Collaborative Cash Delivery

Data Portability and Digital Identity in Humanitarian Aid: A DESK REVIEW

Author: Paul Currion for the COLLABORATIVE CASH DELIVERY (CCD) NETWORK
with inputs from Aaron Martin, Emrys Schoemaker and Keren Weitzberg

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 with inputs from Aaron Martin, Emrys Schoemaker and Keren Weitzberg.

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

BACKGROUND

This desk review provides a landscape of the state of policy and technology with respect to data portability and digital identity in the humanitarian sector. It introduces key concepts and raises critical questions for the sector as it considers new approaches to beneficiary-centric digital identity based on the principle of data portability. This document is accompanied by a separate analytical report prepared by Paul Currion which builds on the desk review with a targeted commentary and tailored guidance meant for CCD Network members within the framework of its ECHO-supported project on data portability.

Key takeaways

- Data portability can be understood across different dimensions, including technical aspects, legal rights, and humanitarian opportunities. These dimensions are complementary and need to be understood holistically during program design and implementation.
- Data portability should be distinguished conceptually from interoperability. While related, they are not synonymous. Critically, data portability and interoperability will empower beneficiaries differently in terms of accessing and managing their data.
- Successfully developing and implementing data portability and interoperability mechanisms in the humanitarian sector will require political will, institutional commitments, policy decisions, and, subsequently, technological capabilities that current forms of humanitarian data sharing do not. Traditional humanitarian data sharing will not disappear even if strong data portability and interoperability mechanisms are achieved.
- While centralized, federated and decentralized digital identity models can all in theory be built to facilitate data portability and interoperability, the self-sovereign identity movement has explicitly endorsed principles for both.
- Beyond digital identity, the humanitarian sector's experience with cash-based assistance should inform any strategy for data portability and system interoperability. Recent commitments by donors are meant to bolster interoperability in humanitarian cash programming but the role for data portability in cash strategies is generally unremarked.
- A paucity of empirical research to date on beneficiary demand for data portability represents an opportunity for targeted learning activities by the CCD Network and other interested stakeholders.
- The current limited evidence from the humanitarian sector's experiences with data portability and interoperability is mixed regarding both the demonstrated benefits to beneficiaries and the possibilities for interoperability across systems based on different protocols and algorithms.

What do we mean by data portability?

For the purposes of this desk review, we can understand data portability across three dimensions:

On a **technical level**, data portability generally describes **models and standards aimed at facilitating requests for data to be transferred to a person or third party**—including competing services or platforms. These models and standards usually focus on personal data, but not exclusively so. These approaches provide a technical means to free data from closed platforms or 'walled gardens', which may be seen as user-unfriendly or anti-competitive. In the area of digital identity specifically, which is discussed in more depth later in this report, portability models seek to make it easier for people to exercise control over their identities by facilitating the release and transfer of identity or profile data.

DATA PORTABILITY GENERALLY DESCRIBES MODELS AND STANDARDS AIMED AT FACILITATING REQUESTS FOR DATA TO BE TRANSFERRED TO A PERSON OR THIRD PARTY

Porting data efficiently from one service/platform to another requires common technical formats[1] and interoperability commitments. In many cases, because service providers are competitors, data portability objectives may also necessitate a legal basis to drive implementation and compliance.

It is also worth distinguishing data portability from the notion of self-managed data, which is core to self-sovereign identity (SSI) models. As discussed above, data portability is about requesting a copy of the data that an 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 generally retains their copy of the data. On the other hand, SSI models imply that the service provider might never hold the data, but only requests it on a case-by-case basis, with the individual's wallet or similar technology presumably being the 'official' version of the data. The choice between these two versions of portable data should be carefully taken during the design stage based on an assessment of user needs and the application context.

1 See chapter 3 on technical aspects of data portability and data sharing: https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/

As a **legal right**, specifically Article 20 of the EU General Data Protection Regulation (GDPR), data portability gives data subjects **"the right to receive the personal data concerning him or her, which he or she has provided to a controller** [i.e. an organization which has requested or required that data], **in a structured, commonly used and machine-readable format**" and "**the right to transmit those data to another controller without hindrance** from the controller to which the personal data have been provided."[2]

Despite the fact that this right has been less well exercised in the EU compared to more established data subject rights (such as the right to access one's personal data),[3] other jurisdictions are following suit in advancing data portability provisions in modernized data protection frameworks.[4] These emergent legal rights to data portability are interesting, among other reasons, because they engage with different aspects of technology like 'machine readability' while attempting to remain technologically neutral.[5]

Relevant case law on data portability is very limited in the EU.[6] Although the European Commission's own evaluation of GDPR found low appetite among the public for data portability,[7] new legislative instruments like the Data Act aim to give people even more control over their data through a **reinforced** data portability right: copying or transferring data easily from across different services, where the data is generated through smart objects, machines, and devices.[8]

At a sectoral level, for example in the area of financial services, open banking initiatives like the EU's revised Payment Services Directive (PSD2) are also facilitating the freeing up of data by enabling third-party providers to access a customer's payment account information upon their request in order to provide payment initiation or account information services.[9] Other sectors, like the energy sector, are following suit.

