IMPROVING CASH-BASED INTERVENTIONS
MULTIPURPOSE CASH GRANTS AND PROTECTION
Enhanced Response Capacity Project 2014–2015

Know Your Customer Standards and Privacy Recommendations for Cash Transfers

UNHCR
The UN Refugee Agency

World Vision

Know Your Customer Standards and Privacy Recommendations for Cash Transfers

April 2015

This document was prepared for the Office of the United Nations High Commissioner for Refugees and World Vision International by Ryerson University. It was written by Avner Levin, Anupa Varghese and Michelle Chibba.

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.

Contents

CONTENTS

CONTENTS

Executive Summary

This report reviews how Know Your Customer (KYC) standards – rules designed to combat criminal money laundering and terrorism financing - are applied in humanitarian cash programs. The report examines the practices of aid agencies and their processing of the personal information of aid beneficiaries for KYC purposes, and the report assesses the privacy implications of the processing of such information. The report provides a number of recommendations and guidelines in relation to the application of KYC rules and data privacy measures in humanitarian cash programs that are listed below.

With respect to the application of KYC standards to humanitarian cash programs, the report recommends that aid agencies consider the following:

- Creating specific humanitarian KYC standards, in collaboration with governments and international organizations
- Ensuring that aid agencies, rather than beneficiaries, are treated as customers by service provider for KYC purposes
- Developing simplified KYC forms for humanitarian purposes
- Limiting the disclosure of information of refugee beneficiaries
- Leveraging their status as NGOs when negotiating contracts with service providers.

With respect to the data privacy practices of aid agencies in humanitarian cash programs, the report recommends that aid agencies consider the following:

- Explicitly incorporate personal information protection principles into humanitarian KYC guidelines.
- Creating privacy policies specifically to govern beneficiary personal information
- Eliminating the use of personal information collected for KYC compliance for other, secondary purposes.
- Basing beneficiary privacy policies on the principle of notice rather than the principle of consent.
- Endorsing the principle of data minimization.
- Providing beneficiaries with a personal information protection framework and not merely the confidentiality of information.
- Requiring alternatives to biometric information collection where possible.
- Implementing strict safeguards for collected biometric information.
- Postponing inter-agency personal information sharing until such time that robust data privacy practices are in place.
- Deferring Big Data analytic initiatives until a proper Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) are completed.

CONTENTS

Introduction

The provision of cash as a form of humanitarian aid has steadily increased in popularity amongst aid recipients, aid agencies and donors over the last few years.[1] Cash based programming is thought to empower aid recipients, by offering them control over their resources, and is considered to be a more dignified and less paternalistic form of aid than the traditional provision of goods and services.[2]

However, the handling of cash and cash-like aid (such as gift cards, or electronic wallets) necessitates the consideration of issues that do not occur with the provision of goods and services, but that are known to the providers of financial services, such as money laundering concerns. The financial services industry has adopted, around the world, some version of identification and authentication standards with respect to its clients, known as Know Your Customer (KYC) standards. These standards create privacy and data protection challenges for aid agencies providing cash programs as a form of humanitarian aid.

The Privacy and Big Data Institute at Ryerson University has been commissioned by World Vision to investigate the compatibility of KYC standards with the principles of personal information protection, and to offer specific suggestions as to how aid agencies will be able to protect the personal information of aid recipients while ensuring that cash based programming is not subject to abuse.

The project undertaken by Ryerson's Privacy and Big Data Institute is one component of a larger initiative led by the UN Refugee Agency (UNHCR) together with its partners (including World Vision) in order to improve cash based programming and funded by the EU Humanitarian Aid and Civil Protection Department (ECHO) through an Enhanced Response Capacity grant.

The report which follows details our findings and recommendations with respect to KYC and data protection (DP) standards as based on aid work conducted in several large cash programs, and on conversations with the aid agencies involved. The first section of the report reviews the existing KYC standards in the relevant jurisdictions, and the second section reviews the existing DP standards as well as provides our recommendations with respect to the protection of privacy in these circumstances, which include the interest of aid agencies in sharing personal information with their partners in the provision of humanitarian cash programming.

[1] *Delivering Money. Cash Transfer Mechanisms in Emergencies*, Page vii, Paul Harvey et al, CALP, 2010, http://policy-practice.oxfam.org.uk/publications/delivering-money-cash-transfer-mechanisms-in-emergencies-112500

[2] *Cash Transfer Programs in Emergencies*, Page 6–7, Edited by Pantaleo Creti & Susanne Jaspars, Oxfam, http://policy-practice.oxfam.org.uk/publications/cash-transfer-programming-in-emergencies-115356

Major Humanitarian Cash Transfer Programs

As a preliminary step we determined the major crises that have been the recipients of cash based programs in recent years. Based on a review of information provided through the UN OCHA Financial Tracking Service (FTS) website on funding for 2014 Response Plans[3] and 2015 Regional Response Plans,[4] in particular the *Regional Refugee & Resilience Plan 2015–2016 In Response to the Syria Crisis*,[5] we determined that the Syrian Crisis[6], (which encompasses the countries of Turkey, Syria, Lebanon, Jordan, and Iraq), the Palestinian Territories, Somalia, and the Philippines received the most significant funding for cash programs.

We then researched the KYC standards and the DP standards in each of these countries, as well as whatever practices were implemented by the aid agencies that operated (or are operating) cash based programs in these regions. The results, by country, are detailed below.

Know Your Customer Standards

The Financial Action Task Force (FATF) is an inter-governmental agency that creates standards and guidelines for the international financial sector. FATF and its regional bodies monitor the implementation of these standards and guidelines by their member states. The FATF has made 40 non-binding recommendations (the FATF Recommendations) designed to assist banks and other financial institutions tackle money laundering and financing of weapons and terrorism. Know Your Customer (KYC) standards are derived from the FATF Recommendations.[7]

Countries that are members of the FATF, including Turkey, or countries that are members of one of the FATF regional bodies, such as Syria, Lebanon, Jordan, Iraq and the Philippines, and some countries that have no membership in the FATF or its regional body, such as the Palestinian Territories, have made the FATF Recommendations into law by adopting relevant legislation. Other countries, such as Somalia, that are not members of the FATF or any FATF regional body have no legislation adopting the FATF Recommendations.

Financial institutions that are based in or operate in countries that have adopted the FATF Recommendations through relevant legislation must abide by these laws. Financial institutions that are based in or operate in countries that do not have any relevant laws may have nevertheless put in place KYC standards, due to other concerns. Although the FATF Recommendations are non-binding, financial institutions that operate without any KYC standards lack international legitimacy and reputation.[8] Furthermore, the KYC standards have become an international standard that all financial institutions, and especially international financial institutions, are expected to put in place.

[3] Funding to 2014 Response Plan. UNOCHA Financial Tracking Services. http://fts.unocha.org;

[4] 2015 Response Plans. UNOCHA Financial Tracking Services http://fts.unocha.org/pageloader.aspx?page=special-2015Overview

[5] http://www.3rpsyriacrisis.org

[6] *The 2015 Strategic Response Plan (Syrian Arab Republic)* at page 5, http://www.humanitarianresponse.info/operations/syria/document/2015-syrian-arab-republic-strategic-response-plan, states that from September 2014 onwards, a regional approach was taken in response to the Syrian crisis, which meant that aid programs and funding would target the Region and specifically the countries of Syria, Lebanon, Iraq, Jordan and Turkey.

[7] *The FAFT 40 Recommendations*, October 2003, www.fatf-gafi.org/media/fatf/documents/FATF Standards - 40 Recommendations rc.pdf; *International Standards on Combating Money Laundering and Financing of Terrorism & Proliferation-The FATF Recommendations*, February 2012, www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[8] *Customer due diligence for Banks*, October 2001, Basel Committee on Banking Supervision, www.bis.org/publ/bcbs85.htm

National KYC regulation

Turkey[9], Syria[10], Lebanon[11], Jordan,[12] Iraq[13], The Palestinian Territories[14], and the Philippines[15] have enacted anti-money laundering legislation. The administration of these laws in each country is overseen by the central bank of that particular country. The central bank of each country has established rules and regulations, including those pertaining to KYC, which must be followed by certain entities based in or operating in each country. Although there are important differences among the anti-money laundering laws of each country, they are generally similar in nature. Below is a basic overview of these laws.[16]

Which entities are required to implement KYC standards under these laws?

All financial and quasi-financial entities must comply with KYC rules. The entities that must put in place KYC standards include banks, entities that issue credit/debit/bank/electronic payment cards and traveler's cheques, foreign exchange bureaus, financial intermediaries, financing entities, postal and transportation services that deal with money, investment entities and insurance entities.

Aid agencies are not included under the list of financial and quasi-financial entities that must comply with KYC rules. Therefore, they do not have any obligations with respect to KYC. However, it is likely that any entity with which the aid agency would partner in order to deliver a cash-based program (such as a bank, or a remittance service) would be subject itself to the law and be required to implement KYC standards. Aid agencies that possess the necessary infrastructure may wish to consider the possibility of operating independently as a result.

The regulated entities and their branches, agencies, representatives, commercial proxies and similar affiliated units must comply with the KYC rules in the country which they are based and in the country which they operate. For example, a Turkish bank must comply with the Turkish KYC rules when operating in Turkey. It may also be required to comply with Turkish KYC rules when operating in Syria. A Syrian bank operating in Turkey must comply with Turkish KYC rules. The Syrian bank may also be required to comply with Syrian KYC rules while operating in Turkey.

[9] *Law No. 5549 On Prevention of Laundering Proceeds of Crime*, www.masak.gov.tr/userfiles/file/Law No_5549(Amended 18_06_2014).pdf); *Regulation on measures regarding prevention of Laundering Proceeds of Crime and Financing of Terrorism*, www.masak.gov.tr/userfiles/file/ROM_amended_10_june_2014.pdf

[10] *Legislative Decree No. 33*, www.unodc.org/tldb/showDocument.do?documentUid=6370&node=docs&cmd=add&country=SYR

[11] *Law No. 318 Fighting Money Laundering*, www.sic.gov.lb/law.shtml; *Basic Circular No 83 addressed to Banks and also Financial Institutions*, www.bdl.gov.lb/circulars/index/5/33/0

[12] *Law No. (46) For the Year 2007, Anti-Money Laundering and Counter Terrorist Financing Law*, www.jsc.gov.jo/Public/english.aspx site_id=1&Lang=3&Page_Id=2360&Menu_ID2=198

[13] *Anti-Money Laundering Act of 2004*, www.cbi.iq/index.php?pid=LawsRegulations

[14] *Anti-Money Laundering Decree Law No. (9) of 2007*, www.pma.ps/Portals/1/Users/002/02/2/Legislation/Laws/Presidential_Decree_No_9_of_2007_on_Anti_Money_Laundering.pdf; *Anti-Money Laundering Instructions for Banks Operating in Palestine No (1/2009)*, The State of Palestine, National Anti-money Laundering Committee, Financial Follow-up Unit, www.ffu.ps/index.php?option=com_content&view=article&id=10&Itemid=9&lang=en

[15] R.A. No. 9160 (*Anti Money Laundering Act* (AMLA) of 2002), as amended by R.A. No. 9194 & R.A. No. 10167, www.amlc.gov.ph/archive.html; *The Revised Implementing Rules and Regulations of R.A. No. 1960, as amended by R.A. No. 9194 and R.A. No. 10167*, www.amlc.gov.ph/archive.html

[16] See also an extensive global overview prepared by PwC "Anti-money laundering know your customer quick reference. Understanding global KYC differences. January 2014.

What KYC standards must be implemented by the relevant entities?

