OCCASIONAL POLICY PAPER

OCHA
United Nations
Office for the Coordination
of Humanitarian Affairs

Humanitarianism in the Age of Cyber-warfare:

Towards the Principled and Secure Use of Information in Humanitarian Emergencies

OCHA POLICY AND STUDIES SERIES
October 2014 | 011

OCHA

This publication was developed by OCHA Policy Development and Studies Branch (PDSB) and mFieldWork
Kirsten Gelsdorf, Chief, Policy Analysis and Innovation Section.
Hansjoerg Strohmeyer, Chief, Policy Development and Studies Branch
This paper was written by Daniel Gilman (OCHA) with support from Leith Baker, and edited by Matthew Easton. Research support was provided by Nathalie Guillaume.

This publication was made possible with advice and support from John Scott-Railton and Ron Deibert (Citizen Lab), Alexander Beck (UNHCR), Nathaniel Raymond (HHI), Carly Nyst and Anne Crow (Privacy International), Massimo Marelli and Laurent Gisel (ICRC), Anahi Ayala Iacucci (Internews), Danny O'Brien (Electronic Frontier Foundation), Frank Smyth (Global Journalist Security, Genevieve Wills (WFP), Valentina Falk (OHCHR), Christopher Wilson (The Engine Room), and Kristin Bergtora Sandvik (PRIO).

For more information, please contact:
Policy Development and Studies Branch
United Nations Office for the Coordination of Humanitarian Affairs (OCHA)
E-mail: ochapolicy@un.org

OCHA POLICY AND STUDIES SERIES
October 2014 | 011

CONTENTS

KEY MESSAGES:

1. New information and communication technologies in humanitarian response create opportunities for improved humanitarian response as well as risks to the privacy and security of affected communities.
2. The current system tends to restrict sharing of relatively harmless data, while not sufficiently protecting information that could be used to identify individuals and communities.
3. The information that humanitarians can collect will be shaped in the future by factors that include:
   a) privacy laws and any appropriate exceptions for disasters and crisis.
   b) ethical considerations, such as the need for practices that ensure information is used responsibly, particularly when obtaining consent is not practical.
   c) the extent to which political or criminal groups target humanitarian operations, as well as the level of government surveillance.
4. To respond to these emerging issues, humanitarian organizations should:
   a) prioritize transparency and evidence based humanitarianism and ensure that scarce resources for data security are focused only on truly sensitive information.
   b) support ethical innovation, ensuring that projects using new or untested systems are held to a higher standard of oversight, and codes of conduct are regularly updated and enforced.
   c) adopt codes of conduct and operational procedures for the ethical and principled use of information, in particular personal data, at the organizational level, and consider adopting universal guidelines for the use of information in humanitarian crisis.
   d) invest in risk analysis and information security, including ensuring basic data security training for staff, and where needed, affected communities, and working with experts to better understand, prevent and respond to attacks.
   e) promote the idea of a "humanitarian cyberspace" that humanitarian information systems should be off-limits for attacks and advocate that in some cases cyber-attacks on humanitarian actors are violations of international humanitarian law.
   f) advocate for the co-creation of legal frameworks with affected communities to protect their data in emergencies.

GLOSSARY:

CII	community identifiable information: data from which a geographic, ethnic, religious, economic or political group can be identified.
EULA	End User License Agreement: a legal contract between a software developer or vendor and the user, which specifies the rights and restrictions that apply to the software.
ERC	ethics review committee: a body tasked with approving and monitoring studies or other projects, most often medical or behavioral research involving human subjects.
IATI	International Aid Transparency Initiative
IHL	international humanitarian law
ICRC	International Committee of the Red Cross
IOM	International Organization of Migration
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
PGEA	pro-government electronic actors: Hackers and others who act in support of a government, but whose relationships to the government are unknown, imperfectly understood, informal, or controversial.
PII	personally identifiable information: information from which an individual can be identified, such as names, ID numbers, physical, postal or email addresses, telephone numbers, photographs, age, gender or biometrics.
PIA	privacy impact assessment
RAT	Remote Administration Tool or Remote Access Tool: software used to access or control a computer from a distance, whether for legal or illegal objectives.

PART I: Introduction

Humanitarian assistance is driven by information. From early warnings to needs assessments to final evaluations, information determines priorities and resource allocation. In addition, a crisis drives people to collect and share personal information that they otherwise wouldn't: the names of missing family, medical conditions and needs, and their current location and that of their homes. In fact, the humanitarian principle of impartiality, requiring aid to be given on the basis of need alone, makes this information essential.

In 2013, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) examined emerging issues relating to information and communications, particularly the spread of cell phones and connectivity, advanced data analytics and other tools. *Humanitarianism in the Network Age,* the first UN report to identify information as a basic need in humanitarian response, sketched a vision of a future in which affected people produce and share information in real time with each other and with humanitarian responders, disasters are better anticipated through sophisticated monitoring systems, and accurate data and analysis clear the fog of war.

> ***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.***
>
> **Article 12, Universal Declaration of Human Rights**

However, the "Network Age" also comes with risks and challenges. A humanitarian crisis can create a justification for waiving concerns about how information is collected and used, even as cyber-warfare, digital crime and government surveillance rises, particularly in unstable contexts.

To deal with these challenges, *Humanitarianism in the Network Age* recommended that the humanitarian sector develop robust ethical guidelines for the use of information. It specifically called for "do no harm" standards that clearly address liability, privacy and security. This report looks in more depth at these issues and makes recommendations to ensure that emerging technology is used responsibly.

Part II: The evolution of humanitarian information systems

Humanitarian information systems still often rely on aggregated reports, offline spreadsheets and manual collection. These shortcomings reflect both the reality of gathering information in a crisis and a lack of mechanisms for exchanging data.

But the problem also results from a culture that resists sharing information, often over vague security concerns. Without clear protocols in place to evaluate risk or classify how information should be shared, decisions are often ad hoc. Data of little or no sensitivity may not be shared, while sensitive data is insufficiently protected.

