Collaborative Cash Delivery

SAFE PASSAGE: **Options for Data Portability in the Humanitarian Sector**

AN ANALYTICAL REPORT FOR THE CCD NETWORK

Prepared by Paul Currion

COLLABORATIVE CASH DELIVERY (CCD) IS A NETWORK OF 14 OF THE LARGEST INTERNATIONAL NGOS WHO COLLECTIVELY DELIVER OVER $1BN IN LAST MILE CASH AND VOUCHER ASSISTANCE EVERY YEAR.

www.collaborativecash.org

AUTHOR: Paul Currion for the Collaborative Cash Delivery (CCD) Network.

ACKNOWLEDGEMENTS

This research and publication was made possible through a grant being implemented by World Vision International and Germany on behalf of CCD with funding provided by the European Commission's Humanitarian Office (ECHO).

European Union

CONTENTS

INTRODUCTION:

from Policy to Practice

This report draws on a desk review of existing literature, a series of interviews with key experts, and the experience of the author. In it we analyse the current situation, outline the risks that are involved in working in this new space, and present the members of the CCD Network with potential opportunities to engage with the issue of data portability as constructively as possible.

In the last two to three years there has been major progress amongst the larger humanitarian actors in the development of policy guidance relating to data, particularly around data protection and the emerging approach of data responsibility. This guidance has made greater alignment at the global level possible around key issues such as data protection (at least between a certain set of actors).

Meanwhile, outside the humanitarian sector new socio-technological developments have emerged which create the possibility of fundamentally new architectures that might address long-standing coordination problems, and specifically the challenge of data portability. In this report we refer mainly to Data Stewardship and Self Sovereign Identity as examples of these developments, but these two do not exhaust the design landscape.

Practice trails behind policy in our approach to data-related issues. At the operational level, even humanitarian organisations with well-developed policies continue to lack both the capacity to implement these policies consistently, and the capacity to take advantage of new technical developments in a timely manner. As well as the gap between global and operational capacity, it goes without saying that smaller organisations, particularly local actors, who are often the main point of contact for recipients of aid, lack capacity the most.

This raises a question of prioritisation. Given that there are pressing and unresolved issues around e.g. data protection, and given that there are limited resources (particularly staff attention) to deal with these issues, the strategic importance of data portability cannot be assumed – it must be argued for. These organisations are likely to assign different priorities to different topics, and if data portability is not seen as a high priority by a sufficient number of organisations, there will not be the critical mass necessary to move it forward.

This is even more important for data portability than other data-related issues (such as data protection), because by definition it requires multiple participating organisations, not just internal policy and process. Most staff usually do not see the potential of wider ecosystems of data, since their focus is of necessity primarily within their own organisations; and the nature of grant-based projects means that they have limited incentive to engage with wider initiatives, absent either personal interest or a specific mandate from their organisation. As a result most organisations still have a general approach of locking down their data rather than sharing it, especially as the potential harms and potential value of data both become clearer.

Data Portability in Context

“Data portability” is not a standalone issue, but is deeply connected to issues of data governance, digital identity, informed consent, data rights, data protection and so on. This is useful because we can place data portability in this wider context when discussing it, but it also creates two challenges for productive discussions. The first is simply that some of these issues are more urgent than others in the short term (e.g. data protection) which can draw attention from issues which are less urgent but equally important in the longer term, such as data governance.

The second challenge is that these issues and the terms used to discuss them are not always well-defined, or subject to a shared understanding of their definition, which can lead to discussions becoming derailed in unproductive ways. More than one respondent raised questions regarding the foundational point of what constitutes a digital identity, leading us to question whether collecting PII, assembling credentials or providing wallets really means that you are creating a digital ID. A lot of time is spent participating in discussions around the nature and requirements of digital ID which might be better spent on developing, testing and implementing the solutions that meet the needs of the communities we serve.

IT MAY BE MORE APPROPRIATE TO THINK OF THESE AS DIGITAL PROFILES

From an NGO perspective it may be more appropriate to think of these as digital profiles, which can be associated as necessary to a digital ID provided by another institution with a stronger mandate to do so. Of course such an approach does raise the question of how much trust we can have in such institutions, and what the unintended consequences of relying on them might be – as the humanitarian community discovered when the Taliban took over government functions in Afghanistan in 2021. Developing data portability requires understanding the dynamics within each participating institution; unlike other initiatives, it also requires understanding the dynamics between those institutions.

At present the landscape for an inclusive approach to data portability is not encouraging, with the major players heavily invested in systems which are largely not people-centred. Governments historically have tended to adopt a centralising approach to data which privileges their perspective rather than that of the governed; since governments provide the bulk of funding for humanitarian response, their policies incentivise humanitarian organisations to adopt similar approaches.

