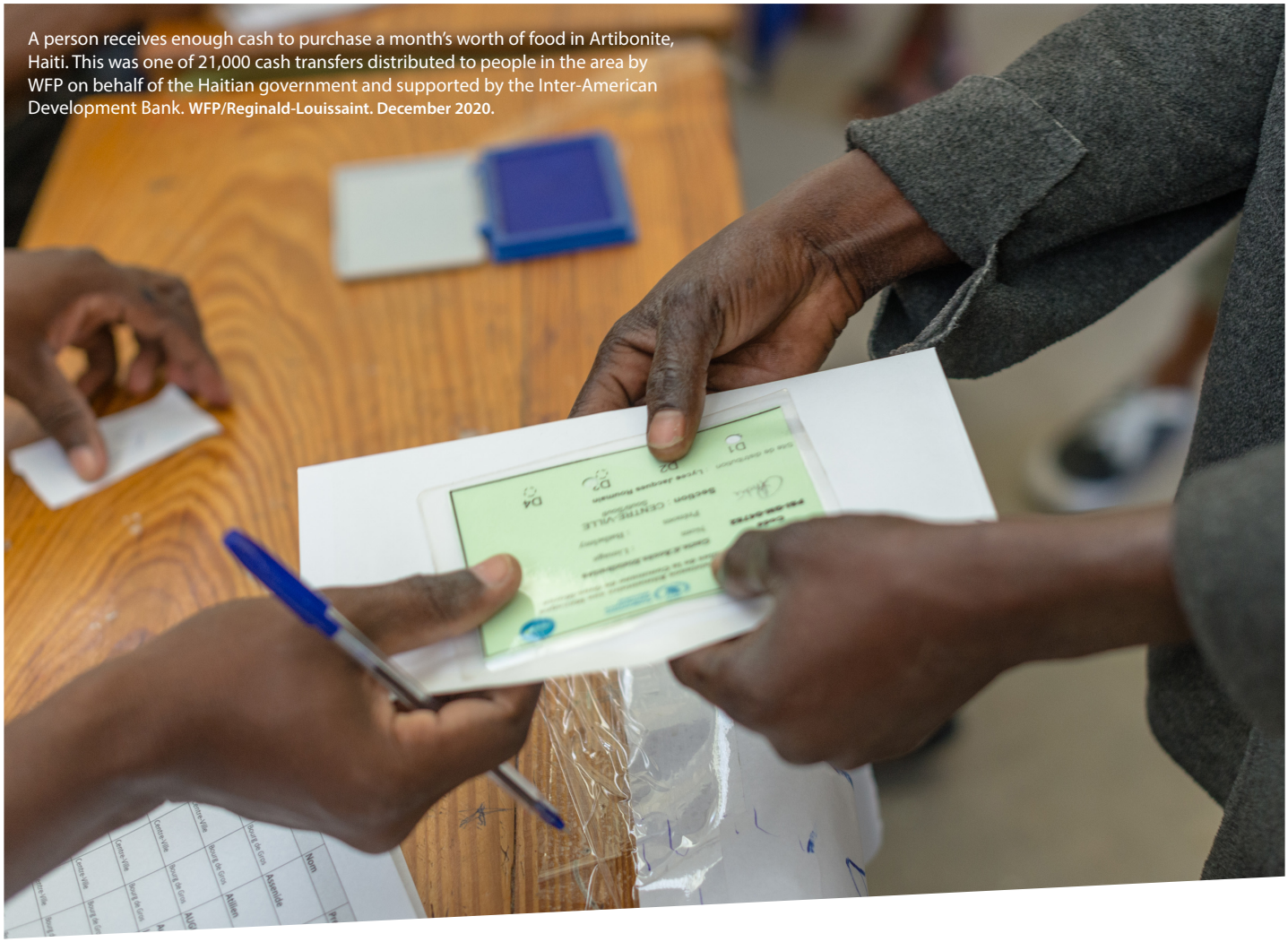
CaLP
The Cash Learning Partnership

CASE STUDY:

RESPONSIBLE DATA SHARING WITH GOVERNMENTS

WFP/Claire Nevill. March 2018.



A person receives enough cash to purchase a month's worth of food in Artibonite, Haiti. This was one of 21,000 cash transfers distributed to people in the area by WFP on behalf of the Haitian government and supported by the Inter-American Development Bank. **WFP/Reginald-Louissaint. December 2020.**

ACKNOWLEDGEMENTS

This case study was commissioned by CaLP with funding from the German Federal Foreign Office (GFFO).