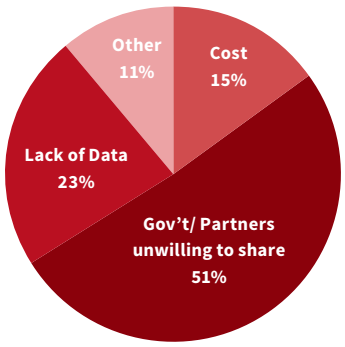


Figure 1. What are the challenges of obtaining data? A 2013 Survey of OCHA Field Information Management Officers

However, humanitarian information collection is rapidly becoming more sophisticated and communal. Organizations are promoting more rigorous data collection methods, open standards and data sharing,[1] even as they are gaining access to vast new sources of information from mobile phones, banks and e-transfers, social media, businesses, satellites and elsewhere.

New technology also allows much more comprehensive collection in the field. With a mobile device humanitarian workers can rapidly collect survey data and assess needs, while integrating these responses with GPS location, photos or other types of data. For example, the KoBo Toolkit, an open-source platform for mobile data collection, has been used in the Central African Republic to support a joint exercise known as a multi-cluster initial rapid assessment (MIRA).[2] Humanitarians are also collecting entirely new types of information, such as bank accounts and financial data for cash programming,[3] and biometrics, such as fingerprints and iris scans, in Kenya, South Sudan, Malawi and elsewhere.[4]

Humanitarian organizations are handling increasing volumes of detailed and sensitive information, often outstripping their capacity to analyse risks and sensitivities. Due to an increased focus on accountability and transparency to donors, information previously used only for implementation is now stored or reported as evidence of project achievements, such as geo-tagged photos of schools or clinics. Many of these new technologies raise difficult ethical questions about how much information should be collected or retained and who has the right to access it.

As they grow, these systems also become more tempting targets for groups with criminal and political motivations. At the same time, the real added value of data collection comes from analysis and verification, which becomes possible when data is shared and combined. Data must be exchanged easily between humanitarian actors, while companies and individuals must trust that the information they provide is used responsibly to save lives.

This is the paradox: effective response in the "Network Age" requires open data and transparency, but the more information that is shared the more risks and challenges for

[1] For example, see the Humanitarian Exchange Language, a set of technical standards for the exchange of humanitarian operational data. Available from http://hxl.humanitarianresponse.info/

[2] "KoBoToolbox Used by OCHA in Central African Republic", 11 August 2014. Available from http://www.kobotoolbox.org/updates/2014/02/kobotoolbox-used-ocha-central-african-republic

[3] The Cash Learning Partnership, *Protecting beneficiary privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, 28 November 2013. Available from http://www.cashlearning.org/resources/library/389-protecting-beneficiary-privacy-principles-and-operational-standards-for-the-secure-use-of-personal-data-in-cash-and-e-transfer-programmes

[4] See http://kanere.org/2013/11/30/classified-fingerprinting/, http://www.unhcr.org/50dc5a309.html, and http://www.unhcr.ie/news/irish-story/unhcr-pilots-new-biometrics-system-in-malawi-refugee-camp

privacy and security emerge. Finding the right balance requires a clear definition of what information needs to be protected and what should be open.

Information about places and objects, such as pre-positioned stocks or medical facilities, is critical to a humanitarian response, and may be very sensitive. However, the primary concern should be information about people and communities. Personal data or *personally identifiable information (PII)* refers to information from which an individual can be identified, such as names, identification numbers, physical, postal or email addresses, telephone numbers, photographs, age, gender or biometrics. The use of personal data is also covered by a range of legal rights and international agreements.

Even when individuals cannot be identified, it is important to consider *community identifiable information* (CII), or data that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic or political. As humanitarians improve data analysis to identify clusters of need, or underserved populations, these same tools allow other actors to target ethnic or social groups. As a result, although not considered legally in the same class as personal data, community identifiable information poses unique risks when working in areas of conflict or social unrest.

Finally, an emerging concern is that *metadata* can be used to cross-reference and de-anonymize other datasets or to see that data has been sent to an organization, even if the content isn't visible. For example if a survey is conducted using mobile phones, like the 2013 household food security assessments by the World Food Program in North Kivu province in the Democratic Republic of Congo, there will be records of phone numbers, cell towers, and the time messages were sent, all of which can identify participants.

New Ways to Collect Humanitarian Data

SMS and cell phones:
SMS surveys and hotlines can collect data even from remote areas.

Mobile devices:
Smart phones and tablets can be used to collect and rapidly collate field survey results, adding GPS coordinates, photos and other data.

Social media:
Social media can provide snapshots of situations for needs assessments or for sharing information with communities.

Cell-phone data:
Cell-phone data can be used to track movement and displacement, monitor spending patterns and many other uses.

Big data and private sector data:
Other large data sets from private companies and governments have potential humanitarian uses.

Crowdsourcing and Digital Humanitarians:
Humanitarians are using volunteer and technical communities or the public to produce and analyse data.

UAVs and satellites:
Unmanned aerial vehicles and a new generation of satellites will provide detailed images and data, even in remote areas.

Biometrics:
Biometric scans can produce unique identifiers for individuals even when there is no formal ID.

Case Study 1 – Biometric registration in humanitarian projects

Biometrics, such as fingerprints and iris scans, allow unique identification of individuals, even when they lack documents. Increasingly common in humanitarian response, particularly in camp situations, biometrics provide a powerful tool for financial accountability, helping ensure that benefits go to the correct people. At the same time, the technology raises concerns about privacy, inappropriate use and accuracy. A number of countries have debated and rejected the use of biometrics, particularly when stored in centralized databases, for their own citizens.[5] After the Kakuma refugee camp in Kenya introduced a mandatory biometric food registration system in 2013, refugees expressed concerns about the exposure of their identity to multiple aid agencies and the government, all of whom have access to a centralized database.[6]

There are also concerns about "scope creep", as a biometric database developed for aid distributions could be linked with others or appropriated for security or political purposes. For example, when UNHCR was discussing sharing biometric information, including iris scans, with the Lebanese Government, refugees expressed concern about the security of the data with one worrying, "They'll take that information and give it to the Syrian government."[7] The databases can also be a tempting target for cyber-groups or criminals.

When any verification system is linked directly to aid delivery, there is also the practical question of how reliable the technology is. In the past, biometrics scans have had a substantial error rate, and may create biases against certain classes of people: iris scans may not work with the blind or people with cataracts, while fingerprints can be difficult to capture from those who do a lot of manual labour, particularly women.[8] In September 2013 in the Mbera camp in Mauritania, for example, 6500 refugees were denied aid because of problems with the biometric registration system.[9] While the efficiency of these systems continues to improve, it is important to consider other types of supplementary verification and have an efficient appeals process. Biometrics systems, like other new information technologies, promise efficiency gains for donors and aid organizations, but must be balanced against privacy and technical concerns, and the feelings of affected people.