2 https://ec.europa.eu/newsroom/article29/items/611233
3 https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/
4 For example, Kenya's new data protection law includes a right to data portability. See Section 38: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019#sec_38
5 https://dl.acm.org/doi/10.1145/3267305.3274152
6 In the Netherlands, for example, case law has largely focused on what is meant by a 'machine-readable' file format https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/
7 https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/
8 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_1114
9 Inge Graef and colleagues analyze the 'spillover' effects of these sector-based data portability dynamics https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/9.1/EuCML2020002

As a **humanitarian** priority, data portability could provide **a means to increase aid beneficiary autonomy by giving them more control over their data**, precisely by making it easier for people to transfer their data to them personally or another humanitarian organization upon request, or perhaps through an even stronger version of data portability, i.e. self-managed data, shaped by SSI ideals.

However, a meaningful discussion on the possibilities for data portability in the humanitarian sector requires that we first understand existing policy commitments and everyday practice as regards the transfer of data in the sector, the extent to which humanitarian organizations' technical capacities could facilitate (more sophisticated forms of) beneficiary control and data portability, and the extent to which data portability is a priority for beneficiaries themselves. We also need to consider how data portability could address concerns about monopolization, competition, and vendor lock-in with respect to humanitarian technology in general and in the humanitarian digital identity space specifically.

KEY RESOURCES on data portability

- A 2018 blog post by the UNHCR on "bridging the identity divide" ponders whether portable, user-centric identity management could create value for refugees in the absence of international standards that ensure cross-border recognition of self-controlled digital identities.
- A 2022 blog post by the International Association of Privacy Professionals (IAPP) discusses the "obscure" right to data portability in the EU context, while reporting that most EU countries report no relevant supervisory enforcement or case law.
- Inge Graef and colleagues (2020) explore the "uneasy relationship" between the GDPR's right to data portability and different sector-specific data access regimes. They note that, in the absence of appropriate technical infrastructures, data portability measures can be "expensive, slow and cumbersome".

And interoperability?

While the two terms are often used interchangeably, it is important to distinguish 'data portability' from 'interoperability'. Interoperability can be understood as the ability of different service providers to work together and communicate data with one another. Such interconnections can also allow users to combine multiple services in complementary ways.[10] Digital platforms use software intermediaries like application programming interfaces (APIs) to enable system interoperability, and security is an important consideration in these exchanges. While data portability and interoperability are distinct concepts, they can overlap. For instance, continuous or real-time data portability requires a degree of interoperability for systems to be able to communicate with one another to share data on a regular basis.[11]

INTEROPERABILITY CAN BE UNDERSTOOD AS THE ABILITY OF DIFFERENT SERVICE PROVIDERS TO WORK TOGETHER AND COMMUNICATE DATA WITH ONE ANOTHER

Technology policy expert Ian Brown describes a sliding scale of interoperability obligations that could be imposed on platforms by regulators or other authorities.[12] He distinguishes between five levels of these obligations:

1. **Platform-permissioned vertical interoperability**, whereby users connect their accounts, identities or profiles on complementary services from a third party to a platform, with its express permission.
2. **Open vertical interoperability**, whereby users connect their accounts, identities or profiles on complementary services from a third party to a platform, **without** the platform's permission. This could enable **real-time data portability**.
3. **Public horizontal interaction**, where no external user authorization is required.
4. **Private horizontal interaction**, where external user authorization is required.
5. **Seamless horizontal interoperability**, whereby users have the ability to use directly competing services.

10 https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm
11 https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm
12 https://www.ianbrown.tech/2020/10/26/the-technical-components-of-interoperability-as-a-tool-for-competition-regulation/

In a 2021 policy paper,[13] the Organisation for Economic Cooperation and Development (OECD) elucidates the interrelated dynamics of data portability, interoperability and competition specifically. While acknowledging the limited implementation of data portability and interoperability measures on many digital platforms (not limited to digital identity), the OECD points to a few emergent lessons that can inform a discussion on the possibilities for data portability and interoperability in humanitarian digital identity initiatives:

- **Clear, coherent objectives matter** – According to the OECD, data portability and interoperability measures implemented for reasons other than promoting competition, i.e. for the purposes of strengthening data protection, "may not have pro-competitive impacts unless designed with market dynamics in mind". It is worth bearing this lesson in mind when designing data portability models for the humanitarian sector, and in particular to reflect on what constitutes relevant market dynamics in the delivery of aid.
- **Beware of unintended consequences** – Data portability and interoperability measures can have unintended consequences if they create new barriers to entry or entrench incumbent technologies. Careful thought must go into system design and the choice of technologies (both back-end and front-end).
- **Oversight is key to effective implementation** – Oversight by a regulatory body or independent third party may be needed to set standards and adjudicate disputes among stakeholders. It is unclear at present which existing body or entity within the humanitarian sector could fulfill this role. For the UN system, OCHA is an obvious starting point but for the broader humanitarian system including non-UN agencies, there is no clear authority in this space.