The research for this publication was conducted between June and September 2020 by Linda Raftree, an independent consultant.

The publication was developed by Linda Raftree (@meowtree), with editorial and content supervision and support from Anna Kondakhchyan (@akondakhchyan). This case study benefited from invaluable input from the many organisations and CVA practitioners, who have generously contributed their lived experience to the research process and who, because of the sensitive nature of this research, shall remain anonymous.

The views expressed in this publication are the authors' alone and are not necessarily the views of the donors or of CaLP member agencies.

CaLP is a dynamic global network of over 90 organisations engaged in the critical areas of policy, practice and research in humanitarian cash and voucher assistance (CVA) and financial assistance more broadly.

For more information, please visit CaLP website at www.calpnetwork.org

Follow CaLP on Twitter: @calpnetwork

Front cover image: The government of Uganda, UNHCR and WFP are working together to biometrically verify all refugees by the end of the year. WFP is providing cash and food assistance to over one million refugees affected by recurring climate shocks.

Members of CaLP work in a wide variety of contexts, including those experiencing active conflicts, refugee crises, internally displaced populations and blockades. In these situations, cash and voucher assistance (CVA) actors often navigate challenging questions around data sharing with partners as part of a consortium, with donors, with third party service providers and with government authorities. Data sharing between and among any CVA actors can be challenging.

In recent months, there have been an increasing number of questions among CVA actors about data sharing with government authorities in fragile settings or conflict environments. The growing emphasis on linking humanitarian cash and voucher assistance (CVA) and government-led social protection systems[1] has contributed to an increase in concerns about data sharing with governments. The COVID-19 crisis has further accelerated interest in the links between CVA and social protection due to the increasing use of cash assistance in the face of widespread economic downturns and loss of formal and informal employment. Quarantines and lockdowns have also pushed humanitarians to incorporate more digital modalities into their work.

While many humanitarian actors recognize the importance of working in collaboration with and strengthening government systems, concerns persist over the sharing of detailed CVA recipient data with governments, especially in contexts where authorities are unfriendly toward segments of the population, for example, where refugees may be at risk of forcible removal or where governments are actively taking sides in a conflict.

Both humanitarian CVA and social protection are activities that necessitate the handling of high quantities of personal and sensitive data. Effective linkages between the two require that clear data governance and data-sharing arrangements exist across the entire intervention life cycle. It is critical that agencies uphold the best interests of affected populations when making decisions about data sharing. However, operating contexts are varied and often require CVA actors to use creative strategies to negotiate multiple challenges in determining which decisions will lead to the greatest benefit and the least harm for crisis-affected persons.

This paper looks at different strategies that CVA actors could implement to mitigate real and potential harms that sharing CVA beneficiary data with governments could cause for crisis-affected populations. Some 35 individuals working across the CaLP membership in several countries were interviewed for this paper. Because the topic is sensitive, we have anonymized interviewees. We have also redacted the names of organizations and countries in some instances.

WHAT ARE THE RISKS OF SHARING DATA WITH GOVERNMENT?

Sharing beneficiary data can be extremely useful for programme planning and budgeting, avoiding duplication, supporting linkages between CVA and social protection, and ultimately achieving greater efficiencies and impact in people's lives. However, data on religion, political affiliation, ethnicity, or other demographic data can also be used to harm individuals or groups.

In many instances, organizations collect personal and sensitive data on highly vulnerable individuals, including in some cases national ID, biometric data, phone number, address, children' names, parents' names, bank account or other financial information, citizenship status, health data (e.g. during COVID-19 responses), and more. They also hold data on group identities and behaviours, such as where urban refugees live, locations where cash or vouchers will be delivered or handed out, migration routes and other data that could be gleaned from analysing patterns in anonymized data within large population databases.

It's a high-risk item in the agenda. Not only the likelihood of mismanagement is high but the impact of it is extremely high. Extremely high-risk.'

1 Smith, G. (2020) 'Supporting the Linkages between Humanitarian Cash and Voucher Assistance and National Social Protection Systems.' The Cash Learning Partnership.