1. Permanent Business Relationship

In general, an entity must determine the identity of its customer before establishing permanent or long-term business relations between the entity and the customer. An entity must also determine the purposes and nature of the business relationship that the customer seeks to create with the entity.

Some, but not all, of the statutes reviewed provide a definition for the "customer". Based on the definition of the "customer" and the usage of the term "customer" in the legislation, it appears that a customer is anyone who is the following: a natural or legal person who initiates or creates a business relationship with the entity; or who initiates or carries out the transaction(s); and/or the natural or legal person on whose behalf the transaction(s) is being carried; and/or the natural or legal person who will ultimately benefit from the transaction(s); and/or the natural/legal person who instructs the person to initiate or carry out the business relationship or transaction. It is a very comprehensive definition.

If the customer is a natural person, the entity will have to use either original or notarized copies of official government issued documents to determine the identity of the person by verifying the person's name, address, signature, job details, family history and nationality.

If the customer is a legal person or an unincorporated association, then the identity of the natural person(s) who has the authority to represent the incorporated company or organization or unincorporated association will have to be verified using original government issued documents or notarized copies of government documents and official documents pertaining to the company's or organization's or association's legal status and its governance structure. If the identity of the customer cannot be verified, then the entity cannot establish business relations with the customer.

It is questionable whether case based programs constitute a permanent business relationship and therefore whether the above standard is applicable to aid agencies and their partnering entities.

2. One-time/discrete transaction(s)

When a customer seeks to use the entity to carry out a single or a limited number of transaction(s), the entity must verify the identity of the customer. In some cases, the identity of the customer need only be verified if the transaction is above the monetary limit set by the relevant national authority. Some of the laws require that the identity of the customer be verified for any discrete or one-time transaction irrespective of the monetary amount of that transaction. In the one-time or discrete transaction(s) relationship between the customer and the entity, there is no ongoing or permanent business relationship.

In practice, entities follow the same KYC rules for permanent business relationships and relationships consisting of one-time/discrete transaction(s). This is the case in Syria[17] and most of the other countries.[18] Despite the Syrian practice it may be that if relatively low cash amounts are provided to each aid recipient by cash programs then these would be below the regulatory threshold, and therefore would be another reason to exempt cash programs from KYC requirements.

3. Customer Identification

An entity is required to identify the customer if an entity suspects or believes or has reason to believe that the customer may intend to or will use the entity to carry out a transaction for the purpose

[17] *Mutual Evaluation Report of the Syrian Arab Republic on Anti-Money Laundering and Combating Financing of Terrorism*, Page 61, MENAFATF, 15 November 2006,http://www.menafatf.org/TopicList.asp?cType=train_sub1

[18] PWC

of money-laundering, financing criminal or terrorist activity. The identity of the customer must be verified using the original or notarized copies of official documents and before the transaction is processed.

If the customer is a natural person, the entity will have to use either original or notarized copies of official government issued documents to determine the identity of the person by verifying the person's name, address, date of birth, place of birth, signature, job details, family history and nationality, etc.

If the customer is a legal person or an unincorporated association, then the identity of the natural person(s) who has the authority to represent the incorporated company or organization or unincorporated association will have to be verified using original government issued documents or notarized copies of government documents and official documents pertaining to the company's or organization's or association's legal status and its governance structure.

If the identity of the customer cannot be verified, then the entity cannot establish business relations with the customer or carry out any transaction(s) on behalf of the customer. Additionally, the entity may be required to report any suspicious activity to the appropriate regulatory body.

4. Monitoring, Records, and Reporting

Entities must keep records of the documents used to identify their customers, periodically update the records, regularly monitor the activities of the customer, report any suspicious activity to the relevant authority, provide reports if requested by the relevant authority, and fulfil regular reporting requirements under the applicable legislation.

5. Ultimate responsibility lies with the entity

It is the entity or entities, who establishes or facilitates or who is involved in the creation of the business relations with the customer or who facilitates or is involved in or carries out the customer's transaction, which must comply with the KYC standards. The entity must satisfy itself that the customer is not using the entity as an avenue for illegal purposes, such as money laundering for criminal activities or financing of terrorism. The KYC framework ensures that entities will be held liable for the illegal actions of their customers. Customers do not have any responsibility or obligations under the KYC rules. Their obligations originate from criminal legislation or legislation enacted for national security purposes.

Given that the responsibility and liability lies with the entities, entities may take a cautious approach and refuse to establish business relations with customers or work with intermediaries if they feel that either the dealings with a particular customer or an intermediary may be too risky or may attract unwanted scrutiny from a national regulatory. An example of this cautious approach is seen in the case of the Somalia Hawalas and Barclays bank which is explained below under the heading of Somalia. A better understanding of the KYC framework will allow aid agencies to have an informed conversation with regulated entities and ensure they are only subjected to standards that are correctly applicable.

Case in Point – Somalia

Somalia does not have national anti-money laundering legislation or any national KYC rules.[19] However, banks operating in Somalia do have KYC standards in place. For example, the International Bank of Somalia (IBS), which opened in October 2014 in Somalia,[20] has put in place KYC standards,[21]

[19] *2012 International Narcotics Control Strategy Report* (INCSR), Vol II, Page 160, Bureau of International Narcotics and Law Enforcement Affairs, March 7 2012, U.S. Department of State, www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184117.htm

[20] *Somalia's new bank seeks to spur economic growth*, Shukri Mohamed in Mogadish, December 24, 2014, http://sabahionline.com/en_GB/articles/hoa/articles/features/2014/12/24/feature-01

[21] IBS KYC Policy, www.ibsbank.so/index.php?page=page&MasterPageID=17&ID=17; IBS AML, www.ibsbank.so/index.php?page=page&MasterPageID=17&ID=18

and the Salaam Somalia Bank also has an anti-laundering and KYC policy.[22] According to the Salaam Somalia Bank KYC policy, the identity of the customer is verified using the customer's photograph, and documents proving the customer's identity and address.

The majority of financial transactions in Somalia are carried out through money transfer companies called Hawalas.[23] An individual gives a Hawala agent money to be transferred to another person. The Hawala agent then contacts its business partner located in a place close to the recipient. The Hawala agent provides the business partner with the name, address and telephone number of the recipient, the amount of the transfer, and an identification code for the transaction. The Hawala agent can transfer the money to the business partner using a bank or a courier. The business partner uses the identification code or an identification document to obtain the money from the intermediary bank or courier. The recipient then obtains the money from the business partner.[24]

Many Somalis living abroad send money to their relatives living in Somalia through Hawala. International remittances sent to Somalia require a partnership between a bank located in the country of the sender and a Somali Hawala. Many of the international banks, such as Barclays bank, are closing their accounts with Somali Hawala agents because they are concerned that the Hawala agents do not have robust KYC standards in place.[25] Barclays bank may not be able to verify the identity of the end-recipient and the purpose or nature of the remittances sent to the recipient in accordance with KYC requirements and anti-money laundering, terrorism financing laws of the countries in which Barclays bank is based or operates.

Applying KYC Standards to Humanitarian Cash Programs

The manner in which KYC standards will apply to a humanitarian cash transfer program will depend on which country the program is being implemented, the nature of the service provider(s) or entity or entities that the aid organization will use to deliver the cash payments to the aid recipients, the intermediaries or partners that the service provider may use in delivering the cash payments, the humanitarian situation that the aid organization is dealing with, any donor requirements and applicable legislation of donor countries, and also any applicable legislation of the country in which the aid agency is registered, based, or operates.

This complicated state of regulatory affairs is potentially mitigated by two overarching issues that were noted above. First, aid organizations should be able to convincingly argue that a humanitarian cash program does not create a permanent business relationship between the regulated entity and the aid recipient. Second, aid organizations should be able to argue that the amounts delivered to individual aid recipients fall below the threshold that triggers the requirement of KYC standards. As a practical matter, aid organizations should ensure that their programs are structured accordingly.

As previously noted KYC standards regulate entities and not individual customers. Aid organizations are not presently covered by the many categories of regulated entities directly. Based on the program data provided by various agencies it is clear that there are no recognized standards or guidelines for the application of KYC standards in the humanitarian context. The application of KYC standards to humanitarians program thus far has been through contractual obligations imposed by regulated entities upon aid agencies in order to ensure that the partnering commercial entity would remain

[22] http://www.salaamsombank.com/pages.php?id=16

[23] *2012 International Narcotics Control Strategy Report* (INCSR), Vol II, Page 160, Bureau of International Narcotics and Law Enforcement Affairs, March 7 2012, U.S. Department of State,http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184117.htm

[24] *Guidelines: How to use Hawala in Somalia*, Page 3, Adesco on behalf of Somalia Cash Based Response Working Group (CBRWG), https://ochanet.unocha.org/p/Documents/120311GuidelinesonHawalaFinalDraft.pdf

[25] *Remittance-dependent Somalis brace for Barclays' money transfer deadline*, Majid Ahmed in Mogadishu, August 8, 2013, http://sabahionline.com/en_GB/articles/hoa/articles/features/2013/08/08/feature-02

in compliance throughout the delivery of the cash program on behalf of the aid agency. In the contract between the regulated entity (also known as the service provider) and the aid agency, the service provider stipulates what information must be collected from the beneficiary for the purposes of KYC compliance, who is responsible for collecting that information, and what documents the service provider will accept for the purpose of verifying the beneficiary's identity. In essence, through contractual obligations imposed on the aid agency by the service provider, the aid agencies assists with or participates in specific KYC compliance as required by the service provider and based on the service provider's interpretation of the KYC rules. Below, some examples are provided to illustrate how KYC rules are applied in the humanitarian cash programs.

Case in Point – the Philippines

One of the methods used to transfer cash to aid beneficiaries in the Philippines is remittance transfers. The process for establishing a remittance transfer is as follows: the aid agency sets up an account with a remittance company, such as Western Union, or a bank. The agency provides money and recipients' information to the company or the bank. The remittance company then provides the aid agency with a tracking number specific to each recipient. The recipient can obtain his/her money from the company or bank by providing the company or bank with the tracking number and identification documents.[26]

The remittance companies and the banks differ as to the identification documents they require or accept. Generally, remittance companies in the Philippines are more flexible than the banks. For example, aid recipients had an identification card issued by the aid agency or by another NGO ("NGO ID"). Remittance companies agree to accept NGO ID cards, but the banks in the Philippines are unwilling to accept NGO ID card.[27]

The remittance companies, like the banks, in the Philippines have to comply with KYC standards. However, the Philippines government allows remittance companies to put in place less onerous KYC standards than the banks because the remittance companies are involved in low-value transactions which present a diminished risk of money laundering or other illegal activity. The simplified KYC standards require that remittance companies verify the identity of the recipient either through government-issued documents or through NGO-issued IDs.[28] Banks, on the other hand, could only accept documents issued by the Philippines government to establish the identity of the recipients.[29]

Citibank in the Philippines

In an unconditional cash grant program implemented in response to the 2012 typhoon, the aid agency partnered with Citibank to deliver cash to beneficiaries through prepaid cards. The contract between the service provider, Citibank, and the aid agency, imposed all of Citibank's KYC obligations on the aid agency. According to the contract the aid agency was responsible for the collection of beneficiary KYC-related personal information, for explaining the purpose of this collection, for ensuring the accuracy of the information, for verifying the identity of the beneficiary and for uploading the information onto a secure server provided by the service provider. The contract also stated that Citibank would not be liable to any other party for the aid agency's failure to provide accurate information.