13 https://www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm

KEY RESOURCES on interoperability

- An 2020 article by Chris Riley of Mozilla provides an introduction to how interoperability fits within the existing landscape for competition regulation and explains how key interoperability concepts apply to digital platforms.
- The aforementioned 2021 OECD report on data portability, interoperability and digital platform competition provides a rich analysis of the existing evidence in this space. While not specific to digital identity or humanitarian applications, it does elucidate some emergent policy considerations. The report is accompanied by a series of expert videos, which may also be of interest.
- With an eye on humanitarian developments, in an academic paper Shirin Madon and Emrys Schoemaker analyze how the opening up on UNHCR's digital identity platform might facilitate new forms of data interoperability and data sharing.

Isn't this just data sharing in everyday humanitarian practice?

Situating the discussion on data portability and interoperability in the humanitarian context requires that we look at how data is currently shared and transferred by various stakeholders. This is a complex topic that is the subject of different policy debates, governance frameworks, and research initiatives. For our purposes and as background, we can distinguish between four different kinds of humanitarian data sharing relationships.

Data sharing between humanitarian organizations: Humanitarian organizations regularly share different kinds of data among themselves. For example, UNHCR, WFP and UNICEF have collectively agreed to share data (both personal and non-personal) for humanitarian cash programming purposes.[14] These arrangements are generally governed by data sharing agreements but the technical details involved are normally unremarked in these documents. It is possible to glean some details from public reporting, for example in the case of the trilateral agreement between UNHCR, WFP and UNICEF, requirements for a data sharing portal have been established by a Data Interoperability Task Team to facilitate data exchange between the agencies' systems.[15]

14 https://www.unhcr.org/602e24a94.pdf
15 https://www.unhcr.org/615c44634.pdf

At the global level, the Humanitarian Data Exchange[16] based on the Humanitarian Exchange Language[17] has offered the most systematic approach to data sharing. It demonstrates the possibility of developing a technical standard and trusted institution, although uptake has been limited and the type of data it holds is operational rather than personal.

Looking outside the UN system, the Collaborative Cash Delivery Network has established its own Data Sharing Working Group to facilitate data sharing among its members. It has agreed to focus its efforts on the creation of unique identifiers to support case referrals as well as de-duplication,[18] the development of models and standards that are technology-agnostic, privacy-friendly and beneficiary-centric, as well as the development of practical tools such as guidance and templates for data sharing agreements.[19]

HUMANITARIAN ORGANIZATIONS ARE OFTEN LEGALLY REQUIRED TO SHARE CERTAIN KINDS OF DATA WITH GOVERNMENT AUTHORITIES IN COUNTRIES IN WHICH THEY OPERATE.

Data sharing between humanitarian organizations and government authorities: Humanitarian organizations are often legally required to share certain kinds of data with government authorities in countries in which they operate. For international organizations (e.g. UN humanitarian agencies), the rules governing these data exchanges will form a part of the Host Country Agreements that outline the conditions for these agencies to operate. There is often a lack of transparency about what the terms and conditions of these agreements cover,[20] which has led to occasional controversies related to data sharing.[21] Among the Host Country Agreements that are publicly available, data sharing provisions—especially with security services—are commonplace.[22]

16 https://data.humdata.org
17 https://hxlstandard.org/
18 De-duplication refers to methods for eliminating redundant data in datasets
19 https://www.collaborativecash.org/data-sharing-working-group
20 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179
21 See, for example: https://www.accessnow.org/unhcr-wfp-iris-scan/
22 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179

For humanitarian organizations lacking legal privileges and immunities, domestic laws will specify any mandates or requirements to share data with government authorities. These laws may not sufficiently protect the data and rights of beneficiaries, e.g. in terms of providing robust personal data protection, and thus may present additional challenges for humanitarian organizations that are legally required to share data. These are thorny problems that do not go away in a scenario in which widespread data portability is achieved. In fact, as noted above data portability has been advanced legally largely through relevant mandates in data protection legislation, so the lack of a modernized data protection framework in a given jurisdiction is not only a challenge for governing data sharing, it is also an impediment to facilitating new forms of data portability.

Data sharing between humanitarian organizations and private sector actors: Humanitarian organizations may share data with commercial partners for different reasons, including expectedly for the purposes of delivering humanitarian assistance (e.g. cash aid, connectivity provision, etc.). In these situations, contracts will often specify the terms of the data to be collected and shared between humanitarian and commercial actors, and for which purposes. These contractual requirements may be shaped by larger legal and regulatory mandates, for example AML/CFT rules that specify what data about banking customers needs to be collected and shared for due diligence reasons, or SIM registration laws that require identity data about mobile users to be recorded and in some cases shared with regulators. An outstanding question, which is not sufficiently addressed in the literature, is how data portability approaches will interface with these forms of legally mandated data collection and sharing, which are increasingly relevant to digitally enabled humanitarian programming.