A 2020 paper produced for the International Committee of the Red Cross (ICRC) Data Protection Office identified key risks with humanitarian engagement in social protection programming, including:

- low data protection infrastructure and standards in some governments;
- the limited ability of humanitarian organizations to monitor onward data sharing and processing, including sharing with other bodies and use of data for purposes other than social protection;
- social protection data being combined with other datasets to reveal sensitive information;
- potential changes in future data sensitivity and technology.[2]

Interviewees for this paper cited examples of potential harm from data sharing with governments that do not welcome refugees, irregular migrants, and asylum seekers, such as the potential that CVA recipient data is used for tracking, deportation, or detention purposes. It was recognized that data could also be used to identify populations who are assumed to be aligned with a particular side in a conflict, or shared with other country governments who have an interest in tracking refugees, and who could potentially do harm to those refugees' families.

Interviewees also noted that a close relationship between an agency and a government authority can weaken the trust between that agency and its partners, if these partners have concerns about how authorities might use data. Even in cases where data sharing is legitimate, one person noted, governments change, requiring caution and data sharing only in cases where there is clear justification and where data minimization and other data protection mechanisms to protect individuals and groups have been put in place. Clear accountability mechanisms are also necessary in case agreements are not honoured.

> The government will be different today from what it will be tomorrow. You have to start from the assumption that data will be used to do harm.'

In some cases, recipients of CVA are aware that their data can put them at risk, but in general, understanding of data sharing and issues around coercion are not well understood by the majority of beneficiaries. In Iraq, for example, an initiative has been running over the last several years to transition the most vulnerable segments of humanitarian cash caseloads over to government social protection programs. The Cash Consortium for Iraq (CCI)[3] began conversations with affected populations regarding their data and the possibility of humanitarians referring them for government assistance. The CCI included a 'willingness to be referred' question on their regular feedback surveys with affected populations. Overall willingness was much higher than anticipated, however, there was distinct variation across different geographical areas. The Consortium is planning to conduct additional research with target populations to better understand their awareness of risks and their attitudes toward different types and levels of data sharing.

WHY MIGHT IMPLEMENTING AGENCIES BE ASKED TO SHARE DATA WITH GOVERNMENTS?

There are a number of reasons that governments might request access to non-personal data about the programmes that humanitarian organizations are implementing, for example, geographic location of programmes or information about local partners. Government authorities may also request personal data about recipients of CVA for various reasons.

- Some of these requests to share data can be considered *legitimate*, with goals and purposes that are aligned with humanitarian mandates and legal frameworks. In these cases, organizations will find it reasonable to share data at specific levels of aggregation under the right conditions and within established agreements.[4]

2 Xu, R., Quijano Carrasco, C., Capotosto, J. (2020) 'Data protection risks of humanitarian engagement in social protection.' ICRC Data Protection Office.
3 The CCI is a partnership of the Danish Refugee Council, the International Rescue Committee, the Norwegian Refugee Council, Oxfam and Mercy Corps as lead agency.
4 The GSMA has published a set of guidelines for mobile network operators to guide data sharing during the COVID-19 pandemic, for example.

- Where motivation is less clear, data-sharing requests could be categorized as *semi-legitimate* or blurry and require more information and discussion before a decision on data sharing (or not sharing) is made.
- Other requests might be deemed *illegitimate*, and agencies will want to avoid sharing data that they suspect could be used to harm vulnerable or affected persons and groups or data that could be used for reasons that are not aligned with humanitarian principles or good governance mechanisms.

Some examples of the three categories of data requests are listed below:

Legitimate reasons for data sharing requests:

- When eligible populations are being included in a social registry run by a government;
- When there is a need to avoid duplication of benefits across programmes/agencies/organizations;
- When assuming responsibility for a population formerly served by humanitarians and/or as part of a handover or exit strategy;
- When complying with Know Your Customer (KYC) and Financial Action Task Force (FATF) global recommendations;[5]
- When humanitarian or other agencies are suspected of corruption or bribery and government wants to undertake an audit.

BOX 1: DATA SHARING FOR CVA AND SOCIAL PROTECTION LINKING

Governments might be building their list of beneficiaries for social protection programming. Their goal will be to identify individuals in need of social protection (for example, those with a disability, the elderly) who will consistently receive social protection assistance. If an emergency arises, the government needs to be able to identify people from the social registry list who are not receiving social protection for pre-existing reasons. They will need to cross-reference their list with lists held by humanitarian agencies so that agencies can provide CVA to those who are not already receiving it from the government.