This is explicit in the field of CVA, for example, in statements such as "donors expect to see cash programmes use, link to or align with local and national mechanisms such as social protection systems".[1] The risks of this are largely glossed over in favour of arguments made on the basis of value-for-money criteria rather than humanitarian principles;[2] such approaches align particularly well with larger organisations such as the UN operational agencies, which must work closely with governments and share a similar bureaucratic logic.

- The Common Cash Statement signed by UNHCR, WFP, UNICEF and OCHA is explicit that the four entities are committed to "harmonize data management through interoperable systems and data sharing agreements".[3] While this statement concerns only cash distribution, it is almost impossible to imagine that the entities will not try to extend this to data relating to other sectors.
- While UNHCR's plan is to create a portable digital identity for all refugees that will be valid on a cross-border basis is admirable, it is paired with a broader ambition to ensure a dominant (if not monopoly) position for their PRIMES system, making PRIMES' CashAssist module the main point of contact for Financial Service Providers, and integrating PRIMES with government social registries.
- WFP is investing in digital transformation, building up government partnerships and entering into agreements with national governments to upgrade their systems. In Iraq, this means digitising the Public Distribution System; while in Ukraine, WFP has directly contracted the private company which provides the Social Action Information system to the government; in both cases reinforcing legacy approaches to data.

[1] Various governments (2019) *Common Donor Approach for humanitarian cash programming.* It is worth mentioning that this document also mentions in passing "beneficiary ownership of their own data".

[2] Humanitarian Outcomes (2020) *Linking Social Protection and Humantarian Cash and Voucher Assistance.* CALP Network, London.

[3] UNHCR (2018) *UN Common Cash Statement (UNCCS) Questions & Answers.* UNHCR, Geneva.

ALTHOUGH PORTABILITY MAY BE POSSIBLE, BENEFICIARY ACCESS TO DATA IN THESE SYSTEMS IS LARGELY SYMBOLIC, AND MEANINGFUL ACCOUNTABILITY IS LARGELY ABSENT

Whether or not these entities can deliver on their ambitions is not relevant; they will continue along these paths and governments will continue to support them. If we accept the framing of data as an asset, however, this evidence suggests that they are seeking to establish what amounts to a cartel for humanitarian data. More worryingly these systems are clearly not based on a beneficiary-focused approach – although portability may be possible, beneficiary access to data in these systems is largely symbolic, and meaningful accountability is largely absent – and may in practice stifle attempts to build alternative approaches.

Outside of the major institutions, there is a fragmented horizontal and vertical landscape of data; there are some thematic areas where sharing is more consistent than others, but even in these cases sharing is incomplete and often not as useful as it could be. The Centre for Humanitarian Data has demonstrated that developing a technical standard (the Humanitarian Exchange Language) and trusted institution for data sharing (the Humanitarian Data Exchange) is possible.[4] However uptake has been slow, many datasets remain incomplete and – crucially for this report – the HDX deals only with open data, and the Terms of Service prohibit sharing any data that includes personally identifiable information.[5]

As part of this landscape we attempted to survey former and current NGO projects that related to data portability in some way, with disappointing results.[6] While there have been a number of projects in this space, they are largely one-off pilots which receive some media coverage at their launch – particularly when new technologies are involved, such as Self Sovereign Identity (which is discussed below) – but which then disappear from public view without even any indication of whether they succeeded or failed (DIGID is a notable exception in this case). As a result there is little coherence or continuity when compared to UN-led projects; the latter, while opaque, usually fit into longer-term strategic plans and/ business processes. For NGOs to match this will require their own multi-year funding.

[4] OCHA (2022) *The State of Humanitarian Open Data 2022:* Assessing Data Availability across Humanitarian Crises. Centre for Humanitarian Data, The Hague.

[5] HDX Terms of Service, https://data.humdata.org/faqs/terms

[6] Due to budget limitations we did not interview NGO representatives; since the CCD Network includes leading NGOs in this space, we assumed that the members would be more aware of NGO projects.

The current landscape of humanitarian data sharing is thus one which primarily serves the interests of institutions over the people that those institutions serve, and it is increasingly clear that these interests may not align. Proponents of the status quo generally rely on arguments based on efficiency rather than rights – particularly under pressure from senior management and institutional donors[7] – but quality of service is not solely a question of efficiency. A people-centred approach to data management presents an alternative to this, and data portability is likely to be a critical part of such an approach.

BOX LESSON

The DICOM Standard, or The Need for Long Views

Similar problems are encountered in other sectors; for example, despite the universal acceptance of the DICOM (Digital Imaging and Communications in Medicine) standard in radiology, in practice there is a breakdown between institutions, including a lack of government leadership.

The reasons for this will be familiar to humanitarian data advocates:

- privacy concerns outweighing portability benefits
- difficulty in associating imaging records with the correct patient
- inadequate regulation and leadership[8]
- proprietary software solutions which are for-profit and silo-ed from other solutions
- lack of clarity regarding who this portability is to benefit, the patient or the physician.