[5] Gus Hosein and Carly Nyst, Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries, September 2013, Available from http://ssrn.com/abstract=2326229 or http://dx.doi.org/10.2139/ssrn.2326229.

[6] "Classified Fingerprinting," Kakuma News Reflector, A Refugee Free Press, 11 August 2014. Available from http://kanere.org/2013/11/30/classified-fingerprinting/

[7] Elise Knutsen and Samya Kullab, "Power to Strip Refugee Status Agreed," *Daily Star*, 2 June 2014. Available from http://www.unhcr.org/cgi-bin/texis/vtx/refdaily?pass=463ef21123&id=538d5b5f8.

[8] Katja Lindskov Jacobsen, "Making design safe for citizens: A hidden history of humanitarian experimentation", Citizenship Studies, 2010, 14:1, 89-103.

[9] Gus Hosein and Carly Nyst, "Aiding Surveillance".

ABOVE April 2013, Maban, South Sudan: Elizabeth is registered using biometric finger printing, at the Doro refugee camp, Upper Nile State. Photo: OCHA

New information technologies also subtly introduce actors into the interactions between organizations and the people they work with. New technology, such as tablets to collect and upload data, brings in application developers, as well as mobile, internet and data storage companies, and government regulators. The new process relies on the goodwill and security consciousness of multiple organizations, often in different legal jurisdictions. Humanitarian organizations must think carefully about how partners and service providers will treat personal and sensitive data.

The tension between the need for detailed information to target aid and the risk to privacy and security is not new in humanitarian and protection work, nor is it limited to new technologies. The issue has been addressed broadly in the SPHERE Standards Protection Principle One and in some

organizations, for example, by the international Organization for Migration's 2010 Data Protection Manual. Other organizations have policies in place or are developing them.[10]

However guidance on data protection for humanitarians remains insufficient and is often outpaced by technological developments. Guidance documents and practices do not address many emerging issues, such as privacy laws, safe handling of metadata, standards for anonymization, assessments of cyber-security, or the role of technology providers. Ensuring that new information systems are effective and aligned with humanitarian principles will require an in-depth look at emerging legal, ethical and security issues.

Part III: Law and humanitarian information

International bodies have long recognized the rights of individuals to control how their personal information is used, such as the General Assembly, in its 1990 Guidelines for the Regulation of Computerized Personal Data Files, or its 2013 resolution on "the right to privacy in the digital age"[11], the United Nations Human Rights Committee,[12] the OECD[13] or the International Conference of Data Protection and Privacy Commissioners,[14] Regional organizations, such as APEC,[15] the Council of Europe,[16] ECOWAS[17] or the EU[18] have also adopted data protection and privacy standards.

National data protection and privacy laws are becoming much more common.[19] From 2011 to 2013, the number of countries with a privacy law covering the private or public sectors increased from 76 to 99. Analysts predict that by 2023 the vast majority of countries will have a data protection and privacy law.[20]

While United Nations agencies have special privileges and immunities from national law, NGOs and other humanitarian partners must deal with a patchwork of laws both in their headquarters and in countries where they work. In addition, when working with implementing partners, in clusters, or through other coordination structures, they must determine which organizations bear legal responsibility for compliance.

Countries have different mechanisms for dealing with exceptional circumstances after a disaster. Australia and New Zealand have created special provisions for use of personal information following an emergency or disaster to enable government agencies to share information with authorized humanitarian actors.[21] Well-designed, clear legal frameworks both foster preparedness, by allowing for prior agree-

[10] For instance UNHCR will soon replace internal 2001 Confidentiality Guidelines with a data protection policy. *The Professional Standards for Protection Work* (2013), edited by the ICRC, includes a chapter on "Managing sensitive protection information" and the Cash Learning Partnership's 2013 publication *Protecting Beneficiary Privacy* offers principles and operational standards for the secure use of personal data in cash and e-transfer programmes.

[11] General Assembly resolution 68/167.

[12] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994); Guidelines for the Regulation of Computerized Personal Data Files (adopted by GA Resolution 45/95 of 14 December 1990).

[13] Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), Recommendation by the Council of 23 September 1980, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

[14] International Standards on the Protection of Personal Data and Privacy (The Madrid resolution), Resolution adopted at the 31st International Conference of Data Protection and Privacy Commissioners, 5 November 2009.

[15] Asia-Pacific Economic Cooperation (APEC) Privacy Framework, endorsed by APEC Ministers in November 2004, finalized in September 2005.

[16] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108 of 28 January 1981. This Convention is also open to ratification by non-Council of Europe members, for instance Morocco and Uruguay.

[17] Economic Community of West African States (ECOWAS), Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, adopted at the 37th Session of the Authority of Heads of State and Government, Abuja, 16 February 2010.