The scenario in Box 1 is an example of legitimate data sharing between humanitarians and government for CVA and social protection linking. When governments are building their social protection programmes and there is no reliable census or other administrative data to draw from, they may request access to data from humanitarian agencies to fill in missing information. Although many humanitarian actors now agree that strengthening linkages between humanitarian CVA and social protection is a good idea, there are often different levels of willingness among CVA actors regarding whether certain kinds of data, such as names, national ID, phone numbers and other demographic data, should be shared with government authorities. This can lead to a dynamic within Cash Working Groups and other consortia in which it is difficult to come to a united decision about whether all CVA actors in a particular response will share data with government authorities, even when it is deemed to be for legitimate purposes.

> If you are working in a headquarter office you will be less worried about data sharing, but in communities where you are doing a humanitarian response, the issues are much more live and concerning.'

5 Financial Action Task Force (2020) 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations'.

Semi-legitimate or 'blurry' reasons for data sharing with governments include:

- When the motivation for a data-sharing request is unclear and more information is needed to determine whether it is justified;
- When legitimate beneficiary data sharing disguises a suspected motivation of political gain (whether the data sharing is offered by an organization, agency or a third party, or is requested by a government);
- When a lack of clarity about CVA activities and related processes leads to legitimate concerns by government, yet these are accompanied by illegitimate requests for CVA beneficiary data.

BOX 2: GOVERNMENT CONCERNS ABOUT CVA ACTIVITIES

In March 2019, the Economic and Financial Crime Commission (EFCC) of Nigeria arrested and detained Mercy Corp staff and vendors for transmitting cash in a rural area. The EFCC insisted on accessing the beneficiary list along with other operational documents before staff could be released. Mercy Corps did not share the beneficiary list due to concerns about how EFCC might handle the data and the possibility that it could be shared with other security agencies. In addition, Mercy Corps considered that sharing this data violated the humanitarian principle of independence, as it compromised their ability to work autonomously from the government agency and the principles and standards for the secure use of personal data in cash and e-transfer programmes.

Initial negotiations with the EFCC were held to release the detained staff. A position was developed to guide the Humanitarian Country Team in negotiations and high-level advocacy with the federal government and relevant ministries to improve the operational environment for CVA. Detained staff and the confiscated cash were released. The Cash Working Group (CWG) summarized the money laundering act (MLA), which the EFCC had invoked when they halted the cash distribution. This helped the Humanitarian Country Team and donors better understand the MLA and the Anti-Terrorism Financing Act. The CWG trained partners on financial regulations and continued meeting with the EFCC, and held a session to present on CVA, its rationale, and partners.

Together, the CWG and the EFCC agreed on guidelines and forms of cash movement that require countersigning by the partner moving cash and several others. The CWG provided a summary to the EFCC of the different laws in Nigeria on data protection and used that to frame what data could be shared and what could not be shared. It also developed a concept note for the development of a National CVA Policy, aimed at strengthening the operational environment for CVA in Nigeria, and a Terms of Reference for the Task Team that would steer the development of the national CVA policy.[6]

In the second case example in Box 2, the motivations of the anti-graft agency (the EFCC) were not entirely clear, and there was cause for concern about sharing personal and sensitive data on affected populations with government agencies. The Cash Working Group conducted a number of meetings and worked with federal government to enable a greater understanding of data protection according to the law and to humanitarian principles. This allowed the work to continue with the greater involvement of the EFCC in the process and without the need to share certain beneficiary data that could have put CVA beneficiaries at risk.

Illegitimate reasons for data sharing include data sharing outside of legal frameworks and data sharing that is legitimate but unethical,[7] for example:

- When a government authority asks for beneficiary lists in order to add unqualified individuals to registries;
- When a government authority demands that recipient or other data be shared in order to allow a CVA programme to proceed;
- When an organization or agency gains power and influence by sharing CVA recipient data with government authority without beneficiary consent or when other organizations or agencies have refused to share it;

6 Cash Working Group, Nigeria (2020). 'Position Paper submitted to the Humanitarian Country Team'.
7 While legal frameworks help answer the question 'can we do this?' ethical frameworks help answer the question 'should we do this?'

- When beneficiary data is requested with the purpose of screening and excluding specific eligible persons or groups from receiving humanitarian aid (such as CVA);
- When a request for data sharing could result in targeting or active harm to a particular group of people (IDPs, refugees, ethnic group, political group) or when it is suspected that data will be shared onward to others who could use it to harm a particular group;
- When data sharing is non-transparent or unaligned with the original purpose for data collection;
- When data sharing requests are used to gain financial or political advantage or as a means of exercising power and control.