Developing and implementing DICOM has so far taken three decades, in a sector which was ready and willing to adopt it, and the process is not yet complete; but the standard is essential for modern medicine.

[7] See for example Fast, L. (2022) *Data Sharing Between Humanitarian Organisations and Donors: Toward Understanding and Articulating Responsible Practice.* NCHS Paper 06, April. Bergen: Norwegian Centre for Humanitarian Studies.

[8] Avrin, D. *The "P" in HIPAA Stands for Portability*. Journal of Digital Imaging (2022). https://doi.org/10.1007/s10278-022-00645-4

The Demand for Data Portability

Our desk review identified almost no literature on the topic of data portability in humanitarian action, and very limited literature on data portability more widely. It also identified that, in contexts in which data portability is a live issue, such as under the jurisdiction of the EU GDPR, there is little uptake of this right to portability.[9] However three interview respondents asserted that once the concept – and more importantly, the benefits – are explained to people, they become more interested.

While this is based on anecdotal rather than systematic evidence, it does seem plausible; we might assume that demand will increase as new models of data portability are developed and piloted, and as users become aware of the benefits of data portability. Nevertheless most of these models are being developed under market conditions in relatively mature or rapidly maturing digital economies, where the individuals' concerns and priorities are likely to be different to those in crisis situations. We should therefore be cautious about assuming that data portability initiatives developed in more mature digital economies can be exported to other contexts without significant adjustment.

WHAT PROBLEM ARE WE TRYING TO SOLVE, AND WHO SHOULD BE RESPONSIBLE FOR SOLVING THAT PROBLEM?

As with any new technology, we must first ask: what problem are we trying to solve, and who should be responsible for solving that problem? In practical terms most of our answers to this question revolve around access to and continuity of services, but this may not be the most pressing issue for aid recipients. While refugees (for example) may benefit from improved access to work opportunities and payment platforms by being brought onto online platforms, at the same time they face new risks such as fraud; one interviewee explained how refugees in one location now receive multiple phone calls from people claiming to be UNHCR staff, asking for personal information.

[9] Reuss, J. and Bilderbeek, N. (2022) *Data portability in the EU: An obscure data subject right*. The International Association of Privacy Professionals.

These are communities that are already suspicious of online platforms which ask for their personal information – they recognise the need to provide such information for e.g. KYC, but they are subject to surveillance regimes which they wish to minimise. What they are looking for is for UNHCR to establish fraud prevention mechanisms in a similar way that banks have; what they are not asking for is for UNHCR to pass the responsibility for managing their own data down to them as individuals. Data portability – in this case, in the sense of data sovereignty – is the solution to the wrong problem.

Given the large investment required to make data portability a reality, we must therefore also ask: how often does the problem we are trying to solve actually arise, and is data portability required to solve that problem? For example, ensuring continuity of health services may not require full data portability via Self Sovereign Identity (for example), but simply record-sharing based on minimum data standards and contractual obligations under local law. We must be able to justify more innovative approaches, particularly those which place additional responsibilities on aid recipients – as well as additional risks.

Balancing Risk against Opportunity

Interviewees for this research repeatedly emphasised not just the risks of data collection – one comment was that every piece of data should be seen as a potential liability, not an asset, although this was perhaps too pessimistic – but the meta-risk that these would lead to aversive behaviour on the part of humanitarian organisations. Uncertainty about how to mitigate risks, especially in partnership situations, can create what has been termed “reticence risk”, defined by OCHA as “the decision not to share data because of uncertainty”.[10]

[10] Centre for Humanitarian Data (2020). *The State of Open Humanitarian Data*. OCHA, The Hague. See also the Centre’s *Guidance Note #3: Data Responsibility in Public-Private Partnerships* (2020).

BOX LESSON

Covid Passports, or The Need for Mission Focus

One instance of portable data that has received much attention is that of COVID vaccine passports. Health passports in general are relevant to discussions about data portability in the humanitarian space since they are intended to be valid across borders and between institutions. The debate around COVID passports has been vigorous and informative, and cannot be easily summarised; however it is clear that there are valid concerns about both how and why they have been implemented which should inform CCD's data portability work.[11]

1. **Path dependency**, where "once an infrastructure exists, it will make certain future choices more favourable and block others", with no guarantee that the path taken is the best for the data subjects – as is the case with security infrastructure at airports.
2. **Mandate creep**, through which systems which begin as voluntary become mandatory, without the due diligence or democratic oversight we would want, such as with the Aadhaar identity system in India.
3. **System lock-in**, where systems persist even after the need for them is no longer present, which is likely to happen with the health passport system, contributing to the creation of surveillance infrastructure.
4. **Data repurposing**, since by definition the data on a health passport is meant to be seen by multiple parties, but "when the repurposing of highly sensitive medical data is considered, severe privacy risks emerge".
5. **Exclusion risks**, where those who cannot or will not participate in the scheme are disadvantaged, through the transformation of a collective problem into an individual responsibility.