As this desk review was being prepared, a new working paper on data sharing and 'third-party monitoring' in humanitarian response was published by the Humanitarian Policy Group.[23] The report explores risks and mitigation efforts around data sharing for the humanitarian sector with a focus on the data sharing relationships involved in third-party monitoring, i.e. the process of an independent entity assessing the outputs and performance of humanitarian programs. These assessments are often undertaken by external, private sector organizations on behalf of donors, and thus third-party monitors must be factored into any analysis of the humanitarian data sharing ecosystem.

23 https://odi.org/en/publications/data-sharing-and-third-party-monitoring-in-humanitarian-response/

Data sharing between humanitarian organizations and donor agencies: Data is regularly shared between humanitarian organizations and their donors for different reasons including reporting and auditing. While much of this data is aggregated,[24] in some cases personal data is shared with donors.[25] These dynamics have been the focus of two recent analyses: a 2021 report on the risks associated with humanitarian data sharing with donors prepared by the Global Public Policy Institute[26] and a separate 2022 analysis published by Larissa Fast on articulating responsible practice in data sharing between humanitarian organizations and their donors.[27] UN OCHA has also published a guidance note[28] on responsible data sharing with donor organizations.

It is important to emphasize here that these four data sharing relationships (between humanitarian organizations, between humanitarian organizations and government authorities, between humanitarian organizations and commercial parties or other private sector entities, and between humanitarian organizations and donors) have **institutions as their nodes**. Very rarely, if at all, is the beneficiary at the center of a decision to share or transfer their data, or is even in a position to reliably access data about them held by a humanitarian organization or its partners in government, the private sector or at donor agencies.

VERY RARELY, IS THE BENEFICIARY AT THE CENTER OF A DECISION TO SHARE OR TRANSFER THEIR DATA, OR IS EVEN IN A POSITION TO RELIABLY ACCESS DATA ABOUT THEM

This is where the current work picks up, but it is crucial to understand that effectively developing and implementing data portability and interoperability mechanisms will necessitate political will, institutional commitments, policy decisions, and, subsequently, technological capabilities that current forms of humanitarian data sharing do not. Moreover, it must also be stressed that traditional humanitarian data sharing, for example with government authorities, will not go away even if strong data portability and interoperability mechanisms are achieved. While data portability could be a sea change in terms of empowering beneficiaries to better access and manage their data, it is not a regime change.

24 Data aggregation is the process where raw data is gathered and expressed in a summary form for statistical analysis.
25 https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/
26 https://gppi.net/2021/09/06/data-sharing-with-humanitarian-donors
27 https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/
28 https://centre.humdata.org/guidance-note-responsible-data-sharing-with-donors/

KEY RESOURCES on humanitarian data sharing

- WFP and UNHCR have published a short video explaining their global data sharing addendum: "Neither agency should collect data from an individual or household if the same data has already been collected by the other agency."
- In a 2021 case study for the CALP network, Linda Raftree and Anna Kondakhchyan discuss responsible data sharing with governments, with a particular focus on data sharing in cash and voucher assistance programs undertaken in fragile settings or conflict environments.
- Sean Martin McDonald (2019) provides a critical analysis of humanitarian data sharing and the implications for trust.

Honing in on the digital identity domain

To this point, the discussion has focused on what we mean by data portability and interoperability, and explained current data sharing practice and governance in the humanitarian sector. But the potential of innovations in digital identity is, in part, to positively disrupt these dynamics to the benefit of the individual—that is, to put people at the center of decision-making about their data and how it is shared. We will therefore review key digital identity concepts and models before turning to assess how they might inspire greater data portability and interoperability.

A **digital identity** is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person.[29] Debates on digital identity are increasingly intertwined with high-level policy discussions on legal identity and in particular the achievement of Sustainable Development Goal 16.9 ('legal identity for all by 2030'). For this reason, in some cases it may be more productive to think about humanitarian data portability in terms of digital **profile** data.[30] These profiles could include health data, for example, or financial information.

At a high level, **a digital identity model** can be centralized, federated or decentralized.

In **centralized** models, the organization that creates a person's digital identity that is required for its service remains at the center.

29 https://id4d.worldbank.org/guide/glossary
30 https://thisisamos.com/2022/09/13/what-if-we-called-it-a-profile/

This model makes the person dependent on the organization for the verification of their identity. The proliferation of centralized digital identity systems, including in humanitarian contexts, has created a situation in which people may have different digital identities (or profiles) for each organization they receive services from. Not only does this increase the management load for people whose digital data is duplicated across multiple providers' systems, with attendant data protection and security risks, it also results in inefficiencies and unnecessary redundancies for organizations, including humanitarian agencies that often work together locally as part of response efforts. A notable example of a centralized digital identity system in the humanitarian domain is the World Food Programme's SCOPE platform.