Official requests for data sharing can be addressed through formal means. In conflict situations, however, requests to share data may come from different levels of government, and these can pose a challenge for CVA actors. While some illegitimate requests may come through official channels, others fall into the category of forced requests or coercion. These require different strategies.

These are sensitive topics that are not being addressed. It's so critical, but at times if you push back you can't work in that location. Sometimes it's the local authorities -- the district-level authority, not the central government -- that is trying to make organizations bend their own rules. Here again, this is a case of negotiation and diplomacy. We put the beneficiaries at the heart of any conversation that we start.

In [...] and [...] people are so reluctant to share. Governments and other groups are fighting, and we don't know what to do regarding sharing and accessing information. If the situation becomes critical and it's life threatening, we have to give data or we're not allowed to access the area.'

Across humanitarian responses, data is commonly shared for illegitimate reasons. In some cases, being forced to share data with government authorities is seen as 'the cost of doing business', yet sharing data can have dire consequences for CVA recipients. Some field practitioners interviewed for this paper expressed concern about whether it is possible to deny requests for data. They worry that organizational management is not armed with the right tools to refuse to share data in challenging contexts where power imbalances are at play.

Illegitimate data sharing, forced data sharing, and coercion are *critical data incidents*.[8] The definition of a personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.'[9] When data sharing is forced or coerced, or beneficiary lists are forcibly altered or disclosed, technically this is a critical data incident or a breach, and it should be treated as such. (Note: coming soon – CaLP's **proposal for community critical data incident management**).

8 See OCHA's work on Critical Data Incidents.
9 European Union's General Data Protection Regulation (2018)

AN UPHILL BATTLE?

Data sharing with government, like data sharing overall in CVA programming, is fraught and challenging, with few ready-made solutions or good practices. Frontline staff and enumerators might be putting their lives on the line by refusing to share data, or they might not be allowed to access particular zones of a country.

> It's a tricky argument if you don't share data with government. If you are supposed to work in a particular country, there is a limit as to what you can push back on.'

Holding to high standards can be frustrating, according to some CVA practitioners, because while they may refuse to share beneficiary data, other entities might be less resistant.

> … agencies are sharing with authorities under different pretexts with no data-sharing agreement. I would push back on data sharing, and government officials would come back and tell me "here is the distribution list that your donor […] has given us, so ha ha ha"."

In other cases, power dynamics make it difficult to operate programmes.

> A particular government authority has bullied the NGO who manages the camp under his authority into sending an email request for sensitive data on behalf of this government authority to other NGOs working in the camp. If I remember correctly, one or two agencies have stopped programming because of this demand. I spoke to our counterparts at other agencies, including a UN agency, and they have been bullied themselves by this authority, who has a lot of power.'

Data-sharing agreements between humanitarian agencies and government authorities have led to a gap in data protection in some cases. Some organizations conduct needs assessments together with governments who sign off and certify beneficiary lists. The limited ability of humanitarian organizations to monitor further sharing and processing of data that is shared with governments was raised by interviewees for this short paper and also highlighted in a recent International Federation of the Red Cross study on data protection risks of humanitarian engagement in social protection.[10]

> It's a game between NGOs and governments in terms of giving up or influencing beneficiary lists …. Biometrics and other types of accountability mechanisms make it more difficult to alter beneficiary lists …. In fragile contexts, understanding how to negotiate is an important skill.'

10 Xu, Quijano Carrasco, & Capotosto, J. 'Data protection risks'.

STRATEGIES TO MANAGE DATA-SHARING REQUESTS FROM GOVERNMENT AUTHORITIES

Put the best interests of CVA recipients first

Where possible, agencies should advocate for clear frameworks that articulate the conditions under which government authorities could ask for data and that specify any checks and balances or countervailing factors that may empower them to refuse a data-sharing request if it were deemed inappropriate or against the interests of the beneficiary. In the absence of these frameworks, CVA implementing agencies will have to determine whether they are willing to share data, depending on their mandate and role and their arrangement for being in a country or for collecting data as part of a CVA programme.