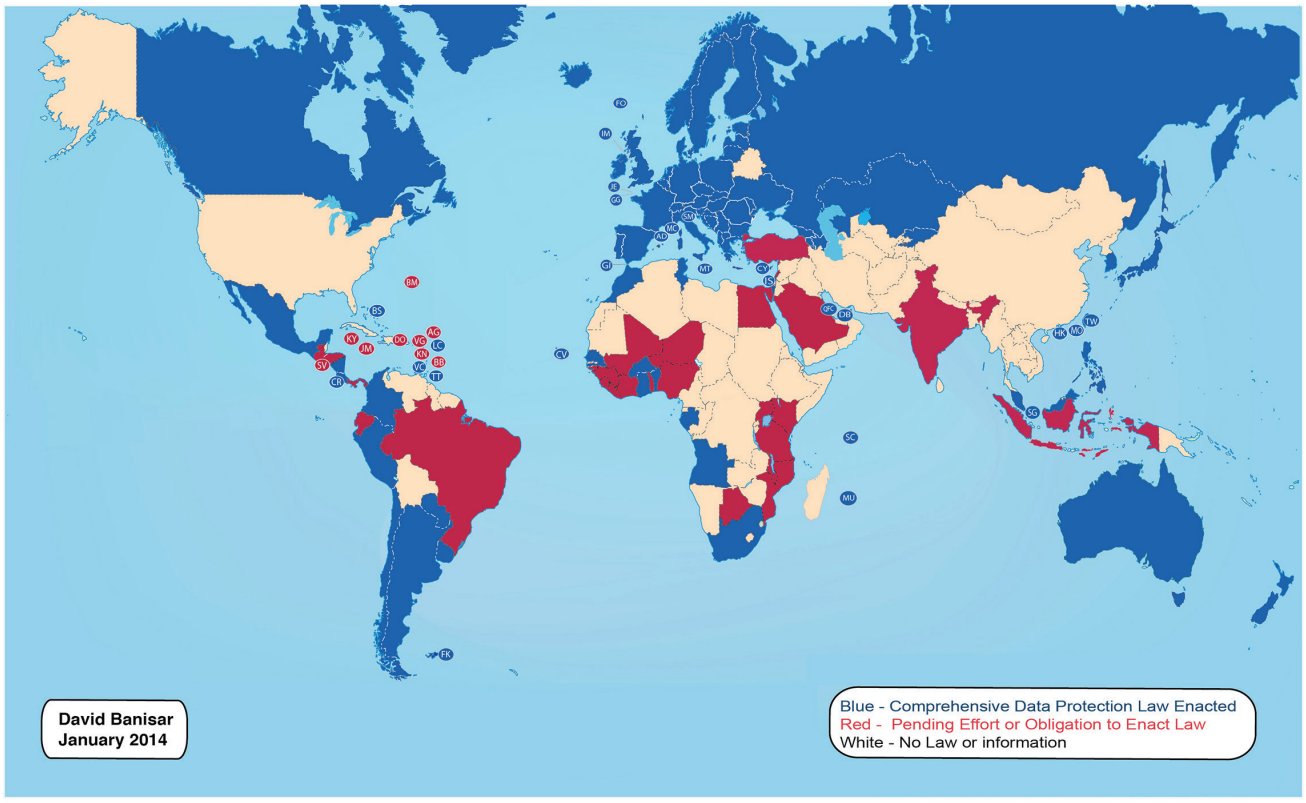
[18] European Union (EU) Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

[19] David Banisar, "National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map", January 28, 2014, Available from SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

[20] Graham Greenleaf, "Global Tables of Data Privacy Laws and Bills," UNSW Law Research Paper No. 2013-39, 16 June, 2013. Available from SSRN: http://ssrn.com/abstract=2280875 or http://dx.doi.org/10.2139/ssrn.2280875

[21] Joel R. Reidenberg, Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu, "Privacy and Missing Persons after Natural Disasters", (Washington, DC and New York, NY: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars, 2013).

National Comprehensive Data Protection/Privacy Laws and Bills 2014



Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.

UN Human Rights Committee

ments on information sharing, and reduce the potential for accidental or inappropriate release of data in an emergency.

With private sector actors providing so much data, corporate contracts and end user license agreements (EULAs) also affect access to information. For important new sources of data, such as mobile phones, humanitarian organizations will need to work with major companies and industry associations to ensure that post-disaster information sharing is covered in these agreements or in separate frameworks. Data protection and privacy laws, and the terms of use that companies develop based on them, will increasingly shape the way that humanitarians gather and share information.

Part IV: Ethics and humanitarian information

While humanitarian principles address a number of issues about how humanitarian assistance is delivered, there is an inherent contradiction around the use and protection of information of affected people in humanitarian operations. Absolute protection would make humanitarian response impractical by not allowing the collection of any information, while the public listing of personal details would likewise endanger lives. Clearly, the imperative to save lives under difficult circumstances must be balanced with the responsibility to do no harm.

> ***The refugees felt insecure and harassed to have to present their fingerprints to collect the rations.***
>
> **Refugee leader, Kakuma camp, Kenya**

Therefore, even where there are no legal implications for the collection and use of personal data, ethical considerations are central to humanitarian work. While some information is inherently sensitive, such as data about human rights violations or gender-based violence, leaks of any kind of personal data can result in individuals being targeted for violence or harassment due to ethnicity, religion, medical history, or just because they have received aid or worked with international organizations. Repressive governments may target refugees, other beneficiaries, and their families for persecution, even years later.

Because it is hard to predict what may lead to negative consequences, it is important to have consistent standards on what is personal information and how to treat it. Humanitarian organizations also need to honestly balance the criticality of their programming with the responsibility to uphold privacy. A crisis cannot be considered a blanket waiver to collect information without regard to risks.

Informed consent in humanitarian emergencies

Outside of emergencies, people regularly agree to share personal information. The basis for this sharing is *informed consent*, an ethical (and in some cases legal) mechanism that ensures that individuals voluntarily provide information with full knowledge of relevant risks.[22] While this process is fairly straightforward in an everyday transaction, in a humanitarian crisis it becomes much more complex, if not impossible, due to practical constraints:

- ***Urgency:*** Humanitarian operations are intended to save lives. This imperative can, rightly or wrongly, trump other considerations.[23]
- ***Unknown procedures:*** It is difficult for humanitarian agencies to predict how data will be used, who will have access to it and how it will be secured. It is therefore hard to convey the risks and benefits.
- ***Low literacy and technological awareness:*** Humanitarian programs often operate in areas with low literacy, making the use of standard consent forms difficult. A lack of familiarity with technology may obscure the fact that information could be available anywhere, in a matter of minutes and for years afterwards.
- ***Remote data gathering:*** Humanitarians increasingly collect data via satellites or other remote sensing tools, or are given access to data by governments or companies. As a result, individuals may not know what information has been collected on them, and humanitarians may not be able to ask for consent.

[22] Beyond data collection, informed consent is central to ethical humanitarian action, such as in the Humanitarian Accountability Partnership Standard Commitment, which calls for "upholding the right of people in need to receive assistance and protection on the basis of their informed consent."

[23] A 2002 discussion of research ethics argued that a "consent model might be waived during the acute emergency phase for public data collection activities (surveillance, outbreak investigations), but only for a short period of time." *Research Ethics in Complex Humanitarian Emergencies: Summary of a Workshop* (Washington, DC, The National Academies Press, 2002).