[26] *Cash Transfer Mechanisms and Disaster Preparedness in the Philippines*, Page 16, Gregoire Poisson, CALP, 2011, www.cashlearning.org/resources/library?keywords=&region=all&country=all&year=2011&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1

[27] *Cash Transfer Mechanisms and Disaster Preparedness in the Philippines*, Page 17, Gregoire Poisson, CALP, 2011, www.cashlearning.org/resources/library?keywords=&region=all&country=all&year=2011&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1

[28] *Notes on Regulation of Branchless Banking in the Philippines*, Page 8, January 2010, CGAP, www.cgap.org/sites/default/files/CGAP-Regulation-of-Branchless-Banking-in-Philippines-Jan-2010.pdf

[29] *Cash Transfer Mechanisms and Disaster Preparedness in the Philippines*, Page 19, Gregoire Poisson, CALP, 2011, www.cashlearning.org/resources/library?keywords=&region=all&country=all&year=2011&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1

The contract did not stipulate what KYC-related information must be collected from the beneficiary, but Citibank provided a personal information form that had to be filled out by the beneficiary or by the aid agency on the beneficiary's behalf. The form listed all of the information that was required by the Philippines Central Bank to be collected for the purposes of KYC. This information includes a beneficiary's full name, date and place of birth, nationality, permanent and current address, phone and email contact details, tax identification number, social security system number, government serve insurance system number, employer name and nature of work, and source of funds. Some beneficiaries did not have all of this personal information. It is not clear whether any beneficiaries were denied benefits as a result.

All of the KYC-related personal information was passed on to the service provider. The aid agency was aware that the service provider used the information to issue prepaid cards to each beneficiary. But the aid agency did not know what the service provider did with the information once the cards were issued to the beneficiaries. The Citibank example is one in which KYC standards are rigidly applied to a humanitarian crisis with little discretion given to the aid agency, and causing difficulties in the provision of humanitarian aid.

Union Bank in the Philippines

In a different cash program, implemented in response to the 2014 typhoon, the aid agency used Union Bank, to deliver cash to beneficiaries through prepaid visa cards. Union Bank provided the aid agency with a KYC form that the beneficiary had to complete similar to the Citibank form. Beneficiaries had to provide their full name, date and place of birth, nationality, permanent and current address, phone and email contact details, tax identification number, social security system number, government serve insurance system number, employer name and nature of work, and source of funds.

However, in this instance the aid agency recognized that the beneficiary was not creating a permanent or temporary business relationship with the service provider. As a result, the aid agency requested that the service provider allow the beneficiary to put the aid agency's name under the source of funds. The service provider did accommodate the aid agency's request. The aid agency used a government issued ID to verify the beneficiary's identity if the beneficiary had a government issued ID or an official certificate or an ID issued by the aid agency.

The Philippines Central Bank had produced a list containing documents that can be used by service providers to verify a customer's identification for the purposes of KYC. To facilitate humanitarian work in response to disasters, the Philippines Central Bank relaxed some of the requirements for KYC compliance.[30] They extended the list of documents that were acceptable for use in verifying the identity of the beneficiary. The extended list of documents included ID created by an aid agency. Additionally, the service provider could rely on the basic beneficiary information, such as name and address or date of birth, to issue the payment instrument to the beneficiary so long as the aid agency provided the remainder of the beneficiary personal information within a limited time period.[31] The aid agency was aware that the service provider used the information to generate the prepaid cards and also that the service provider retained the information for a number of years.

Case in Point – Haiti

In Haiti, the Haitian government modified some of its KYC standards so that humanitarian cash programs could be delivered to those affected by the 2010 earthquake through mobile wallets. The mobile wallets were based on a bank model, which involved a partnership between a bank and a

[30] *Electronic Transfers Scoping Study and Preparedness Plan*, Page 12, Gabrielle Smith, ACF Philippines, December 2013, www.actionagainsthunger.org/publication/2013/12/electronic-transfers-scoping-study-and-preparedness-plan-acf-phillipines

[31] *Electronic Transfers Scoping Study and Preparedness Plan*, Gabrielle Smith, ACF Philippines, December 2013, www.actionagainsthunger.org/publication/2013/12/electronic-transfers-scoping-study-and-preparedness-plan-acf-phillipines

mobile network operator (MNO).[32] The aid agency partnered with Unibank and two MNOs, Digicel and Voila, to deliver cash to beneficiaries using the beneficiaries' mobile phones.

In this case, the aid agency set up a bank account with Unibank. The bank transferred money into the aid agency's bank account. The money in the aid agency's bank account was transferred to beneficiaries as electronic money into their electronic wallet accounts that were set up on their mobile networks. Once the transfer was made, the beneficiary's MNO sent the beneficiary a text message notifying the beneficiary that the money was available. The beneficiary could then use the electronic money for goods/services where electronic money was accepted or convert the electronic money into cash. The recipient could also go to the nearest bank agent, typically located in a post office or a store, and withdraw the electronic money as cash. The electronic wallet was debited or credited as soon as the transaction took place.[33]

In Haiti, much like in the Philippines, the Haitian Central Bank had relaxed KYC rules to facilitate humanitarian work for those affected by the earthquake. The relaxation of the KYC rules provided the impetus for the service providers to relax their own KYC measures. Under the simplified Haiti KYC standards, the aid recipient did not have to provide any additional identification documents or fill out any KYC forms for an electronic wallet with a limit of 4,000 HTG (~85 USD). The MNO used the information the aid recipient had already provided when s/he obtained a SIM card, which included a photo ID and address. If the aid recipient wanted an electronic wallet with a limit of 10,000 HTG (~215 USD), then s/he had to fill out a form and provide a government approved ID and address at a bank branch, MNO outlet or bank agent.[34]

On the KYC form, the beneficiaries had to provider their full name, date and place of birth, type, number, and expiration date of government issued ID, mother's maiden name, address, copy of the government issued ID, and mobile number. In some cases, the aid agency could not comply with the KYC requirements because some beneficiaries did not have government issued IDs or some beneficiaries were illiterate and could not fill out the KYC forms and sign them. The aid agency requested that the KYC requirements be altered. One of the MNOs was granted permission by Unibank to accept aid agency issued ID instead of government issued IDs. The other MNO allowed the aid agency to fill out the KYC form for beneficiaries who were illiterate so long as the aid agency provided a letter stating that the personnel assisting the beneficiary with the KYC form was the aid agency's employee.

KYC Recommendations

Minimizing Information Collection and Disclosure while Meeting KYC Standards

Governments have shown a willingness to take a balanced approach to regulation of money laundering, particularly in a humanitarian crisis situation. Governments are willing to modify KYC standards and create tiered-KYC measures to ensure that people's needs are met.

The Philippines and Haiti examples indicate that aid agencies should conduct preliminary inquiries before entering into a contract with an entity to deliver humanitarian cash benefits. Agencies should ensure of course that entities do not appear on any government's terrorism financing or money

[32] Innovation in emergencies: the launch of mobile money in Haiti. Kokoévi Sossouvi. Humanitarian Exchange Magazine. Issue 54 May 2012. www.odihpn.org/humanitarian-exchange-magazine/issue-54/innovation-in-emergencies-the-launch-of-mobile-money-in-haiti

[33] Innovation in emergencies: the launch of mobile money in Haiti. Kokoévi Sossouvi. Humanitarian Exchange Magazine. Issue 54 May 2012. www.odihpn.org/humanitarian-exchange-magazine/issue-54/innovation-in-emergencies-the-launch-of-mobile-money-in-haiti

[34] *E-Transfers in Emergencies: Implementation support Guidelines*, Page 49, Kokoévi Sossouvi, CALP, www.cmamforum.org/search?q=calp&go=Go

laundering list[35] but also the degree to which the entity is required to comply with anti-money laundering regulations and KYC standards, and whether it has any flexibility in the application of the standards.[36]

In general, KYC identification standards require the name, the date of birth, the contact information (address and telephone number) as proof of the identity of the customer.[37] Depending on the humanitarian situation it may not be possible for aid recipients to provide such documentation. As seen above, natural disasters, for example, may eliminate the ability to verify contact information. The aid agency could then, depending on the humanitarian situation it is working in, give the entity a list of documents that the aid recipient could produce. If that documentation does not fully meet KYC standards then the aid agency could ask the entity, or the government, for a relaxation of the KYC standards for the particular program or humanitarian situation.[38]

Recommendation – Special Humanitarian KYC Standards

Aid agencies should work with governments and with the FATF to create tiered-KYC standards specifically applicable to humanitarian situations.

The creation of tiered standards would provide the opportunity to introduce new forms of identification that would incorporate both the humanitarian context as well as technological developments.

The examples above show that the initial KYC measures stipulated by service providers were not applicable in the specific humanitarian context. Anti-money laundering laws require the regulated entity to deny services to anyone whose identity and information cannot be verified using valid documents, yet in the Philippines and Haiti it was impossible to verify the identity and information of each beneficiary because some of them did not have all of the information required by the service provider's KYC forms, or did not have official government issued IDs, or did not have proficient literacy skills to complete the KYC forms on their own.

All parties – aid agencies, service providers and governments recognized that KYC rules had to be modified. Since the ultimate responsibility for compliance with anti-money laundering laws and the risks and liabilities of failure to comply with these laws lies with the service provider, the service provider will not, as seen from the Philippines and Haiti examples, relax their KYC compliance measures simply because they are operating in the humanitarian context unless governments have allowed service providers to relax their KYC measures; and it is evident that a specific set of KYC measures should apply in the humanitarian context that are different from non-humanitarian context.

Governments showed a willingness to take a balanced approach to the regulation of money laundering. They were willing to modify or relax KYC standards to ensure that humanitarian needs were met. If the KYC measures had not been modified, they would have hindered and prevented the delivery of aid to beneficiaries.

Aid agencies should initiate dialogue or continue dialogue with governments and service providers to push for KYC rules applicable to the humanitarian context. In order to do this, the aid agencies should have a thorough understanding of anti-money laundering laws and the particular KYC rules so that they can have informed conversation with governments and service providers about the challenges of applying KYC rules that are not conducive to the delivery of humanitarian cash programs but rather hinder the delivery of such programs.

35 E-Transfers in Emergencies: Implementation support Guidelines, Kokevi Sossouvi, CALP, www.cmamforum.org/search?q=calp&go=Go

36 *Cash Transfer Mechanisms and Disaster Preparedness in the Philippines*, Gregoire Poisson, CALP, 2011, www.cashlearning.org/resources/library?keywords=&region=all&country=all&year=2011&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1

37 E-Transfers in Emergencies: Implementation support Guidelines, Kokevi Sossouvi, CALP, www.cmamforum.org/search?q=calp&go=Go

38 E-Transfers in Emergencies: Implementation support Guidelines, Kokevi Sossouvi, CALP, www.cmamforum.org/search?q=calp&go=Go

Recommendation – the Aid Agency as Customer

Beneficiaries should not be listed or treated as "customers" for the purposes of KYC standards.

As noted above at least one of the aid agencies in the Philippines recognized that the aid agency was not contracting the service provider to initiate and facilitate either temporary or long-term business or customer relationships between the service provider and the beneficiaries. The aid agency was contracting the service provider to assist the aid agency in delivering aid to beneficiaries and, therefore, it was appropriate to put the name of aid agency and the humanitarian cash program under the title 'source of funds' on the KYC form. This was done once the aid agency had received approval from the service provider.

Aid agencies should point out during negotiation of contracts with service providers that the purpose of anti-money laundering laws is to prevent the use of service providers/regulated entity as a conduit for money laundering, or financing of terrorism or other crimes. The purpose of the KYC rules is to identify the nature of the customer's transaction(s), which is done through verification of the customer's identity, the customer's source of funds, etc.