Organizations should take a 'best interest of the affected population' approach and conduct an assessment to weigh risks that data sharing could cause to affected populations versus risks of refusing to share data. This needs to be incorporated into consent processes, as CVA recipients will need to know if there is a chance that their data would be shared with governments and what the risks might be, so that they can make a decision before providing their data. Negotiation and 'soft skills' will be needed to engage with various levels of government to work out how to keep data secure and also safeguard the affected population more broadly, and to weigh benefits of implementation against the harms of closing down an existing programme that is already providing CVA. In the early phases of planning for CVA implementation, while conducting a context analysis, it is important to assess the political economy of data – who might want data and why, and what value the data holds for whom in the context – and incorporate this into risk assessment and planning.

Know your organization's status and principles

National data privacy laws, if they exist, will likely regulate what data can be shared under what circumstances. Some organizations have established privileges and immunities that are determined through an agreement with a country government. Many organizations have their own established data-protection principles that should be followed, but in the absence of such organization-specific principles, existing sector standards can be used. For example, OCHA's Data Responsibility Guidelines stipulate principles including: fair and legitimate processing of data; purpose specification that is consistent with mandate and balanced with relevant rights, freedoms and interests; necessity, relevancy and adequacy of data processing as related to the purpose that has been identified; clear and reasonable retention periods; accuracy of data; confidentiality of data; security of data; transparency to data subjects, including why information is being shared and how to raise complaints or retract data; data transfers only where appropriate protection is ensured; and accountability mechanisms that can assure adherence to the above.[11]

Have a plan for managing data-sharing situations, and rehearse it

Based on the above status and principles, organizations should put in place and adhere to robust, rehearsed policies and procedures with strong governance that provide guidance on how to handle data-sharing requests. These can help an organization to determine how to approach requests for data sharing with governments. The GSMA's *Mobile Policy Handbook*,[12] for example, sets out restrictions on, and checks and balances for, government access requests for Mobile Network Operators to adhere to when laws and/or licence conditions require them to support law enforcement and security activities in countries where they operate. Role-playing the implementation of such policies helps staff and management to hone the art of making difficult moral decisions in real time. Rehearsing or conducting simulations that guide staff through the process of managing different types of data-sharing situations, including moving through an escalation matrix, can build reactive skills and improve staff capacity to conduct assessments in real time, even in the middle of a high-stress situation. Pre-establishing thoughts, redlines, strategies and escalation paths help staff to interpret and implement principles.

Establish data-sharing policies and agreements

Establishing a data-sharing policy and data-sharing agreements can help to set parameters for what data can be shared with governments and how. These can serve as a baseline or starting point for legitimate data-sharing requests from governments and they can also help with negotiation positions, should semi-legitimate or illegitimate data-sharing demands be made. Additionally, inserting notification clauses into agreements with Financial Service Providers (FSPs) can help in situations where FSPs may be obliged to provide data to a central bank.

11 OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
12 GSMA (2019) 'Mobile Policy Handbook: An Insider's Guide to the Issues'.

Incorporate data minimization, data security and privacy by design

The less data collected; the less data can be shared. While personal and sensitive data are needed to deliver CVA programming, practising data minimization (e.g. collecting the least amount of data possible, retaining it for the least amount of time necessary, de-identifying data as soon as possible) is one way to help minimize the potential impact of data sharing, whether legitimate, semi-legitimate or illegitimate. Data-security measures, such as encryption, tokenization or pseudonymization can also help protect data, especially in cases of illegitimate data-sharing requests.

Use technologies that preserve privacy

Privacy preserving design of data collection will minimize the amount of data that can be shared, because the data simply will not be accessible for unintended or unauthorized use. Moving data off local devices and into the cloud is one option (assuming this is feasible, and that the risks of data in the cloud are lower than the risks of data on a local device). Encrypting phones and devices is another way to protect data. Some organizations are exploring the use of distributed ledger technologies and blockchain for storing personal data for CVA programming. Personal financial data on the blockchain would be under the control of the CVA recipient, enabling data portability.[13] This could mitigate some of the challenges of data sharing in CVA programming. There are many challenges that are yet to be resolved in relation to these emerging technologies, however.