Federated models have emerged in response to centralized systems, which are often derided as being disconnected silos. The key innovation in federated models is a dedicated entity that serves as a bridge between the person and the organization providing a service that requires identity verification. This entity, known as an **identity provider**, holds the person's digital identity data and allows them to access services from different providers without needing to register their identities or profiles multiple times. Importantly, while this model helps address the problem of managing multiple digital identities across different organizations, it still results in centralization. That is, the identity provider is now at the center of the model. In the humanitarian context, these developments have been framed in terms of 'platformization',[31] with UNHCR's digital identity system (PRIMES) emerging as a kind of identity provider for persons of concern in contexts where the system has been recognized as sufficient for identity verification for certain services, for example in Uganda where UNHCR attestation letters can be used to access SIM cards and mobile money services.[32] [33]

Decentralized models for digital identity seek to remove the reliance on centralized parties by empowering users to control and manage their own identity data. Already alluded to above, with the advent of blockchain technology the notion of self-sovereign identity (SSI) has emerged as a popular manifestation of the decentralized digital identity model. It must be stressed that decentralized digital identity models still exhibit certain features of centralization, namely a reliance on a relatively small number of SSI technology providers and expertise.

31 https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12353
32 https://doi.org/10.1080/02681102.2020.1811943
33 https://www.gsma.com/mobilefordevelopment/resources/proportionate-regulation-in-uganda-a-gateway-for-refugees-accessing-mobile-services-in-their-own-name/

A key component of these decentralized models is the **digital wallet** in which users can store their credentials (in the absence of a central database), though as Cheesman (2022) points out, digital wallets do not require the use of blockchain; nor are they necessarily decentralized. "They follow a variety of models, standards, and institutional and infrastructural arrangements, including but not limited to SSI. Among digital wallet projects that use blockchain, some propose a radical alternative to traditional currencies and identity management systems, but some do not – indeed, some of the most significant wallet initiatives are government led."[34] Notably, in September 2022 the Linux Foundation announced its intention to form the OpenWallet Foundation, a new collaborative effort to develop open source software to support interoperability for a number of different wallet use cases. It remains to be seen if humanitarian aid distribution will form part of the use cases.[35]

It is worth pointing out that each of the three models discussed above (centralized, federated and decentralized) can in theory be built to facilitate data portability and interoperability, even if this is rarely practiced in centralized systems which dominate the status quo. The SSI movement, however, has explicitly endorsed principles for both:[36]

- **Interoperability:** An SSI ecosystem shall enable digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards.
- **Portability:** An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice.

Another final key distinction to be made is between **foundational** and **functional** identity systems. Foundational identity systems are civil registers, national identification and population registration systems, which are created to provide identification to the general population (sometimes including non-citizens) for a wide variety of transactions. Functional identity systems manage identification, authentication and authorization for specific sectors or use cases, such as voting, taxation, social protection, travel and more.[37]

34 https://www.bosch-stiftung.de/en/publication/digital-wallets-and-migration-policy-critical-intersection
35 https://www.linuxfoundation.org/press/linux-foundation-announces-an-intent-to-form-the-openwallet-foundation
36 https://sovrin.org/principles-of-ssi/
37 https://id4d.worldbank.org/guide/types-id-systems

KEY RESOURCES on digital identity

- The World Bank's ID4D Practitioner's Guide intends to help in the design and implementation of identification systems that are inclusive and trusted—in accordance with the ID4D's ten Principles on Identification for Sustainable Development and other international standards and good practices.
- Tkyn's "ultimate beginner's guide" to self-sovereign identity provides a good overview of the underlying technology ("the plumbing"), security considerations, and different use cases.
- Margie Cheesman's 2022 brief on digital wallets covers various migration use cases as well as a focused discussion on potential risks emerging from their adoption by vulnerable populations.

Don't forget about cash!

Data portability and interoperability are not just priorities for digital identity—they are also highly relevant to ongoing discussions on the future of humanitarian cash transfers and voucher assistance. The aforementioned trilateral agreement between UNHCR, WFP and UNICEF for a common cash platform involves agencies "harmoniz[ing] their data management approach through interoperable data systems and data sharing agreements, with the objective to move towards a common data management and tracking system based on common beneficiary lists and easy access to beneficiary identification, thereby avoiding duplication."[38]

In September 2022, the Donor Cash Forum (a group of major governmental humanitarian donors supporting cash assistance) published **a Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming**.[39] The statement explains that "for affected populations, interoperability can be a driver for increasing inclusion in programming and increasing rights via **decentralising control of personal data**, whilst also ensuring stronger data protection and safeguarding. We also hope it will save beneficiaries time and effort through reducing assessment fatigue and/or re-registration."

38 https://www.unhcr.org/protection/operations/61e983d64/statement-principals-ocha-unhcr-wfp-unicef-cash-assistance.html
39 https://www.calpnetwork.org/publication/donor-cash-forum-statement-and-guiding-principles-on-interoperability-of-data-systems-in-humanitarian-cash-programming/

The statement, which elucidates ten guiding principles for interoperability in humanitarian cash programming, also highlights other humanitarian initiatives with explicit commitments on interoperability, including the aforementioned UN common cash platform, the CCD Network,[40] and the Barcelona Principles on digital payments in humanitarian response.[41]

While these statements emphasize the benefits of system interoperability, it is conceivable that through further policy reform and technology investment data portability could also become a component of humanitarian cash programming, for example through the deployment of a standardized beneficiary digital wallet.