- ***Inability to give consent:*** The very dynamic of humanitarian assistance compounds these obstacles to informed consent. Almost by definition, those providing information need lifesaving assistance, making it unrealistic to assert that they have the freedom to choose to participate or not.

Because informed consent cannot be meaningfully obtained in many humanitarian situations, responsibility rests with humanitarian organizations to ensure that information is handled responsibly. Protocols for information protection and accountability must therefore be developed and put into practice.

Data protection guidance and standards

While details vary, existing guidelines and codes for collecting information in an emergency[24] largely agree on some common principles:

1. **Lawfulness and fairness:** Information should be collected and processed in a legal and fair manner.
2. **Specific purpose:** Information should be collected for a specific, legitimate purpose and *only* information needed for that purpose should be collected. People should be always clearly informed about the purpose of the collection of the data.
3. **Quality:** Data should be accurate and up-to-date.
4. **Security:** Data should be secured to prevent unintended uses, including the security of the channels by which the data is collected; the places, virtual or physical, where the data is stored; and of the tools used to exchange data between organizations.
5. **Accountability and supervision:** Adequate safeguards and clear lines of responsibility must ensure the responsible use of data. People have the right to know how their data is being used and this must be done within the framework of direct accountability to affected populations.
6. **Retention period:** Data should not be held indefinitely and should be destroyed when no longer needed.
7. **Rights of the subject to be informed, to access, to rectify and to object:** People should be informed about what personal data an organisation holds about them, with a mechanism to receive complaints and address concerns.
8. **Risk assessment:** The data collector should undertake a risk assessment, which should inform the design of the data collection process.
9. **Efficiency:** Duplication of information collection should be avoided to reduce the burden on individuals and communities.

While these principles represent a useful step, existing documents do not cover the full scope of humanitarian activity. In addition, implementation is hampered by a limited awareness among humanitarian actors, compounded by the fact that data protection standards remain under debate more broadly.

At the organizational level, humanitarian organizations need to adopt data protection policies and frameworks, guided by the UN's 1990 Guidelines for the Regulation of Computerized Personal Data Files and incorporating recent developments such as the Madrid Resolution,[25] tailored to the realities of humanitarian response and to the work of their specific organizations. However, collecting and sharing information is a joint venture and privacy protections are only as strong as the weakest link. There is a need for a wider agreement on a core set of principles as a basis for training, policies, and procedures. Clear policies will in turn help to make decisions about information collection and sharing informed and deliberate, rather than ad hoc, and to put the focus on people's needs and rights as a basis for decision making.

[24] These documents include the IOM's Data Protection Manual (2010), *The Professional Standards for Protection Work* (2013) and the Cash Learning Partnership's (CaLP) *Protecting Beneficiary Privacy* (2013).

[25] International Standards on the Protection of Personal Data and Privacy, adopted in Madrid on 5 November, 2009, at the 31st International Conference of Data Protection and Privacy Commissioners.

Part V: Threats to humanitarian information

The challenge of maintaining confidentiality of personal data through appropriate data security measures is multiplied by the proliferation of groups that may target humanitarian organizations. Failure to understand these new threats can put people at risk and undermine the trust humanitarian organizations require to do their work.

As more data systems and devices go online, there has been an explosion of cyber-crime, as well as cyber-warfare, defined as "any hostile measures against an enemy designed 'to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer.'"[26] The sophistication of techniques has also rapidly increased. Inexpensive and easy to use commercial spyware and other tools have expanded access to formerly military-grade capabilities, such as the Stuxnet virus used to sabotage centrifuges in the Iranian nuclear program.

The Age of Cyber-warfare

Motivations for cyber-attacks include:
Political attacks: Political attacks might target organizations perceived to be biased or to represent the international community or a particular country. Attacks could range from website hacking and other nuisances to attempts to undermine community acceptance or shut down operations.

Attacks on communities or groups: Perpetrators may want to target aid recipients, such as marginalized groups or displaced people. This motive could be linked to a conflict or political dispute, religious or ethnic tensions, or social mores, such as targeting women who report sexual or gender-based violence.

Attacks on humanitarian partners: Groups may see humanitarian organizations as a soft point of entry to government or commercial data sets or networks. For example, the Satellite Sentinel Project was targeted by groups interested in access to the satellite feed rather than data unique to the project.[27]

Criminal activity and fraud: Some information that humanitarians collect will be valuable to criminals. Account information for cash transfers is an obvious target, but other types of data may have value for insurance fraud, identify theft, or corruption.

Nuisance attacks that take over social media accounts or vandalize websites, as the Syrian Electronic Army has done to Human Rights Watch,[28] get the most attention. For humanitarians, however, attempts to steal data or to spy on a target are probably the greatest concern since they can endanger assisted people and aid workers.

Many cyber-attacks are not purely technical in nature, but "social engineering" efforts to trick the user into providing password information or installing malware. In Syria malware has been distributed through false Skype encryption tools, hijacked Facebook pages, a malicious link disguised as an investigation into the death of an opposition commander, and emails purporting to contain video evidence of military abuses. There are also reliable reports of people being tortured to give up their passwords, with their accounts then used to transmit malware.[29]

Malware and other tools are cheap and easy to use. For example, the DarkComet Remote Administration Tool (RAT) that was widely used to target Syrian opposition groups was available for free. Once malware is installed, the attacker has almost total access to the target's computer. They can access data, turn on the webcam and microphone, and log keystrokes to identify passwords.

[26] "Cyber warfare", ICRC, http://www.icrc.org/eng/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm.

[27] Interview with Nathaniel Raymond, Director of the Signal Program on Human Security and Technology at Harvard University, June 2014.

[28] Max Fisher, "Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Web Site and Twitter Feed", *The Washington Post*, 17 March, 2013. Available from http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/17/syrias-pro-assad-hackers-infiltrate-human-rights-watch-web-site-and-twitter-feed/

[29] John Scott-Railton, Citizen Lab, "Digital Security and Wired Humanitarians: Three Trends that Should Scare You", presentation at the 2013 Working Group on Emergency Telecommunications. Available from http://wget2014.wordpress.com/tag/the-citizen-lab/>

Even if a database is set up securely with the best encryption and technical data security, a single slip-up by a user can compromise the whole system. Preventing breaches requires both strong security for databases and servers, and awareness and training for all staff.