[11] These points were synthesised from: Ada Lovelace Institute (2021). What place should COVID-19 vaccine passports have in society? Ada Lovelace Institute, London, UK; Gstrein, O. (2021). The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment. European Journal of Risk Regulation, 12(2), 370-381; Committee on Legal Affairs and Human Rights (2021). Covid passes or certificates: protection of fundamental rights and legal implications. Council of Europe, Strasbourg, France.

The risks highlighted by the implementation of Covid passports are serious – even before we ask the question of whether they have successfully delivered data portability – and show how data-related issues can become toxic. Reticence risk is not the only reaction to this toxicity; humanitarian organisations might largely ignore these issues and plough ahead with their projects; try to work around them without actually addressing them; or shield themselves from responsibility by outsourcing projects to private sector actors. Such dysfunctional strategies can already be seen in existing projects, but they are not sustainable, nor do they serve the interests of aid recipients.

In an increasingly data-driven world humanitarian organisations cannot avoid data-related issues; but while data portability has risks, it can potentially act as a way to place aid recipients at the centre of discussions of those issues. The risks involved should not be seen as arguments against any form of data portability; instead they should be used as design cues to ensure that any portability mechanism is developed and implemented responsibly.

Designing for Data Portability

Developing data portability is subject to the same challenges as developing any new technical capacity. The successful introduction of any innovation involves three related factors, each of which involves their own challenges:

1. access to new technology (including processes, not just e.g. hardware and software)
2. the policies to enable that technology within the institution
3. the capabilities to translate that policy into practice.

Hardware and software adoption is often determined as much by procurement policy as it is by technology policy. The “best” service to use will lose out to the easiest service to procure, or which fits into existing organisational processes; and new products whose performance is still untested will often lose out to trusted products whose performance is known. One of the reasons why biometrics have successfully entered humanitarian work is that they are relatively easy to procure and introduce into existing processes, and often have a performance record in government processes such as border control.

Working with service providers on building trust and developing procurement packages can reduce these barriers, but requires a large investment that has only a medium-term pay-off. The other pathway to adoption is to Do It Yourself, although this is usually in complement to procuring external services rather than as replacement, and comes with its own challenges. Creating development capacity within the organisation has to be justified in both managerial and budgetary terms, and there is often a struggle to integrate this capacity into the organisation given other priorities.

In the case of data portability, the landscape is changing too quickly and requires specific expertise to work on that is unlikely to be available to NGOs. To address this service providers – particularly start-ups – sometimes embed themselves within a project. However there is frequently a mismatch between the specific use cases identified by humanitarian organisations, and the more general use cases identified by service providers. These two must be aligned correctly since there are security and privacy implications which the service provider is unlikely to be aware of unless they have internalised the logic of the humanitarian organisations – which is an issue of both organisational compliance and culture.

BOX LESSON

Traverse Volunteer Management, or The Need for Mutual Trust

Between 2018-2021 the Australian Red Cross developed Traverse, a data portability project intended to onboard and manage volunteers and staff for rapid local and international mobilisation, including movement between organisations – a perfect test case for data portability, with a widely-acknowledged use case, a well-defined domain and a clearly-identified community. Selecting a decentralised, self-sovereign approach "because it was seen as a way to give users ownership over their own data and control over how credentials are shared", the project successfully developed a web and mobile platform, and established a multi-sector forum of organisations to develop trust standards and an identity ecosystem for the platform. Despite this the project closed after 3 years because they were unable to get other organisations to adopt the technology. The main challenge identified was "the absence of a governance or legal framework for identity and claims" which made it impossible to overcome organisations' lack of trust in credentials issued by other organisations. Building trust thus emerges as the critical requirement in projects that are meant to circumvent the need for trust.[12]

[12] Schoemaker, E. and Womble, M. (forthcoming). *Traverse: An Australian Red Cross case study of the creation, design, and end of a digital identity platform*. Caribou Digital, London.

SSI as New Way of Viewing Data

A rights-based approach to data portability is not possible unless and until there is an adequate data regulatory framework in place which establishes those rights in the legal domain. Without such legal rights, there is limited incentive for commercial service providers to ensure those rights, and no recourse for data subjects if those rights are breached in any way. Data portability therefore cannot be created from the bottom-up, but will be legislated from the top-down with the weight of some institutional authority behind it, based on e.g. rights of refugees. This has two major implications for the humanitarian sector.