KEY RESOURCES on humanitarian cash

- Following the announcement of the UN trilateral agreement, Elizabeth Tromans (Senior Technical Advisor for Cash and Emergencies at the International Rescue Committee – a member of the CCD Network) published a blog post addressing three key questions regarding problem framing, stakeholder involvement, ownership.
- A September 2022 webinar on the abovementioned **Joint Donor Principles on Interoperability of Data in Humanitarian Cash Programmes** provides context to the Donor Cash Forum statement.

Why would aid beneficiaries want to port their data?

In virtually all of the literature reviewed for this report, it is assumed that the benefits of data portability are either intuitive or that they will become clear to people (in the present context, aid beneficiaries) when the value proposition is explained to them, or where the technology can be demonstrated. Where research has actually been undertaken on user demand, most notably in the EU context in which there are legal protections in place for data portability, it has been found that data portability rights remain under exercised: "the actual problem with data portability in its current form appears to be that it does not seem very useful or popular among data subjects."[42]

40 https://www.collaborativecash.org/_files/ugd/79d5cf_4bc6650c8c874aaf975a5d369f80e518.pdf
41 https://nextbillion.net/eight-principles-for-digital-payments-in-humanitarian-response/
42 https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/

Newly published academic research,[43] based on surveys of German technology users, provides some of the first empirical data regarding people's propensity to port their data. The research finds that people who already attach high importance to privacy or who have high technology competencies demonstrate an increased desire to exercise data portability. "Users reported the greatest need for data portability for data-storage (i.e., cloud) services."

The general lack of interest for data potability among non-expert users could be explained differently: data portability is a relatively new right which might be partly why it is less popular than other data subject rights. Alternatively, the technologies underpinning data portability are still maturing and evolving which means more time may be needed for the public to fully appreciate the realm of possibility.

IT WOULD BE ADVISABLE FOR THE CCD NETWORK TO EMBARK ON AN EMPIRICAL STUDY THAT SEEKS TO UNDERSTAND WHETHER DATA PORTABILITY IS MEANINGFUL TO BENEFICIARIES OR IN WHAT CIRCUMSTANCES BENEFICIARIES WOULD WANT TO PORT THEIR DATA

Instead of writing it off entirely, however, it would be advisable for the CCD Network to embark on an empirical study that seeks to understand not just whether data portability is meaningful to beneficiaries or – put differently – in what circumstances beneficiaries would want to port their data,[44] but also to assess which specific identity credentials or digital profile data they would want to make portable and to discern how important notions like decentralization and self-sovereignty actually are. Anecdotal evidence suggests that beneficiaries would often expect humanitarian organizations to maintain a copy of their data and that they trust these organizations to manage that data responsibly, but these finer points should not be taken for granted and should be validated.

It will also be critical to understand any divergences between the motivations and objectives of CCD Network members (and their donors!) in terms of promoting data portability and interoperability and the desires of beneficiaries.

43 https://dl.acm.org/doi/10.1145/3543758.3543762

44 Margie Cheesman identified at least two use cases ("as yet unproven") in her brief on digital wallets in migration contexts, namely 1) extending access to credit services and local market integration for migrants and 2) digital wallets for cross-border recognition.

KEY RESOURCES on beneficiary perspectives

- Margie Cheesman's 2022 blog post for Data and Society reflects on how blockchain-based digital wallets that were designed to empower refugee women by enabling their greater financial independence, flexibility, security, and ability to save have suffered from unintended consequences.
- In a 2021 open-access commentary, Keren Weitzberg and colleagues encourage digital identity researchers to "to foreground the perspectives of subjects of aid intervention in all their diversity, ambivalence and contradictions".
- In September 2022, Robert Luzsa and colleagues published one of the first empirical studies of data portability from the user perspective, which should inform future research as well as practical initiatives to implement and popularize data portability, including among aid beneficiaries.

Data portability and interoperability lessons from the humanitarian domain

In this section of the desk review, we synthesize the limited public evidence from technical implementations of humanitarian digital identity systems in order to draw lessons for the CCD Network on data portability and interoperability. It is important to caveat upfront that there are very few examples of pilots or other implementations with publicly available information with which to inform the discussion.

One of the more well-documented case studies involves Gravity's work with the Kenyan Red Cross Society, i.e. the DIGID (Dignified Identities in Cash Assistance) project pilot.[45] Gravity's digital identity platform used during the DIGID project is based on decentralized identity and blockchain technology. KRCS volunteers used mobile devices to register beneficiaries by capturing their biometrics and recording biographical details. KRCS staff then cleaned the data using RedRose's data management software, after which Gravity would receive a request to create the beneficiary's digital wallet and credentials. The verified user then received a QR code which they would store in their mobile device if they had one; otherwise the QR code was printed for them. This QR code could subsequently be used to prove one's identity and to receive a token to receive cash assistance.

45 https://hiplatform.org/digid

A lessons learned report,[46] published following the pilot in January 2022, reflects explicitly on interoperability across two dimensions: interoperability with other NGOs and interoperability with other digital identity systems. Regarding the former, the report states that the pilot "was less about direct sharing of information between organizations, but rather the ability for multiple NGOs to read, recognize, and accept the digital credentials issued on their behalf by other humanitarian organizations when such credentials are presented to them by the affected individuals themselves". While this was not extensively tested during the pilot, it appears NGOs were positive about the possibilities for increased recognition and acceptance of digital credentials issued by other organizations.