As humanitarian organizations begin using more sophisticated communication systems and internet-linked tools, other types of attacks are becoming possible as well. Although there are as of yet few examples, *social cyber-attacks* could use social media or other communication to spread malicious rumours or incite panic. In Assam, India in 2011, false social media messages, including doctored photos of violence from other situations, convinced people that riots and violence were happening in their areas, leading to a mass exodus.[30] Humanitarian actors may be vulnerable as they have systems that are trusted for their neutrality and are used to relay messages related to disaster and violence. If an actor wants to cause mass displacement, it is much easier to send out a false SMS blast from a trusted humanitarian source than to actually attack a village.

As humanitarians increasingly rely on infrastructure and devices linked to the internet, such as "smart boxes" for maintaining vaccine cold-chains or autonomous delivery systems,[31] they will need to be aware of the risk of attacks on this "internet of things" that could damage vital supplies or infrastructure and put people directly at risk.

Government surveillance and humanitarian work

Just as the tools available for cyber-groups or hackers have advanced rapidly, more governments have access to sophisticated interception and surveillance software.[32] More sophisticated versions of commercial spyware allow governments to target their own citizens and people in other countries.[33] In addition, some governments may work indirectly through allied groups termed Pro-Government Electronic Actors (PGEA).[34] And if humanitarian workers are not careful, their data systems, particularly biometrics or other individual or household level registration tools, can be co-opted into becoming an extension of state surveillance, even after a crisis ends.

This reality poses a difficult challenge for humanitarian actors, who are committed to a principle of neutrality and who work transparently with the permission of host countries, yet have an obligation not to cause harm to the people they aid. Humanitarians need to consider the level of surveillance and the wider political and security situation in a country when making decisions on what data to collect and who to provide access. This review will be particularly critical when working with civil society partners, who may be much more vulnerable to negative impacts from the leak of information to state security services. In some contexts, humanitarians may need to avoid collecting information they don't want to share with the government.

[30] Rebecca Goolsby, "On Cybersecurity, Crowdsourcing, and Social Cyber-Attack", Aaron Lovell and Lea Shanley, eds. *Policy Memo Series, Commons Lab within Science and Technology Innovation Program,* Woodrow Wilson Center. Available from http://www.wilsoncenter.org/publication/cybersecurity-crowdsourcing-and-social-cyber-attack

[31] See OCHA Occasional Policy Paper "Unmanned Aerial Vehicles in Humanitarian Response".

[32] The Blue Coat Packetshaper, a form of malware used for this type of surveillance, was found in Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela, according to research done by the Citizen Lab at the University of Toronto. See Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, 15 January, 2013. Available from https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

[33] Bill Marczak, et al, "Mapping Hacking Team's 'Untraceable' Spyware", 17 February, 2014. Available from http://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[34] Pro-Government Electronic Actors are defined as "Hackers and other electronic actors whose actions identify them as acting in support of a government, but whose direct affiliation with the government are unknown, imperfectly understood, informal, not subject to standard government hierarchies of command and control, or controversial." John Scott-Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution.* CIWAG case study series, 2013, Newport, RI, US Naval War College, Center on Irregular Warfare and Armed Groups.

Part VI: The Way Forward

The following section looks at what humanitarian organizations can do and are doing at the level of operations to address risks to privacy and data security.

Operational mechanisms for the principled use of information

While more organizations are adopting data protection principles, this is only the first step. Humanitarians must go beyond principles by integrating the protection of privacy into all stages of the programme cycle: project design, data collection, and storing, analysing and sharing information. More organizations need to take advantage of tools to protect the rights of data subjects, particularly in the absence of meaningful informed consent. These tools are particularly useful in the development of new technologies or methodologies, because they require organizations to evaluate risks and downsides before investing in an innovation.

Project design: due diligence, privacy impact assessments and ethical review boards

Codes of conduct require monitoring and enforcement through clear systems of accountability. At the organizational level, data protection officers or other mechanisms must answer critical questions: Is it necessary to collect information in the first place? What level of detail is necessary? Can data be analyzed and disposed of, or must it be kept?

As one tool for answering these questions, the governments of the United States, Australia, Canada and the United Kingdom use Privacy Impact Assessments (PIA) during project design to ensure that all aspects of privacy are addressed. Assessments have been deployed in humanitarian contexts, notably for WRAPS, an American cloud-hosted database used to process refugee resettlement applications.[35] A privacy checklist could be incorporated into donor proposal formats and other project documentation.

[35] See Worldwide Refugee Admissions Processing System (WRAPS) Privacy Impact Assessment. Available from http://foia.state.gov/_docs/PIA/101146.pdf

> ***Data can be either useful or perfectly anonymous but never both.***
>
> **Paul Ohm, University of Colorado Law School**

This approach would still require a clearer understanding of possible harms from privacy violations in the humanitarian context. PIAs and similar tools may be ineffective for new approaches or technologies, where risks are less clear. For these types of innovations, it may make more sense to use ethics review committees (ERC), most commonly found in medical research. The World Health Organization has a long established committee that must approve all funding that involves human research subjects, and Médecins Sans Frontières and Action Contre le Faim have similar mechanisms for new health and nutrition programs. For humanitarian projects, a committee comprised of sector experts, information management specialists, context and cyber-security experts and community representatives could assess project design against codes of conduct and explore the implications of new technologies or methodologies. While ethics review committees for research have been criticized as bureaucratic, the process could be streamlined for humanitarian emergencies or reserved for circumstances where time is less critical.

Any mechanism must address the reality that information technologies create risks just like medical or health interventions do, and their use in humanitarian contexts should be held to a higher standard of review than in the past.

Anonymization and re-identification

Project design must consider how much information to collect and retain. Highly detailed, or granular, data is more flexible and useful, but often humanitarian organizations only need overall needs or trends. To protect privacy, it is possible to *anonymize* data, such as replacing names with codes or removing other personal identifiers, or by *aggregating* data, showing data on several individuals combined.[36]

[36] There are a wide range of technical approaches to anonymization and aggregation, which have different trade-offs and limitations. These include data reduction, data quarantining, inference control, rounding, banding, perturbation, micro-aggregation, rounding and sampling among others.

Security safeguards appropriate to the sensitivity of the information must be in place prior to any collection of information, to ensure protection from loss or theft, unauthorized access, disclosure, copying, use or modification, in any format in which it is kept.