In the non-humanitarian business context, the anti-money laundering laws either explicitly or implicitly define the customer. In the humanitarian context, the beneficiary does not approach the service provider to establish temporary or permanent business relationship. The aid agency contracts the service provider. There is a business relationship between the aid agency and the service provider. The aid agency provides the funds and the service provider facilitates the distribution of those funds. The beneficiaries, selected by the aid agency, receive the funds through the service provider that the aid agency had chosen.

From the information available it seems that if beneficiaries had any problems with either receiving the funds or using the funds then they approached the aid agency and not the service provider. *There was no contractual or any other relationship between the service provider and the beneficiary*.

Recommendation – A Simple KYC Form

Aid agencies should create their own KYC forms that would collect less personal beneficiary information.

In the humanitarian cash programs, aid agencies use service providers to deliver aid. *The nature and purpose of the "transactions" and the source of funds are already known*. There is no doubt as to why the service provider is engaged by the aid agency. In recognition of the fact that it is the aid agency that initiates and maintains a relationship with the service provider, the aid agency should play a lead role in creating a KYC form that collects minimal personal beneficiary information. By using a KYC form created by the aid agency, the aid agency has greater control over determining the appropriate KYC measures to be implemented and has greater control over what information is passed on to the service provider.

In practice, this could mean that only the name and address and an aid agency issued ID of the beneficiary may be required on the KYC form that is passed on to the service provider, and that the KYC form could be filled out by the agency staff on behalf of (potentially illiterate) beneficiaries without the need for any additional letters confirming who completed the KYC form. The form that would be created would depend on the country in which the cash program is to be delivered, the particular humanitarian situation, and the position of the government. Some items that could be eliminated from the Philippines KYC form for example may include employment related information and the source of funds. The aid agency might consider having its own internal KYC form that it could use to collect relevant information to identify and verify the identity of the beneficiaries the agency has selected to participate in the cash program.

Recommendation – Limit Disclosure of Refugee Information

Aid agencies should not disclose the personal information of refugees to governments that may be using KYC standards as a pretext.

Refugees have grave concerns about providing their information to agencies because they are afraid that the government or group that they are fleeing from could access their information. However, refugees are then caught in a "Catch-22" situation because they cannot access aid services unless they are registered as refugees. Generally, aid agencies try to reassure the refugees that their information will not be shared with governments or organizations of concern to the refugees. Aid agencies should be vigilant that governments are not using KYC standards as a pretext to demand disclosure of refugee information.

All beneficiaries are vulnerable and do not voluntarily seek aid or the services of the service provider. Beneficiaries, and refugees in particular, have no other choice. Maintaining greater control over the information that is disclosed to service providers and through them to government will allow refugees to maintain their dignity and ensure that it is not eroded further by participation in the cash program. Ultimately, limiting disclosure of refugee information promotes not only their dignity but their personal safety and security.

Recommendation – Leverage NGO Status

The status of aid agencies as agencies providing aid and the status of these cash programs as programs providing aid, is an important consideration that should be leveraged by the aid agencies when negotiating contracts with service providers.

One of the reasons why aid agencies do not necessarily have to assist the service provider in anti-money laundering regulatory compliance may be because of the protections provided by status of the aid agencies. UN agencies are protected by immunity laws which, for the purposes of cash programs, may mean that they do not have to release information to governments.[39] They do not have to pass on information to service providers that the service provider could potentially pass on to the government. Service providers are required to produce information to governments when requested to show that they are in compliance with anti-money laundering legislation. In the contract between the service provider and some UN aid agencies, the service provider is required to notify the agency when the government has made a request for information. The aid agency then uses its diplomatic channels to address the request.

In cash programs delivered by aid agencies that fall under the umbrella of the United Nations (UN) to beneficiaries who are refugees it is made clear from the outset that there is a business relationship between the aid agency and the service provider. The aid agency opens an account with the service provider. The account is under the aid agency's name. The aid agency gives the service provider a case number that is assigned to each beneficiary. The information that links the case number and the identity of the beneficiary is retained by the aid agency. If a product, such as a prepaid card, is being used by the aid agency, the card will contain the case number of the beneficiary. The personal information that links the case number and the identity of the beneficiary is retrained by the aid agency and is not passed on to the service provider. If cash was distributed through mobile money, the phone and the SIM card were taken out in the aid agency's name and not the beneficiary's name.

The responsibility of identifying the beneficiary and verifying the beneficiary is placed on the aid agency, but not necessarily for the purpose of complying with KYC rules but for the purpose of registering the refugees and providing the cash aid to the refugees. Many of the refugees may not

[39] We have not been able to independently confirm this opinion provided by one of the aid agencies.

have government issued identification documents and aid agencies are increasingly using biometrics, such as iris scans and fingerprints, for identification purposes (see more on biometrics below).

Service providers are not always satisfied with just the beneficiary's case number; they are interested in and sometimes insist on obtaining beneficiaries' identification information. The aid agencies do generally resist such efforts by the service providers. In these instances, it is the aid agency that is dictating what beneficiary information will be provided to the service provider and the aid agency can limit the amount of beneficiary information that is passed on to the service provider. The aid agencies, in these cases, fully understand that it is the service providers' responsibility to comply with KYC rules and that the aid agencies do not have to oblige all of the service providers' information requests under the guise of regulatory compliance. The aid agencies and the service providers are on a more equal footing that in the examples provided above.

Data Privacy

Data privacy, or personal information protection is an increasingly important aspect of privacy, as the capacity of corporations and governments to collect, use, disclose and retain data continues to grow. Regardless of specific interpretation or manner of implementation, personal information protection sets out to accomplish two functions. First, to establish and confer broad rights on individuals, or data subjects, with respect to the collection, use and disclosure of their personal information by other parties. Second, to set out broad responsibilities and obligations of organizations with respect to the collection, use and disclosure of personal information held in their custody.

The first function is commonly known as *information privacy*: the right or ability of individuals to exercise a measure of control over the collection, use and disclosure of their personal information by others. The second is *data protection*: the responsibility of organizations that collect, use, and disclose personal information to abide by an externally established set of rules. It is important to understand the distinction between the two functions. The first approaches privacy from the perspective of the individual data subject, the second from the perspective of the custodial organization.

Many organizations mistakenly believe that personal information is limited to basic "tombstone" data provided directly by the individual such as name, address, phone number, socioeconomic details and so forth. Although statutory definitions vary around the world, personal information can include far more than this, such as any information associated or linked to an identifiable individual (e.g., personal preferences, beliefs, opinions, habits, family and friends); physical and biological attributes (photo images, genetic data); account numbers and any unique identifiers associated with an individual, commercial data (record of sales, customer service requests, returns logins, phone calls), information about an individual provided by third parties (credit reports, employment references), information inferred, derived, or generated from data held about an individual and information generated by devices registered to an individual (phone numbers, computer logins, location data)

The breadth of such information explains why personal information protection is considered essential for the autonomy of individuals and the ability of human beings to define themselves and their sense of identity, as well as their dignity, reputation and freedom from government.

National Data Protection Regulation

In most of the jurisdictions that hosted humanitarian cash programs in recent years there is very little personal information protection. Turkey, Syria, Lebanon, Jordan, Iraq, the Palestinian Territories and Somalia have not enacted national data privacy laws. However, in some of these countries, data privacy is protected through other laws.

Turkey

Turkey has not enacted any data privacy legislation but privacy is partially protected under the Turkish Constitution and various criminal and civil laws.

Article 20 of the Turkish Constitution states that individuals have the right to know whether information is collected about them and for what purposes, to know whether the information is being used for the stated purpose, to know where the information is stored, and to access the information. The Article further states that personal information collected about individuals cannot be processed without their consent unless permitted by law.

Under the Turkish Criminal Code, information about a person's political, philosophical or religious opinion, ethnicity, sexuality, medical history or affiliation with a trade union cannot be collected or shared or retain unless permitted by law and cannot be retain for a period longer than permitted by law.[40]

Iraq

There is no Iraqi data privacy legislation but Article 17(1) of the Constitution of Iraq states that, "each individual has the right to personal privacy, as long as it does not infringe on the rights of others or public decency." Personal privacy is an aspect of privacy distinct from personal information protection, and usually refers to physical privacy, in a person's body as well as their dwelling.

Somalia

The African Union (AU) adopted the African Union Convention on Cyber Security and Personal Data Protection (the Convention) on July 27, 2014. Somalia is a member of the AU. It has not yet implemented the Convention and, therefore, the Convention does not have any legal force in Somalia. Nevertheless, the Convention does provide a template for the legal framework for data privacy laws that may eventually be implemented in the country.

Non-profit organizations (NGOs) of a religious, philosophical or political nature that collect or store data of its members are exempt from the personal data protection obligations under the Convention so long as the NGOs do not share the information they have collected with a third party and the information collected is consistent with the objectives of the NGOs.

Sensitive information, such as biometric information or health data cannot be collected without the consent or permission from the appropriate regulatory body. On the other hand, other personal information may be collected without a person's consent if the data is collected to fulfill a legal obligation, or for public or state interest, or for the protection of the rights and freedoms of the individual.[41]

The person whose data is being collected has the right to know what information has been collected about him/her, the right to access the information that has been collected or stored, the right to

[40] *Global Data Privacy. Directory*, Page 85–86, Norton Rose Fulbright. July 2014, www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf

[41] Article 14(2)(j) of the *Convention*.

refuse the collection of his/her information, and the right to request that the information collected or stored be erased.[42]

Data that has been collected in an AU member state cannot be transported to a non-AU member state unless that state has robust data privacy protection laws.[43] The data that has been collected must be kept confidential, in a secure manner, and only for a limited amount of time.[44]

The Philippines

The Philippines is one of the few surveyed jurisdictions with data protection legislation. It has enacted The *Data Privacy Act of 2012 (the Act)*.[45] The *Act* applies to personal information of Philippines citizens or residents located anywhere in the world.[46] The *Act* does not exclude NGOs, so normally NGOs are expected to comply with the protective measures the *Act* establishes. The *Act*, however, does not apply to information collected under anti-money laundering laws.[47] It therefore permits the collection of information for KYC purposes regardless of the protections it otherwise offers and that are listed in this section.

According to the *Act* personal information can only be collected for a stated purpose, can only be retained for a limited time,[48] and the information must be stored securely.[49] Consent is required for the collection of personal information unless the information is collected to fulfill a legal obligation or government function, to protect a person's freedom and rights, or public order and safety;[50] Consent is always required for the collection of sensitive information.[51]

An individual whose information has been collected does have the right to know the purpose for which it was collected, has the right to access the information collected, has the right to withdraw consent, and has the right to request that the data be deleted.[52]

Anti-laundering Legislation and Data Privacy

All the anti-money laundering statutes mentioned above give national regulators the right to access information collected under KYC standards. Entities subject to the legislation must also report any suspicious activity and details about the customer involved in the suspicious activity. Furthermore, the entity cannot inform the customer that s/he or it has been reported to the relevant authority for suspicious activity.

The Philippines *Act*, the AU *Convention*, and other privacy laws in general either explicitly or implicitly state that personal data of individuals may be collected for national interest purposes without consent. As mentioned above the Philippines Act explicitly states that privacy protections found under the law are not extended to personal information collected under KYC standards.

NGOs that collect KYC information about the beneficiaries of humanitarian cash programs could therefore be required to hand over that information to the appropriate regulatory authority for compliance with anti-laundering or similar legislation or if an investigation into money laundering or

42 Article 16–19 of the *Convention*.
43 Article 14(6) of the *Convention*.
44 Article 20–23 of the *Convention*.
45 www.gov.ph/2012/08/15/republic-act-no-10173/
46 Section 6 of the *Act*.
47 Section 4 of the *Act*.
48 Section 11 of the *Act*.
49 Section 20 of the *Act*.
50 Section 12 of the *Act*.
51 Section 13 of the *Act*.
52 Section 16 of the *Act*.

terrorism financing or other illicit activity is conducted. The personal data would not be protected by the measures that data protection legislation would offer in other contexts.