First, in jurisdictions where data-related rights are non-existent (or where they exist but lack force for any reason) data portability will be difficult to implement. Humanitarian organisations could in theory implement a self-regulated data portability regime based originally on legal requirements from other jurisdictions (such as the EU GDPR), but even this raises issues. One respondent pointed out that such a "eurocentric" view of data subject rights may not be a good fit with the understanding of such rights by governments even within Europe itself (such as in Ukraine, where these issues are live at the time of research).

THERE IS NO SINGLE APPROACH TO DATA PORTABILITY; IT MUST BE SPECIFIC TO LOCAL CONTEXTS

Second, and following from this, there is no single approach to data portability; it must be specific to local contexts. This will complicate any global approach which might be proposed by humanitarian organisations, particularly in jurisdictions where the legal frameworks around data conflict with humanitarian organisations' own principles. Additional complications may also be encountered in implementing data portability on a cross-border basis between different regulatory frameworks, complicating already-complicated issues such as informed consent and privacy requirements.

This creates challenges for one of the main approaches to data portability that is currently being tested, that of Self Sovereign Identity (SSI) initiatives in which the individual is presumed to have ultimate control over their own personal data. Data portability involves requesting a copy of the data that the individual has provided to a service provider, either in order to hold it themselves or to transit it to another service provider, while the service provider retains their copy of the data. SSI means that the service provider never holds the data, but only requests it from the individual on a case-by-case basis, with the individual's wallet presumed to be the "official" record.

Refugees and other marginal populations, who frequently face problems establishing and managing both their foundational and functional identities, and often require their personal data to travel with them in some way in order to ensure both access to opportunities (e.g. paid employment) and continuity of services (e.g. health care). At the same time many migrants occupy legal grey areas – sometimes incidentally, but sometimes deliberately – in which they attempt to maintain control over how much personal information they share and with whom.

On the face of it SSI appears to address many of these challenges. There have been a small number of pilots testing SSI technology, but it is difficult to analyse how successful they have been due to the large amount of marketing hype that surrounds the technology. The author's personal experience of working with blockchain technology leads to the conclusion that most of these pilots did not actually require blockchain, and the promised benefits of SSI remain on the horizon. More critically we can see that, absent an adequate legal framework, SSI is equally unable to provide a rights-based approach as any other technology.

The best we can say at this point is that SSI is "simultaneously the potential enabler of new modes of empowerment, autonomy and data security for refugees… and a means of maintaining and extending bureaucratic and commercial power."[13] Many of these projects require levels of technology access and expertise which are simply out of reach for many aid recipients, and may create additional risks, such as the basic problem that losing a cryptographic key can mean losing access to all your data forever, with no recourse. Even if these pilots do not in fact deliver all the benefits claimed by their advocates, however, the concept of SSI remains valuable because it offers a new way of thinking about how to manage personal identity and related data.

[13] Cheesman, M. (2022) *Self-Sovereignty for Refugees?* The Contested Horizons of Digital Identity. Geopolitics, 27:1, 134-159.

BOX LESSON

Pan Canadian Trust Framework, or The Need for Due Diligence

The Pan Canadian Trust Framework (PCTF) is designed to meet current and future Canadian digital identity ecosystem innovation needs by verifying trust of services and networks. The PCTF is a Trust Framework which does not provide a technological solution, but enables any given technological solution to be developed, tested and implemented within a coherent framework. Since the participating institutions are all part of the Canadian government, the PCTF has the weight of government mandate behind it, as well as a multi-year strategic commitment. However not all of these institutions cooperate to the same degree – particularly large departments and agencies – and in some cases lack trust in their partner institutions, insisting that they need to continue their own processes. Data portability initiatives will only be as strong as the weakest participating institution, and success will therefore require accountability of all participating institutions. In the PCTF context the critical element has been due diligence carried out by an independent entity in order to ensure oversight and accountability.

Data Stewardship as a Way Forward

“Data stewardship” is a model of data governance in which an intermediary facilitates or holds consent and decision-making on behalf of users, sometimes with a fiduciary responsibility under law. The idea has been developed as an alternative to commercial models of data management, which are largely exploitative and disempowering, and is being explored by a range of institutions as varied as museums, energy suppliers, government agencies, and trades unions. (Note: while some examples of data stewardship are quite long-standing, the formalised concept is relatively recent, and as a result the terminology used to describe data stewardship is still not entirely settled and terms may overlap.)

BOX LESSON

Data Stewardship, or The Need for Appropriate Forms

Data stewardship can be established for a number of purposes, including informing, consulting, involving, collaborating, and empowering participants; there are large scale examples such as the UK Biobank, which has been stewarding biomedical data for 500,000 volunteers since 2006.[14] Data stewardship can also be implemented through different legal forms, including trusts, cooperatives, and corporate/contractual mechanisms,[15] which come under a general category of "data institutions" which are defined as "organisations whose purpose involves stewarding data on behalf of others, often towards public, educational or charitable aims."[16] However these concepts have emerged in the specific context of UK law, and other forms are likely to be possible and necessary in other legal contexts; recent discussions have explored how data stewardship might be applied to situations relating to international migration,[17] smallholder farms in India,[18] and climate change in Peru[19] but these are in relatively early stages.