Offer choice of modalities

When there are concerns that data shared with governments could lead to harm, affected people need to be fully and transparently informed as part of the consent process. While CVA processes are becoming increasingly digital, it is possible to reduce the amount of data that is required by offering alternatives. CVA recipients should be given a choice of whether they want to provide their data and, if not, there should be an option to enrol in a CVA programme under a mechanism that requires minimal data collection, or to receive assistance that does not require Know Your Customer (KYC) or similar kinds of data. In Libya, for example, the ICRC negotiated an agreement with an FSP to use sub-accounts where the due diligence and KYC are completed only on the main account holder, and not on those accessing sub-accounts. Sub-accounts are then accessed through, for example, smart cards (e.g. pre-paid or ATM cards) that only have reference numbers attached to them, and no personal details. Beneficiaries are then able to withdraw cash without their personal data being provided to the FSP. Only the main account holder has access to the information linking the card or account to the beneficiary. Another option is to use FSPs where individuals already have accounts, meaning that the KYC process has already been conducted. Not all agencies are able to offer these options, however, due to structure, size and dependencies on other agencies for systems and funding.

Establish secure systems with limited access

System design can help to reduce the amount of data shared with governments, whether legitimate, semi-legitimate or illegitimate. In Yemen, for example, a database was designed that only authorized persons can access based on their role. District level managers cannot access global level data. Enumerators can only upload data into the system, they cannot download it. The system has triggers and safety measures designed into it, for example, time stamps and tracking of what an individual does and looks at within the system. Access levels are controlled by the Cash Consortium of Yemen. Information is unified and security is set so that no one can download data without approval.

Protect frontline staff and enumerators

Sometimes frontline staff and enumerators must field a great deal of illegitimate data-sharing requests. It is important to help keep them safe by designing data collection in ways that reduce their direct access to personal or sensitive data. In Iraq, household-level data is collected using a mobile data collection app, and as soon as an enumerator hits 'send' the data goes to the cloud and nothing is saved onto the phone. If a phone is stolen or an enumerator is threatened, they cannot provide any data even if the phone is unlocked or they are forced to show the phone's contents. Where frontline staff are under pressure or need to negotiate and deter illegitimate data sharing with local government entities, training and support will be required. (It should be noted, however, that when cloud services are used, data crosses international boundaries, which may create other challenges related to cross-border data transmission.) In some cases, it is better for international staff to take on the role of negotiation, as

13 Data portability 'is the principle that individuals have a right to obtain, copy, and reuse their own personal data and to transfer it from one IT platform or service to another for their own purposes'.

they might be less vulnerable to retributory responses than national staff. Conditions might be such that local staff should not operate in their home communities, where they can be identified and pressured or intimidated in various ways to share data, or even harmed.

Work as a united front within humanitarian coordination bodies

Formal and informal humanitarian coordination bodies such as Cash Working Groups (CWG), Humanitarian Country Teams (HCT) or the Inter-Cluster Coordination Group (ICCG) can play a role in helping to align positions and provide guidance to individual members. They can, for example:

- Work to raise awareness and understanding of data responsibility among members;
- Discuss scenarios in which governments might ask for data and determine which of those scenarios are legitimate, semi-legitimate or illegitimate;
- Agree on a coordinated approach and united message at national level on data sharing with governments;
- Provide 'soft governance' by directing policymakers to established guidelines;
- Support Country Humanitarian Teams to take a position and establish red lines around data sharing with governments;
- Agree standards and consistency across actors.

Keep other organizations informed

Individual organizations should:

- Inform the humanitarian coordination body (CWG, ICCG, HCT) if they already share data with governments or are planning to;
- Inform the coordination body if they are approached and asked to share data;
- Work within humanitarian principles and protection guidelines, for example, the core principle of 'do no harm', and follow principles for ethical and responsible data management (your own or borrowed from another organization with strong policies such as the ICRC[14] or OCHA[15]);
- Be transparent about government requests for information. Mobile network operators (MNOs) in particular report that they regularly have to deal with multiple government requests for customer information. While MNOs may have no option other than compliance with such requests, they are increasingly in need of greater transparency about the nature and scale of government access.[16]

CONCLUSION

The role of host governments in emergency responses is increasing, both with respect to social protection and humanitarian CVA. In this data-rich world, demands for data from humanitarian organizations will only increase in the future, and host governments are employing increasingly sophisticated approaches to obtaining it. The CVA community needs to learn from and guide each other, including 'in real time' as these requests are happening, so that consistent approaches can be agreed upon within country teams, cash working groups and consortia.

In all cases, placing the best interest of the affected population at the heart of decisions about data sharing with governments is key.

14 ICRC (2020) 'Data Protection in Humanitarian Action' Second Edition.
15 OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
16 GSMA (2019) 'Mobile Policy Handbook: An Insider's Guide to the Issues'.

www.calpnetwork.org

March 2021