Donor Requirements and Data Privacy

Donors, in accordance with the laws of their countries, may require that aid agencies hand over beneficiary information to the donors. Donors may then be required to give that information to authorities in their home countries.

Case in Point – the United States

The American government will not give aid funding to any aid agency that may pose a threat to the American government. Before an aid agency can receive American government funding, it must go through the U.S. Agency for International Development's (USAID) Partner Vetting System (PVS) and the U.S. Department of State's (State Department) Risk Analysis and Management (RAM) vetting system.

The PVS and the RAM processes require that aid agencies seeking USAID or State Department aid grants/funding must provide personal information to the US government about their employees as well as the employees of their partners, contractors, sub-contractors employees and anyone else involved in the delivery of the programs. The US government will then use the information to confirm whether any of the personnel of the various entities appears on the US government's lists for terrorists or other blacklists.[53]

Some of the information that would be provided to the US government under the PVS and RAM systems includes an individual's name, government issued photo ID, the ID number, any passport number, gender, place of birth and contact information such as address, email and telephone numbers.[54] The American systems violate the privacy laws and principles of data privacy of other countries.[55] These systems could be extended to beneficiary information as well.

Biometrics

As discussed above meeting KYC standards for identification in a humanitarian context is challenging, while identification and authentication requirements are steadily increasing due to national security, transparency and accountability concerns. Generally, identification can be based on something a person *knows* (e.g., a password), something a person *has* (e.g., a benefit card) or something a person *is* – a biometric.

The biometric is increasingly viewed as the ultimate form of identification. Accordingly, it is being rolled out in many applications that require a high level of confidence in identity assurance. In fact, the biometric is rapidly becoming the underpinning of national ID or other ID approaches in countries that lack robust identity registration systems.[56]

Biometric technologies present many benefits, such as stronger user authentication, greater user convenience and improved security and operational efficiencies. However, biometric technologies also present certain risks that organizations should carefully take into account, including risks associated

[53] *Implications of the USAID Partner Vetting System and State Department Risk Analysis and Management System under European Union and United Kingdom Data Protection and Privacy Law*, Counterterrorism and Humanitarian Engagement Project, Page 1, Neal Cohen, Robert Hasty, Ashley Winton, Research and Policy Paper, March 2014, http://blogs.law.harvard.edu/cheproject/research/

[54] *Implications of the USAID Partner Vetting System and State Department Risk Analysis and Management System under European Union and United Kingdom Data Protection and Privacy Law*, Counterterrorism and Humanitarian Engagement Project, Page 1, Neal Cohen, Robert Hasty, Ashley Winton, Research and Policy Paper, March 2014, http://blogs.law.harvard.edu/cheproject/research/

[55] *Ibid*.

[56] A Gelb Center for Global Development – Unique ID in Development and Social Programs. World Bank Pensions Core Course, 2014

with inadequate privacy protection that may cause loss of public support. Biometric technologies provide a powerful unique identifier that can be used inter-operably to compile a profile of an individual without his/her knowledge – otherwise known as unauthorized secondary uses.

Biometric identification requires the comparison of a biometric of an individual against samples stored in an existing biometric database. This process is also known as a *one-to-many match*, and is used by police to identify criminals, by social service agencies to identify qualified beneficiaries, by transportation licensing authorities to issue driver's licenses, to name a few common uses. The global privacy and data protection community have consistently argued against the use of biometrics for most one-to-many identification purposes, and against the creation of large, centralized or interoperable databases of biometric data.[57]

Case in Point – Lebanon

Biometric identifiers were used and stored in databases for several aid programs for Syrian refugees in camps in Lebanon as well as in the Kakuma refugee camp in Kenya in 2003 and the Mbera camp in Mauritania in 2013. The biometric data was stored on centralized databases accessible by aid agencies and governments. Tellingly, refugees raised concerns that governments may have access to their data. The Syrian refugees were concerned that the Lebanese government would give their information to the Syrian government from which they fled. Refugees questioned the need for multiple aid agencies and the government to have access to the information. These concerns highlight the important values that personal information protection serves – such as the value of liberty, or freedom from government, which is of extreme importance when aid agencies assist refugees in war-torn areas.

In contrast, privacy advocates have called for the use of biometrics mainly in verification systems, where a live biometric is compared to a previously stored sample (on a card, or a mobile phone), and the eligibility of the potential beneficiary has already been established by other means. The matching of the biometric is all that is necessary to verify that the person is who he/she purports to be. Such use of biometrics does not require a biometrics database, and is known as a *one-to-one match*. The simplest example is the use of fingerprint ink to identify voters around the world.

Humanitarian Data Protection Policies and Practices

Many aid agencies have privacy policies that protect the privacy rights of their donors, their employees, their partners, other stakeholders in their home countries. These policies do not in general discuss the data privacy of aid beneficiaries or the personal information protection measures that aid agencies, located outside of the agencies' home countries, should implement in relation to beneficiary personal data.

At present, it seems that there are no standard or recognized humanitarian data protection policies that are being used by aid agencies to protect the data privacy of aid beneficiaries. Instead, aid agencies seem to be relying heavily on the contract between the agencies and the service providers to define the purpose of the collection, use and disclosure of data, to collect, use and disclose data for purposes that fall outside of the contract, and to protect the collected data from inappropriate use or disclosure. The contract, and in particular the confidentiality clause in the contract, seem to operate as the *de-facto* privacy policy or the aid agencies' understanding of privacy.

[57] For example the French Data Protection Authority (CNIL) laid down four key criteria to be used when examining biometrics: (1) the use of biometric systems should be limited to the purpose of controlling access by a limited number of people to a zone with high security risks; (2) biometric systems should be proportionate to the purposes and the risks; (3) they should guarantee both the effective identification or authentication of individuals and the security of personal data; and (4) appropriate notice must be provided to individuals in compliance with French privacy and labor law.

The need for privacy policies is particularly critical for cash programs implemented among refugee beneficiaries. Refugees have expressed grave concerns about the collection, use and sharing of their personal information. They fear that their information will be shared with those who may have been persecuting them and caused them to flee their home country. Ensuring that aid agency staff understand the notion of privacy, operate under sound data privacy principles, and are able to explain the parameters of collection, use and disclosure of refugee personal information may assist the refugees and alleviate their concerns. Below are some examples, provided to illustrate the practice of data privacy and information protection in cash programs in general and with respect to refugee beneficiaries specifically.

Case in Point – the Philippines

The Philippines is the only country surveyed which had in force personal information protection legislation. Despite that, the examples below reveal little awareness of the law or its requirements.

Citibank in the Philippines

The aid agency's staff assisted beneficiaries in completing the service provider's KYC form. Before completing the forms, the beneficiaries were told that the information was collected for regulatory compliance purposes and to allow Citibank to issue the cards. The completed form was given to Citibank by the lead staff member of the aid agency's cash program; a copy of the form or the information contained on the form was also retained by the aid agency for "audit" purposes as hard copies and in electronic format on the aid agency's computers.

Although the aid agency understood that they were disclosing the information to the service provider and no one else, they did not know what the service provider did with the beneficiary information or whether the service provider shared that information with another party. The aid agency presumed that the service provider did not share the information with another party because the aid agency and the service provider were required to keep beneficiary personal information confidential under the contract between the service provider and the aid agency. The aid agency was satisfied that, so long as they followed their confidentiality obligations under the service provider contract, i.e. they ensured that they did not share the information with anyone other than the service provider, their data collection practices were sufficient; they did not consider additional privacy issues. Furthermore, the aid agency did not have any privacy policy in place that it could follow when collecting or disclosing beneficiary personal information. The aid agency was not aware of the Philippines privacy legislation that it may have been required to follow.

Union Bank in the Philippines

As in the example above, the aid agency told the beneficiaries that the information was collected for regulatory compliance purposes before completing the service provider's KYC forms. The completed KYC form was given to the service provider and the aid agency understood that the form would be retained by the service provider for certain number of years. The agency did not retain a copy of the KYC form. Rather, the agency had its own form that it used to collect beneficiary personal information. Some of the beneficiary personal information that was collected using the agency's form included, full names and date of births of the head of the household and all the members of the household, the head of household's and any other family members' source of income, and marital and health status of each member of the household.

The aid agency did not have any privacy policies in place that it could follow in relation to collecting or disclosing beneficiary personal information. Nor was the aid agency aware of the Philippines privacy legislation. The aid agency understood that, so long as they ensured that they did not share

the information with anyone other than the service provider, their data collection practices were sufficient. They ensured that they did not share the information with third parties by personally delivering or delivering via courier the KYC forms to the service provider and by numbering each KYC form so that the form could not be duplicated by anyone other than the aid agency.

Case in Point – Haiti

The aid agency that worked with Unibank and Mobile Network Operators (MNOs) in Haiti collected, in addition to collecting the KYC information required by the MNOs' KYC forms, beneficiary personal information using a web-based mobile application to generate identification cards. The beneficiary personal information that was collected included the members of each household, their names, address, position within the household, the GPS coordinates of their place of residence, their medical needs, gender and date of birth. The collected information was stored in password protected files on a database that was accessible to the MNOs.

Before collecting the beneficiary personal information, the aid agency decided to obtain consent from each beneficiary (or household head) for the collection and use of that information. Other than the requirement of beneficiary consent, the aid agency did not follow any privacy policies or look at any national privacy law requirements prior to the collection, use or disclosure of beneficiary personal information. The aid agency understood that the confidentiality clause in the contract between the aid agency and the service provider was sufficient to protect the privacy of the beneficiary personal information. The contract clause generally stated that all parties to the contract were required to preserve the confidentiality of any information generated during the term of and for the purpose of fulfilling the contract unless they were requested to disclose information for legal or state purposes; the party who received a request to disclose information from the state or a legal authority was required to inform the other parties of such a request.

Case in Point – the Democratic Republic of Congo (DRC)[58]

The aid agency and the service provider (Vodacom) collected the following information from the beneficiary: full name, age, gender, date of birth, number of official identification documentation. The aid agency also collected the account number that the service provider assigned to each beneficiary in order to transfer money into the beneficiary's account. The beneficiaries were told by the aid agency that their information was collected by the service provider in order to generate their accounts and facilitate their payments.

The aid agency collected the information from the beneficiaries by requiring the beneficiaries to complete paper forms. This information was transferred to excel sheets by the aid agency. The electronic files containing this information were password protected; the computers on which the electronic files were stored were also password protected. Additionally, the contract between the aid agency and the service provider required all parties to implement measures to protect and secure beneficiary personal data, ensure that the information was not passed onto any third parties, and to use the information for fulfilling its obligations under the contract and for no other purposes.

Case in Point – Jordan

UNRWA and ATM Cards

UNRWA entered into a contract with a service provider for ATM cards for Palestinian refugees who fled from Syria into Jordan. UNRWA did not collect any KYC-related information on behalf of the service

[58] Although the DRC was not one of the major cash aid countries in the years we surveyed we include this example to demonstrate the pattern followed by aid agencies.

provider and the service provider did not, on its own behalf, collect any KYC-related information. But UNRWA did collect beneficiary personal information to create UNRWA identification cards and to complete a household vulnerability assessment.