Professional Standards for Protection Work

Similar approaches can be applied to qualitative data, such as by redacting names or other details in a report.

The approach to anonymizing or aggregating data matters, because of the *mosaic effect*, in which "the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk."[37] Even a few data points, such as birthdate, sex and zip code, allow the identification of identify individuals with reasonable accuracy (87% in one famous study).[38] Effectively removing sensitive data fields is therefore extremely difficult, while aggregation requires a trade-off between the level of privacy and the level of detail that is retained. Humanitarian organizations have to think holistically about the data available rather than assessing the risks of a data set in isolation, and consider both *direct identifiers* such as name and date of birth, and *indirect identifiers* that can be combined with other types of information.

Information sharing and classification

Finally, too few humanitarian organizations have clear *information classification procedures* to sort data systematically into categories based on risk and to specify what can be shared. In a 2013 survey, just 11 per cent of OCHA Information Management Officers had a data classification system with levels of sensitivity and guidelines for how the data should be released.

Such a system requires a clear definition of what constitutes sensitive information and why. Securing data that could create negative consequences for affected populations and partners should be the priority over information that carries abstract reputational risks, such as internal discussion documents. These procedures also require an honest assessment of who has or needs access to data, as humanitarians increasingly share information with researchers, universities, and the private sector.

Classification should cover not just to who can access data, but also the format and standards for how information is shared. For example, the Assessment Capacities Project has four levels that determine who can access the data and the level of anonymization: unprotected, protected, restricted and confidential.[39]

Case Study 2 – Mobile Data Capture and Information Management in the Somali Shelter Cluster

In 2013, agencies working in the shelter sector in Somalia had an opportunity to construct a new system to collect and share data. They were restructuring the coordination mechanism known as the Shelter Cluster in Somalia and standardizing tools and methodologies.

The Shelter Cluster in Somalia partnered with mFieldwork, an organization started by humanitarian practitioners, to provide a mobile data collection platform for joint assessments, IDP settlement mapping and the submission of shelter project profiles. Mobile data capture allowed records to be geo-referenced and available in real time to the Cluster Coordination team in Nairobi. The results were used for response planning, joint appeals and coordination, providing substantial improvements in the evidence base.

However, the Cluster faced considerable complexity when deciding how to share information. The geo-referencing of the records was essential to their utility, but it also introduced

>>

[37] "Open Data Policy-Managing Information as an Asset", Executive Office of the President of the United States, 9 May 2013. Available from http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

[38] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," 13 August, 2009, UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available from SSRN: http://ssrn.com/abstract=1450006

[39] See the SNAP Information Sharing Classification System. Available from http://www.acaps.org/resourcescats/downloader/snap_information_sharing_classification_system/198/1396473548

>>
Personal and Community Identifiable Information, such locations of shelters and household information. Agencies also expressed a concern about reputational risk if their primary data was available to others.

The Cluster chose a three-pronged approach: 1) aggregated information, analysis and maps would be shared publicly through Cluster and OCHA websites; 2) members with shelter projects would have access to primary data for joint assessments, settlement mapping and shelter project profiles; and 3) members with shelter projects would also be given a protected area on the platform where they could share information with the Cluster Coordination Team but not other organizations. The Cluster also developed guidelines for the use of data collected through the platform to ensure common standards and principles.

Enhancing cyber-security in humanitarian contexts

In addition to these practical measures, humanitarian organizations should take a step back and consider the role of data security in their work. Much like physical security, cyber-security is a balancing act. A data security system effective against a really determined adversary will be expensive and labour intensive, and will seriously limit the capacity of organizations to share and collect data. It is crucial to limit efforts at information security to data that truly carries risks.

Humanitarian organizations should also ensure that only the minimum information needed is gathered and that it is stored and shared responsibly, as covered above. But dealing with the risks of attacks requires additional considerations. First, humanitarian organizations need to recognize information security as a fundamental aspect of operations. They will need to work more closely with data security experts when setting up networks and other tools, and ensure regular reviews of vulnerabilities and breaches. This has to be an ongoing process as often systems designed for one purpose are eventually used in different ways, but without appropriate adjustments to the security architecture.

All humanitarian workers, not just information management and IT workers, need training in basic data security protocols such as not using unknown flash drives, looking out for phishing and spoofing attacks, changing passwords regularly and protecting mobile phones. Humanitarian organizations may also need to work with their contacts and networks among civil society and affected communities to ensure that they understand the risks and are taking necessary precautions.

Just as no organization would go in the field without at least a cursory physical security assessment, humanitarian organizations and their partners should also conduct *cyber-security risk assessments* to test information systems and ensure awareness of possible threats. Are there groups already targeting civil society or international organizations? How prevalent and sophisticated is cyber-crime? The level of threat from cyber-groups may not correlate to the physical situation.

For cyber-insecure environments, basic security and services like Skype will probably not offer sufficient protection, although more advanced security tools can help protect data and IT systems or hide the user's location.[40] While these measures will not preclude information sharing, it will make it more difficult, so humanitarians should use these tools sparingly.

If someone steals your wallet, you'll know it. If someone successfully copies your hard drive … you may never know.

Journalist Security Guide

Of course, humanitarians can always move most of their work offline. Not connecting to the internet except in very circumscribed ways, having some computers that are never online, physically transporting data on flash drives ("sneaker-nets"), or even reverting to pen and paper are effective ways to protect data from cyberattacks, though at a great cost in time and efficiency. Yet physical files can also be lost, stolen, destroyed or copied, and the lack of back-ups

[40] These tools include the open-source GNU Privacy Guard, "off-the-record messaging" for chats, and the free anonymizing service Tor for web browsing and messaging.

makes the information even more fragile. In environments in which even advanced security is insufficient, humanitarian organizations may need to simply decide that collecting certain types of information is not worth the risk to vulnerable populations, particularly if the information is not likely to be used for a response.

Transparency, Humanitarian Cyber-Space and International Humanitarian Law

Beyond the chilling effect on sharing and coordination, there are other important downsides to a high-security approach. Even if the data is secure, encryption or anonymization can be a red flag that attracts more attention, just as armoured cars or flak jackets can make humanitarian workers more likely to be targeted. The greatest guarantor of security for humanitarians is in transparency, adherence to humanitarian principles, and efforts to increase acceptance in the local communities, coupled with advocacy to recognize certain types of cyber-attacks on humanitarian organizations as violations of international humanitarian law (IHL).