PERSONAL DATA IS NOT HELD BY OPERATIONAL AGENCIES BUT BY SOME FORM OF THIRD PARTY ORGANISATION

In the context of data portability, data stewardship offers an approach in which personal data is not held by operational agencies but by some form of third party organisation; the data is not ported between organisations, but is accessed by them as required on the basis of consent by the data subject. This potentially overcomes the problem of data being siloed within organisations, but faces a tremendous challenge in terms of persuading those organisations to allow data they have collected to be stored by that third party. Some organisations may see this model as a security risk, a threat to their funding, or a devaluation of their data assets.

[14] Ada Lovelace Institute (2021). *Participatory Data Stewardship: a framework for involving people in the use of data*. Ada Lovelace Institute, London.

[15] Ada Lovelace Institute (2021). *Exploring legal mechanisms for data stewardship*. Ada Lovelace Institute, London.

[16] Open Data Institute (2021). *Designing sustainable data institutions*. Open Data Institute, London.

[17] Kapoor, A., Mohamed, S. and Girish, S. (2022). *Exploring the Potential for Data Stewardship in the Migration Space*. The Dialogue on Tech and Migration, DoT.Mig.

[18] The Global Partnership for Artificial Intelligence (2021). *Enabling Data Sharing for Social Benefit Through Data Trusts: Data Trusts in Climate: An interim report*. GPAI, Paris.

[19] Centre for Open Data Enterprise (2022). *Envisioning a Climate Change Data Ecosystem. Partnership in Statistics for Development in the 21st Century*.

Data stewardship takes an ethical-legal approach, building institutions within specific (usually national) legal frameworks and assigning fiduciary responsibilities under those frameworks. This contrasts with the policy-practice approach which the humanitarian sector takes to data governance, which relies on developing internal guidance which is then incorporated into business processes and staff responsibilities. Policy-practice is easier to understand and implement for humanitarian organisations, since it fits into their existing understanding of how organisations work, while ethical-legal approaches are often difficult to parse – how does data stewardship fit with our current (often under-developed) idea of rights-based approach, and what would a legally watertight mechanism for data stewardship look like across entities with large variations in legal mandates and exemptions?

However the concept of data stewardship fits better with a rights-based approach, and also has more participatory potential than extant data responsibility approaches. There are multiple models for data stewardship, not just within organisations recognising their responsibility for their data, but also for third parties such as data trusts or data cooperatives. This suggests that some implementations of the concept could fit within humanitarian action, but still the various models of data stewardship described in other sectors do not map easily to the humanitarian sector, since they appear to work best for clearly-defined populations supported by accountable institutions in relatively stable situations.

Data stewardship is clearly suited to sector verticals, such as research which involves volunteer participants, research organisations, and regulatory bodies, all within the health sector; it is harder to conceive how this would work across the multiple sectors involved in humanitarian response. Stewardship also works for geographic horizontals, such as clearly-defined communities of shared interest, such as gig workers; it is harder to conceive of how this type of governance would work for a mixture of different communities with different interests, such as refugee and host communities. It is also worth noting that most data stewardship pilots so far have been outside the Global South; while there is increasing interest in countries where regulatory frameworks may be less well-developed, these are still relatively rare and it is still too early to draw any lessons.[20]

[20] The Data Economy Lab (https://thedataeconomylab.com/) is building a global database of data stewardship initiatives; interest can also be seen in policy papers such as Borokini F. & Saturday B. (2021). *Exploring the Future of Data Governance in Africa: Data Stewardship, Collaboratives, Trusts and More*. Pollicy, Kampala.

Finally, it is clear that data stewards must operate in a single legal jurisdiction within which their legal and fiduciary responsibilities are clearly defined and successfully enforced; it is hard to see what that would look like for international organisations working in multiple countries, sometimes specifically in cross-border operations.

What would data stewardship look like, for example, for a Malaysian NGO working cross-border between Pakistan and Afghanistan in partnership with UNHCR, when the Taliban took power in 2021?

Humanitarian organisations are unlikely to be good data stewards themselves due to a) competing priorities and b) limited capacity. Any kind of data steward arrangement for the humanitarian sector would be likely to require the identification or (more likely) creation of a third party to act as steward. Given the internal politics of the sector, there is a good chance that the mandate for this would be granted to an existing mandate organisation such as UNHCR, which has a stronger legal foundation on which to take on such responsibility. As discussed elsewhere in this report, however, such mandate organisations have tended to take an approach which does not lend itself to stewardship.