The information collected included household composition, name, age, gender, date of birth, nationality held of the members of the household, the date and point of arrival for households, the household's access to healthcare and education, the household's shelter conditions, and the household's ability to meet its expenses. This information was collected by UNRWA staff by filling out paper surveys or by entering the information into the electronic survey stored on UNRWA's intranet.

UNRWA deployed several security measures with respect to this information. Only a certain number of staff could access the electronic survey at any one time. The paper surveys were stored in locked cabinets in the field offices, to be destroyed once the assessments were completed, and the electronic surveys and excel charts created using the information from the surveys were stored on restricted access drives located on firewall protected servers.

The beneficiary personal information that UNRWA did collect was not shared with another party. UNRWA's general policy is to not release beneficiary personal information to anyone or any entity outside the agency in order to decrease their vulnerability to persecution, violence and refoulement. This general policy is adapted to local situations, which means that greater restrictions could be applied to any disclosure depending on the circumstance. UNRWA does provide beneficiary personal information in an anonymized and aggregate form to others for reporting and assessment purposes.

Cairo Amman Bank Prepaid Cards

An aid agency entered into a contract with a service provider for prepaid cards for Syrian refugees that fled to Jordan. Initially, the aid agency collected and passed on KYC-related information to the service provider. The aid agency kept a copy of this information for program monitoring and to ensure that payments were processed and made. Prior to and during the collection, the refugee beneficiaries were verbally told that this information was collected and shared in order to generate their prepaid cards and facilitate their payments. Flyers explaining the purposes of the data collection and use were also sent to the beneficiaries' homes. The aid agency was no longer required to collect KYC-related information when they began using beneficiary information that had been collected and verified by UNHCR.

The information collected from the beneficiaries was also shared with the Jordanian Ministry of Planning and International Cooperation, not for the purpose of the implementation of the cash program, but for the purpose of registering the refugees. Registering the refugees with the Jordanian government allowed the refugees to access Jordanian social services and banking privileges.

The aid agency did not have its own privacy policy that could have guided the agency's collection, use or disclosure of beneficial personal information. Nor did the aid agency consider whether there were any national privacy laws that the agency may have been required to follow.

However, the agency's general practice was to store the collected beneficiary information on a password protected excel sheet which was accessible by the cash program's project manager, the aid agency's IT Officer and the service provider staff member responsible for the cash payments. The information was also stored on a password protected database. Only the project manager could access all the information on the database for the purpose of facilitating assessment site visits. Staff members organizing the assessment visits could see the aid agency's case number, address and phone number for a particular household/beneficiary. Furthermore, the information was shared with UNHCR, to ensure that both aid agencies were not duplicating services to the same household/beneficiary, and with the aid agency's "network", to facilitate the provision of any additional services that the household/beneficiary may be entitled to receive.

Informed Consent and Personal Beneficiary Data

Based on the practices of the aid agencies in the examples provided above, it seems that aid agencies do not in general operate on the principle of informed consent. There seems to be an implicit understanding among the aid agency staff that beneficiaries cannot truly consent to the collection, use, disclosure and generally the processing of their personal information.

Indeed, the purpose of cash programs is to assist individuals, affected by humanitarian disasters or crises, allow them to regain control and power over their lives, maintain their dignity and preserve their ability to control their lives and choose according to their needs.[59] As noted above, the purpose of data privacy laws is to preserve individual autonomy. A data protection regime provides individuals with the ability to decide what happens to their personal data. Individuals have control over their personal information and exercise control through meaningful choices. Autonomy, Liberty and Dignity are the core values.[60]

Choice over the processing of personal information and control of information are expressed through agreements. Individuals agree, or not, to the processing of their information, by indicating their consent (or lack thereof). In order for an organization to be able to rely on consent (or on evidence of consent, such as a signed document) it must be voluntary, free and informed. As a concept, consent is applicable to private sector transactions, between members of society (whether individuals, corporations or NGOs). It is less applicable when the processing of personal information is done for a legal or regulatory purpose by government. Governments are typically required to notify individuals about such processing, to ensure transparency and accountability, but the consent of individuals is not actually required, and data protection legislation will typically exempt such activities from the requirement to obtain consent.

Informed consent may very well therefore not be an appropriate principle for humanitarian cash programs to base their policies and practices for several reasons. First, the collection and processing of personal information for KYC standards and in order to comply with legal obligations is typically exempt from data protection provisions. A number of aid agencies in the examples above did not considered it necessary to ask the beneficiaries to consent to the collection of their person information for KYC purposes. It was understood by aid agency staff that the beneficiary had to provide that information to the service provider for KYC compliance purposes. The aid agencies explained to the beneficiaries the purpose of the collection of the information and the use of that information, but did not ask for beneficiary consent.

Second, the principle of consent may be more applicable in situations where the collection of personal information is for other purposes, such as for donor requirements, or for the improvement of program delivery. In the example of Haiti the aid agency did explicitly ask the beneficiaries to consent to the collection of their information by the aid agency, in order to, amongst other things, create an identification card. Some of the other agencies also asked for consent but some agencies felt that consent was not necessary because they had to collect beneficiary personal information to carry out the program and comply with their reporting and monitoring requirements.

In fact, beneficiaries rarely have the ability to give free and informed consent for other obvious reasons – the circumstances of the delivery of aid. Aid agencies indicated that it was not always possible to

[59] *Cash transfers and the future of humanitarian assistance*, July 2012, CALP & Schweizerische Eidgenossenschaft, www.un.org/en/ecosoc/julyhls/pdf13/has_concept_note-calp-sdc.pdf; *Cash Transfer Programs in Emergencies*, Page 6–7, Edited by Pantaleo Creti & Susanne Jaspars, Oxfam, http://policy-practice.oxfam.org.uk/publications/cash-transfer-programming-in-emergencies-115356;Fact Sheet 2- Cash Transfer (EU) http://ec.europa.eu/echo/files/policies/sectoral/Cash_and_Voucher_FS2.pdf

[60] *Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines*, Page 2, Fred Cate, Peter Cullen, Viktor Mayer-Schonberge, March 2014; Cash Transfer Programs in Emergencies, Page 4, Edited by Pantaleo Creti & Susanne Jaspars, Oxfam, http://policy-practice.oxfam.org.uk/publications/cash-transfer-programming-in-emergencies-115356

ask for consent from refugees. Given that aid agencies may often be required to provide lifesaving assistance, there may not be sufficient time to go through the process of getting consent before providing assistance to the beneficiary. In an emergency there is no time for preliminary deliberation or engagement in the weighing of costs and benefits. Benefits are immediate, tangible and essential, while costs are difficult to contemplate and take into proper consideration. The receipt of emergency aid is an attempt by beneficiaries to ensure their survival and the survival of their dependents. It is not a voluntary retail or commercial transaction over goods or services. The collection of personal information in order to provide aid is involuntary and cannot be transformed into a voluntary transaction.

Finally, in an emergency situation the full future extent of personal information processing and disclosure it is often not clear to the aid agencies themselves and they are unable to provide fulsome information to recipients. Beneficiaries as a result, are unable to provide informed consent because they are not fully informed.[61]

Inter-Agency Beneficiary Data Sharing

The sharing of beneficiary personal information between aid agencies is driven by considerations of accountability and efficiency. Agencies need to be able to demonstrate to donors that their delivery of aid is effective and has the greatest possible positive impact on the humanitarian crises that the agency targets and the donors support. A coordinated approach between agencies would avoid duplication and in the inefficient use of resources, but it is more difficult to eliminate overlap and ensure efficiency when several agencies are engaged in similar programs and especially when several agencies are engaged in humanitarian cash programs.

The collection of personal information on beneficiaries by aid agencies, and the sharing of information between agencies, could address some of the feared overlap and inefficiencies by allowing agencies to determine whether individuals are engaged in the collection of benefits inappropriately from several agencies (and diminishing the support available to others) and would enable agencies to provide a more fulsome report on aid recipients to donors.

Categories of personal information that would be collected for the purposes of effective coordination and use of material resources may include the contact information of beneficiaries (name and physical address), gender, physical identifiers (height, weight, complexion, hair and eye colour), displacement and movement records. Aid agencies are also considering the collection of biometric data such as finger prints or iris scan, and in programs that deliver humanitarian cash electronically, the relevant electronic records, such as cell phone data from beneficiaries of mobile money listing spending records.

We used the recent European guidelines on purpose specification to provide guidance for inter-agency information sharing.[62] There are two privacy principles involved in the disclosure or sharing of beneficiary data: purpose specification and use limitation. Purpose specification is an essential condition to processing personal data and a prerequisite for applying other data quality requirements. Purpose specification and the concept of compatible or limited use contribute to transparency, legal certainty and predictability. They aim to protect the individual by setting limits on how information controllers are able to use their data and reinforce the fairness of the processing. The limitation should, for example, prevent the disclosure, making available or otherwise using individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable. An erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles.

[61] *Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies*, Page 10–11, October 2014. UNOCHA Policy Development and Studies Series, www.unocha.org/about-us/publications/policy-briefs

[62] Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Some of the factors to consider in determining whether information should be shared between agencies include: the relationship between the purposes for which the data have been collected and the purposes of further processing, the context in which the data have been collected and the reasonable expectations of the beneficiaries as to their further use, the nature of the data and the impact of the further processing on the beneficiaries and the safeguards applied by the agencies to ensure fair processing and to prevent any undue impact on the data subjects

For example, retaining personal information for auditing purposes seems to be directly related to the original purposes for which it was collected and can be reasonably expected by beneficiaries. Legal requirements to audit aid programs can also contribute towards the legitimacy of such retention and its compatibility with a personal information protection regime.

Sharing information between agencies takes such examples a step further. For example, consider two aid agencies which have their own process of determining benefit eligibility in a natural disaster crisis, such as an earthquake. Each agency requires, as part of their process, that potential beneficiaries provide proof of the physical harm their dwelling suffered. Individuals may approve of their information being shared in the context of streamlining the determination of their eligibility (e.g., by allowing them to submit information just to one agency who would then share it with the other – or as discussed below – to a central repository).

However, the consideration and articulation of further purposes is crucial in such examples. Suppose one agency has a policy that it does not provide aid to beneficiaries that already received aid from another agency. Individuals would not want their information shared in such circumstances. At the very least, transparency around the policy and the purposes for which the information would be used is required.

Of particular concern is the creation of unnecessary databases. Databases offer an easy technological solution for the inter-agency sharing of personal information, but come at a cost to personal information protection. Data protection history shows that databases are almost always used for secondary, unforeseen consequences, such as the big data initiatives discussed below.

Personal Beneficiary Information Systems and Big Data

The term "Big Data" is used to describe a universe of very large datasets that hold a variety of data types. A new generation of technology and information architecture has been created to facilitate the fast processing speeds needed to analyze and extract value from these extremely large sets of data using distributed platforms. In common usage, "Big Data" is used to refer both to these vast datasets and also to the process of analyzing and extracting value from enormous amounts of data across multiple silos of information. Big Data analytics enable organizations to make connections, identify patterns, predict behaviour, and personalize interactions to an unfathomed extent. In its report on Big Data for Development, the UN Global Pulse (June 2012) noted that "Big data for development is about turning imperfect, complex, often unstructured data into actionable information."[63]

With organizations increasingly undertaking data analytics activities to derive new insights, regulators, legislators, interest groups, and citizens have begun to voice concerns about the impact of this activity on privacy – from the misuse or unauthorized disclosure of personal information to data-based surveillance. Once taken for granted, fundamental protections afforded to individuals in the processing of their personal information – e.g., notice, consent, purpose specification, and limitation – are now increasingly being challenged by the nature of Big Data analytics. Some argue that our notion of privacy itself must change, and that the requirements of consent, purpose specification and use

[63] UN Global Pulse. Primer 2013; Big Data for Development 2012;

limitation act as a barrier to Big Data analytics. The Data Protection Principles for the 21st Century, developed by Microsoft and the Oxford Internet Institute,[64] generally dispense with the notion of consent and emphasize a cost/benefit analysis to the use of information, rather than the a-priori articulation of specific purposes currently required.