That said, the report also acknowledges that such interoperability is not necessarily empowering of beneficiaries: "Humanitarian organizations are investing to become interoperable in terms of the beneficiary data in communities they serve. However, these efforts have been with systems owned by organizations where individuals have no direct access, raising questions of whether individuals have a choice in terms of their data being shared and whether they were informed to begin with. The affected individuals continue to lack control and power over their own data."

Regarding interoperability with other digital identity systems, the KRCS also assessed the extent to which the Gravity/DIGID system could interoperate with another pilot it was a part of, namely a Tkyn/121 project.[47] The report acknowledges that "few attempts have been made to demonstrate interoperability within decentralized identity, and this interoperability test is novel because it is between different decentralized identity wallets based on two distinct protocols that leverage very different technology stacks and networks." It continues: "Although both Tykn and Gravity adhere to the W3C standards of decentralized identifiers and verifiable credentials, the protocols have different ways of creating connections and exchanging messages and credentials. In addition, their public keys and schemas are stored on different public ledgers and use different verification algorithms. These issues are actively being addressed in different working groups within W3C and the Decentralized Identity Foundation, but, according to Gravity, it will likely take several years to achieve full interoperability."

46 https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf
47 https://tykn.tech/121-tykn/

Beyond these critical reflections on interoperability, however, is another depressing fact: the Gravity digital identities were not recognized by the Kenyan government for KYC or SIM registration purposes, which means that the KRCS default use of M-Pesa mobile money for humanitarian cash assistance did not benefit from the Gravity digital identity solution, i.e. services could not be extended to people who did not already have a government-recognized credential. This raises a bigger issue that seems to plague many of the digital identity projects currently being undertaken in the humanitarian sector, namely the lack of legal recognition by authorities means the identities have limited value and, perhaps more devastatingly, do not address the crucial issue of multiple enrollments and frustrating user experiences.

KEY REFERENCES on humanitarian data portability and interoperability

- IFRC's 2021 report on digital identity in the humanitarian sector is a key reference for understanding humanitarian needs and case studies. It also raises important questions about interoperability, SSI, and digital wallets for the sector.
- The lessons learned report (2022) following the DIGID project pilot in Kenya is an excellent resource regarding the possibilities for and challenges facing digital identity interoperability.

Concluding remarks

This desk review has shown that there is very limited evidence of successful implementations of data portability in the humanitarian context. In fact, it is still unclear what success would look like and this key question should be a central focus of the CCD Network going forward. Where interoperability is being promoted and advanced by humanitarian actors, one underexplored area is whether these developments serve to empower beneficiaries, in particular with respect to accessing and porting their data across service providers, or if it is aid organizations and their donors who largely stand to benefit from greater efficiencies and data sharing. The analytical report that accompanies this desk review will delve deeper into these complexities and their politics, with a view to charting a path forward as the CCD Network pursues its important work on data portability, interoperability and digital identity.

References

Article 29 Data Protection Working Party. 2017. Guidelines on the right to "data portability". https://ec.europa.eu/newsroom/article29/items/611233

Brown, I. 2020. The technical components of interoperability as a tool for competition regulation. https://www.ianbrown.tech/2020/10/26/the-technical-components-of-interoperability-as-a-tool-for-compe.tition-regulation/

CCD. 2019. Global Collaboration Agreement Collaborative Cash Delivery (CCD) Network. https://www.collaborativecash.org/_files/ugd/79d5cf_4bc6650c8c874aaf975a5d369f80e518.pdf

Cheesman, M. 2022. Blockchain for Refugees. *Data & Society: Points*. https://points.datasociety.net/blockchain-for-refugees-a46b41594eee

Cheesman, M. 2022. Digital Wallets and Migration Policy: A Critical Intersection. *Migration Strategy Group*. https://www.bosch-stiftung.de/en/publication/digital-wallets-and-migration-policy-critical-intersection

Diepeveen, S., Bryant, J., Mohamud, F., Wasuge, M. and Guled, H. 2022. Data sharing and third-party monitoring in humanitarian response. *ODI*. https://odi.org/en/publications/data-sharing-and-third-party-monitoring-in-humanitarian-response/

Donor Cash Forum. 2022. Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming. https://www.calpnetwork.org/publication/donor-cash-forum-statement-and-guiding-principles-on-interoperability-of-data-systems-in-humanitarian-cash-programming/

Doornbos, A. 2022. What if we called it a 'profile'? https://thisisamos.com/2022/09/13/what-if-we-called-it-a-profile/

Fast, L. 2022. Data sharing between humanitarian organisations and donors. *Norwegian Centre for Humanitarian Studies*. https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/

Graef, I., Husovec, M. and van den Boom, J. 2020. Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes. *Journal of European Consumer and Market Law* 9(1): 3–16. https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/9.1/EuCML2020002

