2021. http://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era.

Scarnecchia, Daniel; Raymond, Nathaniel; Greenwood, Faine; Howarth, Caitlin and Poole, Danielle. “A Rights-Based Approach to Information in Humanitarian Assistance.” *PLoS Currents* 9 (September 20, 2017). https://doi.org/10.1371/currents.dis.dd709e442c659e97e2583e0a9986b668.

The Guardian. “Secret Aid Worker: We Don’t Take Data Protection of Vulnerable People Seriously,” June 13, 2017. http://www.theguardian.com/global-development-professionals-network/2017/jun/13/secret-aid-worker-we-dont-take-data-protection-of-vulnerable-people-seriously.

The New Humanitarian. “Aid Agencies Rethink Personal Data as New EU Rules Loom.” The New Humanitarian, January 18, 2018. https://www.thenewhumanitarian.org/analysis/2018/01/18/aid-agencies-rethink-personal-data-new-eu-rules-loom.

———. “Aid Workers Question USAID Counter-Terror Clause in Nigeria.” The New Humanitarian, November 5, 2019. https://www.thenewhumanitarian.org/news-feature/2019/11/05/USAID-counter-terror-Nigeria-Boko-Haram.

———. “Audit Exposes UN Food Agency’s Poor Data-Handling.” The New Humanitarian, January 18, 2018. https://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling.

———. “New UN Deal with Data Mining Firm Palantir Raises Protection Concerns.” The New Humanitarian, February 5, 2019. https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

———. “UN Gives Ultimatum to Yemen Rebels over Reports of Aid Theft.” The New Humanitarian, June 17, 2019. https://www.thenewhumanitarian.org/news/2019/06/17/un-yemen-rebels-aid-theft-biometrics.

The Signal Code. “The Signal Code.” Accessed February 8, 2021. https://signalcode.org/.

Thomas, Elise. “Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN’s Risky Biometric Database.” *Wired UK*, March 12, 2018. https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

Tortoise & Hare Software. “GDPR Principles: Data Minimization,” November 8, 2018. https://tortoiseandharesoftware.com/blog/gdpr-principles-data-minimization/

TU Delft. “Literature Review - TU Delft + IASC Sub-Group on Data Responsibility - Public.” Google Docs. Accessed February 4, 2021. https://docs.google.com/document/d/1znCeT02TEsVz530Dz-RZpvMkyDbRKK6BqaNUgNszOuc/edit?usp=embed_facebook.

UNHCR. “UNHCR Guidance on Protection of Personal Data of Persons of Concern to UNHCR,” 2018.

———. “UNHCR Policy on the Protection of Data of Persons of Concern to UNHCR,” 2015.

UN OCHA Centre for Humanitarian Data. “Data Environment Mapping to Assess the Mosaic Effect.” Accessed February 15, 2021. https://centre.humdata.org/data-environment-mapping-to-assess-the-mosaic-effect/.

———. “Exploring the Mosaic Effect on HDX Datasets.” Accessed February 11, 2021. https://centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/.

———. “Guidance Note Series Data Responsibility in Humanitarian Action, Note #1: statistical disclosure control n.d.

———. “Introducing the Humanitarian Data and Trust Initiative.” Accessed January 6, 2021. https://centre.humdata.org/introducing-the-humanitarian-data-and-trust-initiative/.

———. “Learn How to Conduct a Disclosure Risk Assessment.” Accessed January 26, 2021. https://centre.humdata.org/learn-how-to-conduct-a-disclosure-risk-assessment/.

———. Guidance Note Series Data Responsibility in Humanitarian Action, Note #7, Responsible Data Sharing with Donors, December 2020.

———. “UN OCHA Working Draft Data Responsibility Guidelines,” 2019.

Van Solinge, Delphine. “Digital Risks for Populations in Armed Conflict: Five Key Gaps the Humanitarian Sector Should Address.” Humanitarian Law & Policy Blog, June 12, 2019. https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/.

Weitzberg, Keren. “Gateway or Barrier? The Contested Politics of Humanitarian Biometrics – Datarights Africa.” Accessed January 25, 2021. https://datarightsafrica.org/2021/01/11/gateway-or-barrier-the-contested-politics-of-humanitarian-biometrics/.

Willitts King, Barnaby and Spencer, Alexandra. Humanitarian Policy Group Briefing Note. “Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Principled Humanitarian Action,” December 2020.

———. “The Humanitarian ‘digital divide’.” ODI. Accessed February 9, 2021. https://www.odi.org/publications/16502-humanitarian-digital-divide.

World Bank. 2021. “World Development Report 2021: Data for Better Lives.” https://wdr2021.worldbank.org/the-report/#download