This framework has been described as a form of paternalism, where organizations determine "what is best" for individuals, and those individuals are unable to contribute to any discussions involving the use or misuse of their personal information.[65] Inadequate restraints and a paternalistic approach could lead to what privacy advocates fear most – ubiquitous mass surveillance, extensive and detailed profiling, sharpened information asymmetries, power imbalances, and, ultimately, various forms of discrimination.[66]

The potential risks of big data systems are made more explicit through the examination of the proposed Oxford principles for privacy and big data, which were noted above. It is hard to square the professed respect for the dignity of aid recipients, which is the foundation for the development of humanitarian cash programs, as well as the foundation of data protection and the emerging big data enterprises. These largely commercial initiatives rely on an almost unfettered ability to share information and analyze it for unforeseen purposes and to deliver novel insights. In that sense, the very mission of big data is arguably at odds with the traditional limitation if personal information processing to specific and transparent purposes.

The Oxford proposal seeks, accordingly, to loosen the restriction on the purposes for which personal data could be collected and used. While it does offer a welcome focus on the use of personal information as a contemporary issue that data protection regimes must contend with, it does not offer meaningful protection through its proposed cost/benefit analysis.

For the recipients of aid in emergency crises situations the collection of personal information, if not done with care, could be considered to inflict further harm and add to an already undignified situation which aid agencies seek to alleviate. Allowing for the future processing of such information for as yet-to-be determined big data purposes appears to be at odds with the preservation and enhancement of dignity that aid organizations strive to preserve.

Databases are also an attractive target for cyber criminals, and necessitate an investment in data security. Cyber attackers may sell the information in databases to groups with political interest in the data as well as attempt to use the information in the database to commit financial fraud. Private sector agencies or companies that are involved in creating or maintaining the database or the biometric technology may want access to the database information to improve their products and services and to increase their profit.[67]

Before collecting information and creating centralized databases, aid agencies would have to develop robust cyber-security measures, and engage cyber-security experts to design data access and management protocols, and assign data security privileges.[68] Data sets would need to be anonymized and aggregated to ensure full data and privacy protection. It is not clear whether such initiatives would constitute the most effective use of agency resources – which was the motivation for the inter-agency sharing of personal information to begin with.

64 www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

65 *The Unintended Consequences of Privacy Paternalism*, Ann Cavoukian et al., www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf

66 PbD Big Data Innovation. Deloitte/IPC. 2013

67 Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies, October 2014. UNOCHA Policy Development and Studies Series, www.unocha.org/about-us/publications/policy-briefs

68 Ibid.

Anonymisation, for example, is very difficult to achieve in a Big Data environment, where the ability to re-identify individuals increases rapidly. Refugee beneficiaries, for instance, may only be willing to participate in such databases once they receive iron-clad guarantees that it will not be possible to re-identify them.

Anonymisation

Not all data is personally identifiable. It is important to understand the distinctions between the different forms of non-personal data. *De-identified information* refers to records that have had enough personal information removed or obscured in some manner such that the remaining information does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual.[69] *Aggregated information* refers to information elements whose values have been generated by performing a calculation across all individual units as a whole. *Non-personal, confidential information* is information that often holds tremendous value and importance for organizations, such as business plans, revenue forecasts, proprietary research, or other intellectual property. The disclosure or loss of such confidential information can be of grave concern for organizations but is not considered a privacy breach.

Some kinds of information are not so easily characterized as personal or non-personal information. One such example is *metadata* – information generated by our communications devices and our communications service providers as we use landline or mobile phones, computers, tablets, or other computing devices. Metadata is essentially information about other information – in this case, relating to our communications. While context is key in making determinations about personal information, in the case of metadata it is especially important. The detailed pattern of associations revealed through metadata can be far more invasive of privacy than merely accessing the content of one's communications.

Ideally, information used for statistical or policy development purposes should be fully anonymised. Full anonymisation may, however, not be possible due to the nature of the processing (e.g. where there may be a need to re-identify the data subjects or a need to use more granular data that, as a side effect, may allow indirect identification). Partial anonymisation or partial de-identification may be the appropriate solution in some situations when complete anonymisation is not practically feasible. In these cases, various technological techniques (including pseudo-anonymisation, key-coding, keyed-hashing, using rotating salts, removal of direct identifiers and outliers, replacing unique IDs, introduction of 'noise', and others) should be used to reduce the risk that data subjects can be re-identified. The adoption of safeguards must serve the notion of functional separation – database information used should not be available to support measures or decisions that are taken with regard to the individual data subjects concerned.

Among the appropriate safeguards which may bring additional protection to the data subjects and relieve aid agencies of having to deal with complex technical issues is the arrangement of a trusted third party (TTP). TTP is common in situations where a number of organisations each want to anonymise the personal data they hold for use in a collaborative project. Trusted third parties can be used to link datasets from separate organisations, and then create anonymised records for agencies.

[69] See NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010, p. E–1

Data Privacy Recommendations

The Relationship between Data Protection and Know Your Customer Standards

Several countries with personal information protection legislation have attempted to set guidelines for this relationship, and for how organizations can meet their privacy obligations in the face of anti-money laundering and anti-terrorist financing reporting requirements is one facing a number of jurisdictions with data protection laws. The Privacy Commissioner of Canada provided the following guidelines:[70]

1 Understand the legal requirements and what personal information is necessary to collect to comply with the KYC standard.

2 Determine if the requirement is only to see/review the document or to record a beneficiary's identity document information. Do not make a copy of the document unless it is required by law or for a legitimate business purpose.

3 Clearly outline the aid agency's reporting requirements to service providers.

4 Keep reported personal information up-to-date and accurate.

These guidelines are helpful, and we incorporate some of them into the recommendations of this report. In addition, more specific recommendations are required since based on our research it is apparent that aid agencies do not operate under any beneficiary privacy policies and do not have a clear understanding of the notion of data protection when collecting, using and disclosing beneficiary personal information.

Recommendation – Incorporate Privacy into Humanitarian KYC Guidelines

Guidelines used by agencies to determine the appropriate cash program should be modified to include personal information protection considerations.

In its 2010 guidance document for agencies contemplating a cash aid program in emergencies CALP provides a manual to help aid agencies make decisions about how best to deliver cash to beneficiaries.[71] The manual provides details that aid agencies need to take into consideration when examining delivery options such as the identity of the service provider and the delivery method. The manual provides a full assessment checklist as well as templates and tools.

CALP's assessment checklist, tools and templates could be improved by including consideration of privacy and data protection principles. This can be done by recognizing privacy and data protection as one of the many essential elements to consider in a given context. A requirement to conduct a conceptual Privacy Impact Assessment may be integrated into the checklist, which, when combined with the other objectives and criteria for determining the best delivery mechanism, will strengthen the final approach from a human rights/privacy perspective.

For example, the direct method of delivering cash to recipients in envelopes or vouchers is perhaps the most privacy protective because it likely requires very little identification. Privacy advocates view cash transactions as a means to protect anonymity. Assessing each payment method from a privacy lens may also impact the final design of the delivery mechanism. The section on Identification and

[70] Privacy and PCMLTFA. How to balance your customers' privacy rights and your organization's anti-money laundering and anti-terrorist financial reporting requirements, March 2012, Office of the Privacy Commissioner of Canada, www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp

[71] CALP, "Delivering Money: Cash Transfer Mechanisms in Emergencies"

Authentication could be strengthened to acknowledge the varying degrees of privacy risks with each of the approaches. CALP notes that "The design of each of these elements [of a payment system] can involve trade-offs between cost, complexity, resilience and risk management."[72] Privacy should be an integral part of such a design.

Recommendation – Create Beneficiary Privacy Policies

Aid agencies should create and follow privacy policies for beneficiary personal information that they collect, use and disclose.

The collection, use and disclosure of beneficiary personal information that aid agencies process to carry out their programs should be guided by sound data protection policies and measures. Furthermore, aid agencies must explain to beneficiaries that they collect beneficiary personal information for the agencies' unique purposes and distinctly from the service providers. It is not sufficient for aid agencies to tell beneficiaries that their information is being collected for regulatory compliance and to allow the service provider to provide services when the collected information is also used by the aid agencies for their own purposes. As long as such practices continue beneficiaries should be told that aid agencies also use KYC information or information collected by the aid agency to implement their program and for monitoring and other purposes. Based on our research some agencies are informing beneficiaries in such a manner but some agencies are not.

As a best practice, and in recognition of the dignity and autonomy of beneficiaries, aid agencies should develop privacy policies that take into account their humanitarian mission. Aid agencies should adhere to these policies even when operating in countries or territories without any privacy laws or any formal legal obligation to protect personal information.

The Cash Learning Partnership (CALP) has published guidelines for developing a model beneficiary data privacy policy for aid agencies delivering cash programs (the CALP model).[73] Aid agencies were encouraged to adopt model resolutions in support of the CALP model and demonstrate senior leadership commitment to privacy and data protection. Yet the CALP principles do not seem to map onto internationally recognized Fair Information Practice Principles (FIPPs) and the CALP model could be enhanced by a more fulsome definition of personal information, as outlined above.

There are several general frameworks, all based on the FIPPS and the principles articulated by CALP, that aid agencies could look to creating a recipient-specific privacy policy. One such possible framework is the OECD guidelines for data privacy and protection.[74] The OECD guidelines state that data should be collected and used only for specific purposes of which the recipient should be informed. Personal information should not be used for other purposes, or disclosed to third parties unless required by law (KYC standards would be one such requirement). Aid recipients should be able to access the personal information held about them by the aid agency, and responsibility for the accuracy and security of the personal data rests with the aid agency.

The proposed EU General Data Protection Regulation is another framework that could guide the development of aid agencies' privacy policies. The Regulation, if adopted by EU member states, will create a uniform level of privacy protection across Europe. In addition to the above principles the Regulation offers individuals specific rights, such as the right to be forgotten, the right to object to processing, the right not to be profiled – which could be very significant for aid recipients whose information is collected under KYC standards in order to ensure they are not involved in money

[72] Ibid, p7.

[73] *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure use of Personal Data in Cash and e-transfer Programmes*, CALP

[74] *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), Chapter 1, www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

laundering or terrorism. Significantly, the Regulation obliges organizations to provide privacy to individual by default, and to design privacy into their data processes.[75]

Other, more controversial proposals for data protection have been offered that should be examined by aid agencies. The Data Protection Principles for the 21st Century, developed by Microsoft and the Oxford Internet Institute, referred to above, are one such proposal. The critique of the principle of consent put forward by the Oxford proposal is applicable to the attempt to utilize consent for the delivery of humanitarian cash programs, and indicates that aid agencies should protect the dignity of recipients by alternative means.

Recommendation – Separate KYC Information

Personal information collected for KYC purposes should only be used for those purposes and should not be combined with other personal information or used or disclosed for other purposes.

As stated above information collected for KYC purposes may not be protected under privacy legislation and is most likely exempt. Such information could be retained by the service provider for KYC purposes indefinitely and likely be disclosed to national or international regulatory agencies. Aid agencies cannot prevent service providers from either retaining this information or disclosing the information or doing whatever they need to do to comply with the applicable KYC regulatory requirements.