GSMA Mobile for Development. 2020. Proportionate regulation in Uganda: A gateway for refugees accessing mobile services in their own name. https://www.gsma.com/mobilefordevelopment/resources/proportionate-regulation-in-uganda-a-gateway-for-refugees-accessing-mobile-services-in-their-own-name/

ICHA. 2022. Dignified Identities in Cash Assistance: Lessons Learnt from Kenya. https://cash-hub.org/resource/dignified-identities-in-cash-assistance-lessons-learnt-from-kenya/

Krämer, J., Senellart, P. and de Streel, A. 2020. Making data portability more effective for the digital economy. *Centre on Regulation in Europe*. https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/

Luzsa, R., Mayr, S., Syrmoudis, E., Grossklags, J., Kübler-Wachendorff, S. and Kranz, J. 2022. Online Service Switching Intentions and Attitudes towards Data Portability – The Role of Technology-related Attitudes and Privacy. In Proceedings of Mensch und Computer 2022 (MuC '22). Association for Computing Machinery, New York, NY, USA, 1–13. https://dl.acm.org/doi/10.1145/3543758.3543762

Madon, S. and Schoemaker, E. 2021. Digital identity as a platform for improving refugee management. *Information Systems Journal* 31(6): 929–953. https://onlinelibrary.wiley.com/doi/10.1111/isj.12353

Martin, A. and Taylor, L. 2020. Exclusion and inclusion in identification: regulation, displacement and data justice. *Information Technology for Development* 27(1): 50–66. https://doi.org/10.1080/02681102.2020.1811943

Martin, C., and Zimmerman, J. 2016. Eight Principles for Digital Payments in Humanitarian Response. https://nextbillion.net/eight-principles-for-digital-payments-in-humanitarian-response/

McDonald, S. 2019. From Space to Supply Chains: A Plan for Humanitarian Data Governance. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179

OECD. 2021. Data portability, interoperability and digital platform competition. *OECD Competition Committee Discussion Paper*. http://oe.cd/dpic

Raftree, L. and Kondakhchyan, A. 2021. Case Study: Responsible Data Sharing with Governments. *CALP Network*. https://www.calpnetwork.org/publication/case-study-responsible-data-sharing-with-governments/

Reuss, J. and Bilderbeek, N. 2022. Data portability in the EU: An obscure data subject right. *The International Association of Privacy Professionals*. https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/

Riley, C. 2020. Unpacking interoperability in competition. *Journal of Cyber Policy* 5(1): 94-106. https://doi.org/10.1080/23738871.2020.1740754

Slavin, A. Putz, F. and Korkmaz, E. 2021. Digital Identity: An analysis for the humanitarian sector. *IFRC*. https://www.ifrc.org/document/digital-identity-analysis-humanitarian-sector

Tromans, E. 2019. The UN Common Cash Platform: What does it mean and how is the IRC responding? *CALP Network*. https://www.calpnetwork.org/blog/the-un-common-cash-platform-what-does-it-mean-and-how-is-the-irc-responding/

UN OCHA. 2020. Guidance Note on Responsible Data Sharing with Donors. https://centre.humdata.org/guidance-note-responsible-data-sharing-with-donors/

UNHCR. 2018. Bridging the identity divide – Is Portable User-Centric Identity Management the Answer? https://www.unhcr.org/blogs/bridging-identity-divide-portable-user-centric-identity-management-answer/

UN OCHA, UNHCR, WFP and UNICEF. 2018. STATEMENT FROM THE PRINCIPALS OF OCHA, UNHCR, WFP AND UNICEF ON CASH ASSISTANCE. https://www.unhcr.org/protection/operations/61e983d64/statement-principals-ocha-unhcr-wfp-unicef-cash-assistance.html

UNHCR, WFP and UNICEF. 2020. Data Sharing Agreement among the Office of the United Nations High Commissioner for Refugees, the World Food Programme and the United Nations Children's Fund in the context of programmes involving transfers of cash assistance to beneficiaries in humanitarian situations. https://www.unhcr.org/602e24a94.pdf

UNHCR, WFP, UNICEF and OCHA. 2021. UN Common Cash Statement Progress report – September 2021. https://www.unhcr.org/615c44634.pdf

Weitzberg, K., Cheesman, M. Martin, A. and Schoemaker. E. 2021. Between Surveillance and Recognition: Rethinking Digital Identity in Aid. *Big Data & Society* 8(1). https://journals.sagepub.com/doi/full/10.1177/20539517211006744

Westphal, F. and Meier, C. 2021. Risks Associated with Humanitarian Data Sharing With Donors. *Global Public Policy Institute*. https://gppi.net/2021/09/06/data-sharing-with-humanitarian-donors

World Bank. 2019. ID4D Practitioner's Guide. https://id4d.worldbank.org/guide

Wong, J. and Henderson, T. 2018. How Portable is Portable?: Exercising the GDPR's Right to Data Portability. In Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers (UbiComp '18). Association for Computing Machinery, New York, NY, USA, 911–920. https://dl.acm.org/doi/10.1145/3267305.3274152

Data Portability and Digital Identity in Humanitarian Aid:
A DESK REVIEW

www.collaborativecash.org