Despite this we believe that data stewardship – and particularly participatory data stewardship – could be successful in particular contexts. While many humanitarian emergencies have a period of sudden onset of rapid change, many have a long tail of either sustained need or slow recovery in which data stewardship might make sense. It also fits within discussions about increased localisation and accountability, which should make it easier to gain support. Applying the concept within defined communities for specific sectors in appropriate jurisdictions should be explored as part of the humanitarian community's overall approach to data management.

What can CCD do?

In order to decide which approach to take, the CCD Network members need to answer two key questions: first, how will this approach to portability improve the lives of aid recipients; and second, what value will the CCD Network bring if they take that approach (as opposed to, for example, a commercial vendor)?

Advocacy

THE CCD NETWORK'S MOST CONSTRUCTIVE, REALISTIC ROLE MAY BE TO ACT AS A COUNTERVAILING FORCE WHICH LOBBIES FOR A PEOPLE-CENTRED APPROACH

It became clear during the research that it is extremely unlikely that any alternative protocol to the centralised systems pursued by UN agencies will not really be viable in the face of the UN's stronger mandates, larger scale, greater resources, and – perhaps most importantly – first mover advantage. The CCD Network's most constructive and realistic role may be to act as a countervailing force which lobbies for a people-centred approach, particularly with donor and host governments, in which UN systems would form an integral part – but only a part of a wider system in which data sharing in general is more open and systematic.

The CCD Network can therefore play a crucial role in re-framing data management discussions to place the people that we work for at the centre. The first step is to develop an adequate framing for data portability discussions, for which we identify two potential components:

1. A functional definition which covers: what is data portability when described in terms of specific use cases, how do we measure the success of such use cases, and how would we measure progress towards the goal based on those successes?
2. A simple narrative that describes: why and how data portability can benefit aid recipients; how it might enable service providers to improve their services; and how this might benefit the humanitarian sector in general through improved efficiency?

CCD Network members will need to align around a shared vision as early as possible, preferably based on limited and pragmatic expectations. We identify two areas which need to be approached with caution:

1. Questions are emerging around how to interact with state-run social protection systems,[21] a complicated area where even UN agencies are cautious, despite their closer working relationships with governments. (WFP has apparently decided that data from its SCOPE beneficiary identity and management system will not be transferred to governments due to consent issues.) CCD Network members should address this topic collectively as well as individually; their position will obviously be different to UN agencies which are required to work directly with governments.

2. A people-centred approach may be intended to empower those people but may in practice “responsibilise” them. In such cases responsibility for key functions – i.e. managing personal data – is pushed onto those with less power, without creating the concomitant accountability on the part of service providers. These functions can be delegated by individuals to a stewarding organisation, thus alleviating some of the responsibility and mitigating the associated risks; however in a time when localisation and decolonisation are critical, such an approach may appear overly paternalistic. Striking the right balance in both implementation and messaging is critical.

In terms of positive messaging CCD members might promote the following:

- different use cases require different solutions, i.e. what works in a cash context may not work in a health context;
- no single organisation – or group of organisations – will ever be able to meet all humanitarian needs, and should not have a monopoly on recipient data;
- development of these solutions is a long-term project that requires long-term investment, or what is referred to as ‘patient capital’;
- metrics for success should be built on the perspectives of aid recipients as much as the requirements of aid organisations;
- that quality of service from this perspective is not just about efficiency, but also about accessibility and dignity, which may require compromise;
- successful portability mechanisms need to be inclusive, particularly for local governmental and non-governmental organisations.

[21] Raftree, L. (2021). *CALP Case Study: Responsible Data Sharing with Governments*. CALP, London.

The governments that could mandate data portability are either donor governments – who may insist on it as an efficiency measure – or host governments, who may implement regulatory frameworks that make data portability either a possibility or an obligation.

- In the case of donor governments, the CCD Network should emphasise evidence from government initiatives showing that developing data portability regimes is a multi-year process that requires the development of institutional infrastructure to support it, and that this process will require multi-year funding in order to succeed.
- In the case of host governments, CCD Network members should join existing advocacy campaigns at the national level to improve the regulation of technology to ensure that government agencies and private companies deal with personal data responsibly, regardless of whether that data belongs to aid recipients or not.

Research

The second role that the CCD Network can play is to continue to conduct research into data portability and related issues, while at the same time raising awareness about the topic.

Pure

A detailed analysis of which data could be made portable and for what purposes on a sector-by-sector basis would be a useful starting point for development of data portability. Data portability can be disaggregated into specific domains, including: vulnerability and other assessments; work permits and employment history; personal and family health records; education credentials and course credits; records of receipt of cash benefits.