The aid agencies should consider however the beneficiary information that the service provider asks for on the KYC form, and determine whether that information is necessary for KYC compliance or whether the information requested is more than what would be required for KYC compliance. The aid agency could then negotiate with the service provider as to what information should be passed on to them. *Only the minimal information that would allow the service provider to comply with its KYC obligations should be provided by the agency or passed on to the service provider.*

The copies of the KYC forms that are retained by the aid agency and the information that the aid agency collects on its own initiative for its own purposes will not be exempt from the scope of data protection principles. Given that anti-money laundering legislation does not regulate aid agencies and does not impose KYC compliance obligations on aid agencies, it is not clear why aid agencies would retain a copy of the service provider's KYC form. It appears that aid agencies retain these forms for program monitoring, donor reporting and auditing purposes. Aid agencies should stop such practices.

Policy-Specific Recommendations

Below are some specific recommendations directly related to issues observed in current agency information processing practices.

Recommendation – Notice instead of Consent

Aid agencies should base their beneficiary privacy policies on the principle of notice instead of the principle of consent.

For the reasons discussed above the provision of humanitarian aid is not a situation in which beneficiaries could be said to freely and voluntarily consent to the processing of their personal information. In such contexts aid agencies should be obligated to notify beneficiaries in the most fulsome manner possible about the purposes and the manner in which their personal information will be collected, used, disclosed and retained.

Aid agencies report that when they explain to beneficiaries the purpose for the collection of information, the use for that collected information and the parties that may use that information then

[75] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

beneficiaries, including refugees, are generally more responsive and willing to share their information with the aid agencies once they understand the purpose and the reasons for collection.

In such situations aid agencies must ensure that they work to preserve the dignity of beneficiaries, at all levels. Aid agencies must take care that they will not strip beneficiaries of dignity through the intrusive collection of personal information at precisely the same time they are attempting to empower beneficiaries and provide them with a greater sense of dignity and control through the development of humanitarian cash programs. While beneficiaries cannot be said to meaningfully consent to the collection of their personal information, aid organizations must ensure that are data protection principles and best practices are closely followed.

For example, in the context of KYC beneficiary information, beneficiaries will be required to provide certain information to the service provider for a legal and regulatory purpose. Data privacy legislation either explicitly or implicitly make it clear that consent is not required for personal information that is collected and proceed in order to fulfil certain legal/regulatory obligations. In the Philippines for example, where data protection legislation exists, and where the legislation exempts the collection of information for KYC purposes, it would be appropriate to inform aid beneficiaries that their information will be collected for the fulfilment of a legal obligation-compliance with KYC standards.[76]

Aid agencies should fully explain the purpose for the collection of beneficiary personal information, the potential uses of that information and the disclosure of that information. It may be that meaningful consent will be possible for some purposes and in some circumstances, e.g., for monitoring a program, reporting to donors, or program co-ordination by aid agencies.

In the context of collecting and processing personal information by aid agencies for the purpose of implementing the programs, such as the creation of identification cards for refugees, meaningful consent may not be possible, and notice must be relied upon. As discussed above, aid beneficiaries rarely have the ability to give free and informed consent given the circumstance of the delivery of aid. Refugees or persons affected by natural disasters need aid and protection. The collection of personal information in order to provide aid is involuntary and cannot be transformed into a voluntary transaction.

Nevertheless, beneficiaries, and refugees in particular, have shown that they want to participate in some form of informed consent of the collection and processing of their personal data or at least they want to be informed and acknowledge to the aid agencies their understanding of the collection and processing of their personal data. Aid organizations must, therefore, ensure that their data protection principles and best practices are closely followed

Recommendation – Data Minimization

Aid agencies should practice data minimization at all stages of the information's life-cycle

Some aid agencies have acknowledged that they collect a lot of information from beneficiaries and significantly from refugee beneficiaries even though they intended to collect the minimal amount of data. The information they collect may be more than what is required to implement their program. Having a privacy policy in place based on the particular situation or circumstance of the refugee beneficiaries would curtail the excess collection of refugee personal information.

The privacy policy should allow the aid agency to evaluate the purpose of collection of every piece of information, should promote the collection of minimal amount of data, should collect, use, share, retain and store information in such a way that does not increase their vulnerability and should align with the aid agency's purpose of providing protection to the refugees. The concerns of the refugees in relation to sharing of their information should inform the aid agency's data privacy practices.

[76] *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure use of Personal Data in Cash and e-transfer Programmes,* Page 13, CALP.

Recommendation – Protect Personal Information beyond Confidentiality

Aid agencies must establish personal information protection practices that provide beneficiaries with rights in their personal information beyond contractual promises of confidentiality.

Aid agencies should have proper privacy policies in place that guide the collection, use and disclosure of beneficiary personal information. The confidentiality clauses in contracts between service providers and aid agencies preserve the confidentiality of any information that either the service provider or the aid agency generates or learns about during the term of that contract and usually for a few years afterwards. These clauses preserve the confidentiality of any information (including beneficiary information) that arises under the business relationship between the aid agency and the service provider.

However, personal information protection and confidentiality are different doctrines with different requirements. A data protection regime emphasizes a person's control over their personal information and provides them with the opportunity to make informed choices about the collection of their information as well as with the right to access their information and ensure its accuracy. Confidentiality provides for none of that.

Biometrics, Big Data and Information Sharing Recommendations

It is paramount that aid agencies proceed with caution in these areas. Agencies must focus on their core mission – providing aid and relief to vulnerable populations in times of great need while preserving the autonomy and dignity of beneficiaries. The deployment of biometrics, the sharing of information between agencies, and the embarkation upon big data initiatives should not proceed without a fulsome analysis of the impact of such decisions on the privacy of beneficiaries.

Recommendation – Consider Alternatives

Aid agencies should first examine whether alternative non-biometric means to authenticate users would meet the same objective(s).

Before deploying a new system with implications for privacy an organization should be able to clearly justify the prospective privacy intrusions. Beyond understanding the technical issues surrounding biometric systems, aid agencies must also be able to provide sufficient evidence of the necessity of the technology. Convenience should not be considered a sufficient reason for implementation of such a system. Instead, aid agencies should be able to provide a full and comprehensive explanation of the purpose and benefits (or necessity) of the system, the drawbacks (or inappropriateness) of alternative measures, and the reasons why it was decided that the privacy issues associated with biometrics were outweighed by the necessity of the system.

Recommendation – Implement Safeguards

Procedural and technical safeguards must be implemented once a decision to use a biometric is made.

We suggest the following elements. Biometric information should be collected directly, encrypted, stored separately from other personal information and only used to confirm eligibility for benefits (one-to-one matches). Aid agencies should consider the many privacy-enhancing solutions in this field.[77] Finally, access to biometric information must be strictly controlled, and government access should not be permitted.

[77] See e.g., the use of ECG through a wearable technology device (http://www.nymi.com/the-nymi-band/); or the Match-on-Card (MOC) solution, that does not require a central databases and where the biometric reference inside the card is highly secure and tamper resistant and remains under the control of its owner (http://www.morpho.com)

Recommendation – Inter-Agency Data Sharing

Inter-agency personal information sharing is premature at this point in time and should only be revisited once robust data privacy practices are in place.

Based on our research it appears that agencies are currently not properly equipped to handle personal information for their own purposes or for KYC compliance purposes. Several steps must be taken by agencies individually, such as the development of beneficiary privacy policy and practices, before agencies are considered ready to take on the additional complications of information-sharing with its inherent privacy and security risks. This recommendation should be revisited once the proper personal information protection foundation is in place.

Recommendation – Big Data

Big Data analytic initiatives should be deferred for the time being until a proper Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) are completed.

For reasons similar to those regarding inter-agency information sharing, aid agencies should not presently consider or participate in the creation of beneficiary databases or the combination of such databases with other sources of information, or in the free-form analysis of such information. Organizations that have a mature privacy program utilize risk assessment tools such as a Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) at the earliest stage possible in any initiative or new system development involving personal information to ensure that privacy risks are mitigated and addressed proactively "by design."

Appendix – the World Vision Privacy Policy

World Vision International shared with us a draft Partnership Policy on Data Protection and Privacy dated October 7, 2014 as well as a Guidance Notes. The purpose of this draft policy is to serve as an overarching privacy standard which all entities in the World Vision Partnership, including microfinance institutions, suppliers and vendors must follow.

As discussed above, the requirement for organizations to provide clear notice to individuals is a core privacy principle. Notice is commonly given in the form of a privacy policy. It is no surprise that research findings show that privacy notices impact trust and promote social welfare. However, the usability of many generally-worded policies is troubling.[78]

FIPPs are the bedrock of almost all privacy policies. Many variants of FIPPs exist and are in force around the world today, varying in length, detail, and force of application. Despite superficial differences, they all share common fundamentals. At the broadest conceptual level, all privacy and data protection principles seek both opacity and transparency of data processing.

Opacity-enhancing principles seek to restrict unauthorized data processing by minimizing and safeguarding data, while transparency-enhancing principles seek to enhance visibility and accountability by involving data subjects in the data processing lifecycle, and by establishing governance requirements for data processors. All FIPPs express four "meta-FIPPs:" Data Minimization, Safeguards, User Participation, and Accountability. The enduring confidence of individuals, businesses, and regulators in organizations' data-handling practices is a function of their ability to express the FIPPs' core requirements, which also promote efficiencies, innovation, and competitive advantages. Privacy is not simply about compliance with regulatory frameworks but it is essential for individual trust.

In light of our research above our specific comments and suggestions for improvement of the draft policy are as follows:

1 **Approval**: The policy should be approved by the WVI Board. It is essential for privacy to have senior leadership commitment. An important goal for an organization is to embed privacy into its culture. Members of a board must not only review and approve their organization's privacy plan, but also require regular reporting on training, issues as a result of ongoing monitoring, auditing and evaluation.

2 **Responsibility**: Accountability for privacy requires that at least one individual be identified as having leadership responsibility for privacy.

3 **Publication**: Transparency (Openness) is an essential privacy principle. WVI should draft this policy keeping in mind that it should be made available to the public. Many organizations publish their corporate privacy policy or statement on their website.

4 **Purpose**: The privacy policy should be linked to WVI's mission and/or values. Respect for privacy rights aligns with WVI's value of dignity: "We act in ways that respect the dignity, uniqueness, and intrinsic worth of every person — the poor, the donors, our staff and their families, boards, and volunteers."

5 **Scope**: The scope of the policy should be clarified. Does it only apply to organizations external to WVI or is it meant to also apply to the WVI Board, Executive, staff, volunteers, etc.?

[78] Cranor, Lorrie Faith et al. Are they actually any different? Comparing thousands of financial insitutions' privacy practices. Carnegie Mellon University. The Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11–12, 2013. Washington, D.C.

6 **Background**: WVI should consider adopting the principles of Privacy by Design in order to express WVI's interest in being proactive about privacy, about making privacy the default of their operations and about ensuring that WVI achieves its core mission while at the same time respecting the privacy rights of individuals.

7 **Principles**: Contemporary policies are moving away from reciting foundational principles such as the OECD principles. While these remain the bedrock of privacy they are of little use in a document that should offer organizations and individual specific guidelines and assurances related to WVI's activities.

CONTENTS

This material was developed as part of the European Commission Humanitarian Aid and Civil Protection Department's Enhanced Response Capacity funding (2014–15).

This inter-agency project was led by the Office of the United Nations High Commissioner for Refugees on behalf of its partners: the Cash Learning Partnership, Danish Refugee Council, International Rescue Committee, Norwegian Refugee Council, Save the Children, Oxfam, United Nations Office for the Coordination of Humanitarian Affairs, Women's Refugee Commission, World Food Programme, and World Vision International.

Humanitarian Aid
and Civil Protection