The concept of "humanitarian space", the idea that humanitarian organizations should be free from interference to evaluate needs, monitor the distribution and use of relief goods, and dialogue with the people,[41] can also be extended to virtual communities, a "humanitarian cyberspace" where aid organizations are recognized as not being legitimate targets. It may even be possible to engage in direct outreach and negotiations with the more organized cyber-groups and promote understanding of humanitarian neutrality and other principles within relevant online communities. Humanitarians can also enlist local "white hat" hackers or online activists to test and strengthen cybersecurity. This approach will require outreach in local languages and to online communities, and a nuanced understanding of dynamics locally and within the diaspora community.

Further advocacy and thought on when cyber-attacks on humanitarian organizations constitute a violation of IHL is also needed. The ICRC has found that "means and methods of warfare which resort to cyber technology are subject to IHL just as any new weapon or delivery system has been…" including the obligation to direct attacks only against military objectives.[42] Specifically addressing humanitarian assistance, Rule 86 of the Tallinn Manual on the International Law Applicable to Cyber Warfare, a non-binding study, states, "cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance."[43] In addition, cyber-attacks could also be seen as a violation of rule 32 of customary international law that "objects used for humanitarian relief operations must be respected and protected", as this is generally understood to also cover "destruction, misappropriation and looting".[44] A consensus that even non-disruptive attacks, like data-theft, constitute undue interference in humanitarian operations would be a powerful step. Regardless, humanitarian organisations should insist that governments or other belligerents also take steps to ensure the cyber-security of activities happening in their area of control.

[41] Wagner, Johanna G. "An IHL/ICRC Perspective on 'humanitarian Space'" *Humanitarian Exchange Magazine*. Humanitarian Practice Network, Dec. 2005. <http://www.odihpn.org/humanitarian-exchange-magazine/issue-32/an-ihl/icrc-perspective-on-humanitarian-space>.

[42] Furthermore, cyber-warfare does not have to produce permanent, physical destruction to be considered an "attack". See International Committee of the Red Cross, "International Humanitarian Law and the challenges of contemporary armed conflicts," October 2011, 36-38. Available from http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf See also "What limits does the law of war impose on cyber attacks?", 28 June 2013. Available from http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[43] Michael N. Schmitt (Gen. ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, United States of America, Cambridge University Press, 2013).

[44] "Customary IHL - Rule 32. Humanitarian Relief Objects." *Customary IHL - Rule 32. Humanitarian Relief Objects*. <http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule32>.

Part VII: Conclusion and recommendations

A more connected, data-driven humanitarian system creates an opportunity to save lives and reduce suffering, even as it raises concerns for privacy and security. On one hand, in a humanitarian crisis, in which any delay can cost lives, privacy concerns and consent may be justifiably ignored in the service of the greater good. At the same time, humanitarian principles demand greater moral accountability and consideration of potential harm. Humanitarians also need to address concerns that technologies are being tested without public debate or ability to opt-out.

The bulk of international assistance goes to long-term, complex crises and conflicts,[45] often in areas with weak governance and little regard for human rights, and in which sophisticated surveillance by governments and cyber-warfare by armed groups is increasingly the norm. By modelling best practices in the principled use of information and respect for privacy, humanitarian organizations can set a positive example and allay concerns about their neutrality. Below are some suggested initial steps:

1. Prioritize transparency and Evidence Based Humanitarianism

By increasing the use of open data platforms, information sharing and organizational transparency humanitarian organizations can model best practices and prioritize resources to protecting only the most sensitive information. Organizations should consider joining the International Aid Transparency Initiative, adopting open data standards and supporting initiatives to facilitate information sharing, such as the Humanitarian Data Exchange and the Open Humanitarian Initiative. Organizations should also consider "off-line" and "low tech" ways to share their data, making sure that the very people they collect data from, the affected communities, can perform their right to access data regardless of their literacy rate and technological access.

2. Support ethical innovation

As information technologies continue to develop, humanitarian organizations need to stay ahead of emerging risks to privacy. Projects using new or untested systems or technologies should be held to a higher standard of oversight, such as through ethical review boards, and full consideration should be given to the concerns of affected people and communities. Codes of conduct and other guidance should be regularly updated to reflect new developments and should have clear systems of monitoring and enforcement.

3. Adopt codes of conduct and procedures for the ethical use of information

All humanitarian organizations should have clear codes of conduct or policies for the responsible use of information, with a focus on the principled use of personal data. Beyond the agency level, humanitarian organizations and stakeholders should consider adopting a consensus set of principles or guidance for responsible use of information in humanitarian crisis. Codes of conduct at all levels should be supported with clear internal procedures and capacities for managing information, including anonymization, obtaining or waiving informed consent, and privacy impact assessments and other tools to determine what data should be collected.

4. Invest in risk analysis and information security

Humanitarian organizations need to invest in assessing and classifying data to determine what they need to collect and to hold based on potential risks. Organizations need to invest in strengthening their cyber-security, working with experts as needed, including through active checks for security breaches. All staff should be trained in basic data security practices. Evaluations of threats from cyber-groups in different countries should be factored into the design of programs. Humanitarian organizations should look to other sectors, such as human rights, to see what tools and protocols have already been developed.

[45] World Humanitarian Data and Trends 2013, OCHA.

5. Advocate for a "humanitarian cyberspace"

Organization should investigate ways to engage with online communities and other groups to promote the idea of a "humanitarian cyberspace" and to encourage recognition of humanitarian principles. Humanitarian organizations should advocate that cyber-attacks on humanitarian actors and information systems, as well as civilians, be considered violations of international humanitarian law where appropriate.

6. Advocate for legal frameworks for sharing data in emergencies

Humanitarian organizations should advocate for clear legal frameworks at both the national or international level to govern when and how information from affected populations is shared. Humanitarians should also consider partnering with private sector companies and industry associations, particularly in the telecommunications, internet and social media areas, to develop clear terms of use and agreements for when and how data is released in a crisis.

OCHA

United Nations
Office for the Coordination
of Humanitarian Affairs

OCCASIONAL POLICY PAPER

OCHA POLICY AND STUDIES SERIES
October 2014 | 011