Such disaggregation would make it easier to make the functionality argument for data portability, and make it easier to draw on experiences from other relevant sectors or jurisdictions that have already attempted or implemented portability – whether at the general level (as with GDPR in the EU) or in specific sectors (such as the Health Insurance Portability and Accountability Act in the US).

A larger project might include mapping key dimensions from across different jurisdictions to better understand the data lifecycle across different operating environments, and particularly under different data protection regimes.

Although CCD members will be familiar with the data sources which they use for decision-making, new data sources continue to appear in rapidly changing environments, and how that data is used is poorly understood. While this is likely to be beyond the capability of the CCD Network itself, it may present a partnership opportunity with other organisations (inter-governmental or non-governmental) looking at these issues.

Applied

We have stated above that there is little evidence of demand for data portability even in more digitally sophisticated economies with strong regulatory frameworks. Since there is therefore little evidence of a public appetite for data portability, the argument for data portability is usually made on an a priori basis. A stronger evidence base is needed to provide incentives for organisations to invest in it. In addition the framing of "data portability" must be improved, not just to pitch the idea to recipients of aid, but also to embed it within organisations (through internal advocacy) and to build a culture in which data portability is not just a possibility, but a given.

BUILD A CULTURE IN WHICH DATA PORTABILITY IS NOT JUST A POSSIBILITY, BUT A GIVEN

Some interview respondents claim that once the potential benefits of data portability are explained to aid recipients – such as being able to access other services and avoiding repeated registration with those service providers – the level of interest in updating and accessing their data increases. CCD members could therefore conduct surveys of user interest in and readiness for data portability. These would help to build the evidence base in favour of data portability projects, as well as centering the experience of aid recipients in any such projects.

Such surveys could also form part of awareness-raising work amongst aid recipients, both to shape the development of these projects and to generate the demand for them that is necessary to create momentum. Educating potential users may be critical for the success of data portability, but awareness-raising should be kept as simple as possible, and grounded in the practical implications for aid recipients.

Design

The third role that the CCD Network can play is to act as a design commissioner and sandbox for data portability.

Although the CCD Network should maintain a technology-agnostic approach, it can encourage its members to develop and test the processes that need to happen in order for technology to be adopted within and between organisations: for example, collaborative contracting processes, contract language alignment, improved data sharing agreements, and so on. The CCD could also develop resources that can help CCD members – and other humanitarian actors – to work more responsibly in this space, such as with risk assessment tools to identify digital risks faced by aid recipients. Many of these harms go beyond such geographically-specific frameworks as GDPR; each community will have its own risk profile, since they exist in different rights frameworks, and experience harms in different ways.

THE CCD NETWORK SHOULD MAINTAIN A TECHNOLOGY-AGNOSTIC APPROACH

Other common tools can be developed, such as a diagnostic tool to help organisations to assess their readiness and/or competence to engage, and help them to understand where they need to invest in order to achieve readiness or maintain competence. The development of metrics for data portability is complicated; a metric cannot be just technical (i.e. the implementation of a standard API) or quantitative (i.e. the number of organisations able to port data between themselves) but qualitative – that is, it must include the experiences of users, both positive and negative. Humanitarian organisations already struggle to measure this in general and no single organisation can provide it, since by definition portability is multi-organisational; some form of centralised monitoring body would be needed to aggregate recipient views, which may also be covered by the research.

The research suggests that the approach most likely to succeed is to develop a general framework that can contain specific standards or products, rather than to develop the standards and products themselves. An unofficial PII extension to the Humanitarian eXchange Language or a referral platform between NGOs in a specific location could both fit into such a framework, where the focus would be on ensuring quality, extensibility and interoperability. Such a flexible approach is less threatening to individual corporate interests, can be made relatively future-proof, and can be locally contextualised so that implementation will be different in different locations.

To outline what such an approach might look like, the PCTF (described earlier in the report) emphasises a defined range of “trusted processes” rather than the technology used to implement those processes – processes which can be combined to deliver different government functions – leaving technology decisions to individual parts of federal and provincial government. As well as the PCTF, other examples of framework approaches include techno-political initiatives such as Govstack (https://www.govstack.global/), a framework for software development in support of e-government, and MOSIP (https://www.mosip.io), an open source platform for building foundational national IDs.

The existing model that seems to hold the most promise for a people-centred approach is data stewardship. There are a variety of forms of data stewardship currently being explored in different sectors; although it is likely that humanitarian data stewardship will have its own unique features, there is an emerging community which could support its development. Data stewardship models are not reliant on standards and can incorporate different products – such as SSI, although we did not find specific examples of this – but importantly are completely reliant on the involvement of the data subjects in one form or another. This opens up the possibility for the CCD Network to introduce an approach far more coherent with the principles often expressed by the sector than existing systems.

SAFE PASSAGE:

Options for Data Portability in the Humanitarian Sector

Collaborative Cash Delivery

www.collaborativecash.org