HARVARD
HUMANITARIAN
INITIATIVE

Applying Humanitarian Principles to Current Uses of Information Communication Technologies: Gaps in Doctrine and Challenges to Practice

Nathaniel A. Raymond and Brittany L. Card
Signal Program on Human Security and Technology
Harvard Humanitarian Initiative
July 2015

The goal of this paper is to identify and address current gaps, challenges and opportunities that face the humanitarian sector as it seeks to apply traditional humanitarian principles to the increasingly central role information communication technologies (ICTs) play in 21st Century humanitarian operations. While much has been written about the roles ICTs may play in support of humanitarian action, there is an absence of literature addressing how core humanitarian principles should guide, limit, and shape the use of these technologies in practice.

Overview: New Technologies, New Challenges

ICTs are now an increasingly critical component of 21st Century humanitarian response operations during both natural disaster and armed conflict.[1] ICTs are employed in a variety of ways by a diverse and growing community of governmental, non-governmental, and most importantly, local communities and actors.[2]

Some of the more prevalent, ongoing uses of ICTs in current humanitarian contexts include:

- Remotely collecting and analyzing social media, geospatial and other sources of data;[3]
- Collecting and communicating information in order to improve situational awareness;[4] and

---

[1] "World Humanitarian Data and Trends 2014", UN Office for the Coordination of Humanitarian Affairs, December 5, 2014, http://www.unocha.org/data-and-trends-2014/downloads/World%20Humanitarian%20Data%20and%20Trends%202014.pdf.
[2] Irina Shklovski, Leysia Palen, and Jeanette Sutton, "Finding Community Through Information and Communication Technology During Disaster Events," Proceedings of the CSCW 2008 Conference, November 2008, http://jeannettesutton.com/uploads/cscw460-shklovski.pdf.
[3] "Shamanth Kumar et al., "TweetTracker: An Analysis Tool of Humanitarian and Disaster Relief," Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, 2011, http://www.public.asu.edu/~mabbasi2/papers/kumar2011tweettracker.pdf.

- Better connecting affected populations to response activities, including collaborative on-the-ground program design, management, and evaluation.[5]

Due, in part, to the rapid adoption of ICTs by both responders and crisis-affected communities, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) was the first UN agency to officially propose recognizing information during crises - and the corresponding ability to communicate it - as a basic humanitarian need in 2013.[6] Other traditionally accepted basic humanitarian needs, which are both protected by, and enshrined within international humanitarian law, include food, water and sanitation, shelter, and medical care.[7]

The growing acceptance that information and communication during crisis is tantamount to other recognized humanitarian needs, though still largely prescriptive and informal, is a major development with significant, unaddressed implications for the humanitarian field. The most major implication is that the crucial definitional and doctrinal work of determining what constitutes humanitarian delivery and support for ICT use and access to address this basic need has not yet occurred.

This gap has left practitioners in this burgeoning sub-field of humanitarian action without generally accepted humanitarian doctrine to guide its use and understanding of ICTs in relationship to humanitarian principles. As a result, the absence of accepted guidance has started to affect the degree to which humanitarian actors engaged in this work apply the humanitarian principles.

Some examples of the complex challenges that this gap has created include:

- No minimum standards or professional ethics for the provision and use of ICTs in humanitarian action;
- An absence of guidelines for navigating an increasing reliance on third party actors, particularly private sector companies, to provide basic data and infrastructure; and
- A lack of identified and agreed legal and human rights standards for the use and provision of ICTs and critical data;

---

[4] Nathaniel A. Raymond et al., "While We Watched: Assessing the Impact of the Satellite Sentinel Project," *Georgetown Journal of International Affairs*, July 26, 2013, http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/.

[5] "Communication During Disasters: Examining the Relationship between Humanitarian Organizations and Local Media," Internews, September 2013, http://www.internews.org/sites/default/files/resources/Internews_SIPA_communicating_disastes_2013-09.pdf.

[6] "Humanitarianism in the Network Age," UN Office for the Coordination of Humanitarian Affairs, April 2013, https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

[7] "Humanitarian Needs," Humanitarian Coalition, http://humanitariancoalition.ca/info-portal/factsheets/humanitarian-needs.

As humanitarian actors become ever more reliant on ICTs as part of their workflows, the consequences of this gap in doctrine, theory, and actionable best practices will likely escalate in scale, complexity and magnitude. If allowed to continue, this "blind spot" represents a clear and present threat to the future relevance, realization, and survivability of the principles themselves.

Applying ICTs According to Core Humanitarian Principles and Values

The four foundational humanitarian principles that help determine what constitutes humanitarian action are humanity, neutrality, impartiality, and independence.[8] They are defined as follows:

- *Humanity:* Human suffering must be addressed wherever it is found. The purpose of humanitarian action is to protect life and health and ensure respect for human beings.
- *Neutrality:* Humanitarian actors must not take sides in hostilities or engage in controversies of a political, racial, religious or ideological nature.
- *Impartiality:* Humanitarian action must be carried out on the basis of need alone, giving priority to the most urgent cases of distress and making no distinctions on the basis of nationality, race, gender, religious belief, class or political opinions.
- *Independence:* Humanitarian action must be autonomous from the political, economic, military or other objectives that any actor may hold with regard to areas where humanitarian action is being implemented.[9]

Additionally, the *NGO/Red Cross Code of Conduct* (hereafter, "Code of Conduct") also informs what constitutes core humanitarian principles and values.[10] Though inclusive of the four principles above, the Code of Conduct also includes some requirements specific to the Code. Some examples of the Code of Conduct's principles directly applicable to humanitarian use of ICTs include building response on local capacity; holding humanitarian actors accountable to those they serve and those they accept resources from; and the involvement of beneficiaries in the management of relief aid.[11]

Defining "Humanitarian" Use of ICTs Versus Defining "Humanitarian" Technologies

Defining "humanitarian" activities and "humanitarian" means and methods of delivering information and communication capabilities during crises in accordance with the four core principles and the Code of Conduct have, so far, been stymied to varying degrees. Current efforts have largely focused on defining what constitutes "humanitarian" technologies instead.

---

[8] "OCHA on Message: Humanitarian Principles." UN Office for the Coordination of Humanitarian Affairs, June 2012, https://docs.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf.
[9] Ibid.
[10] "Annex VI: The Code of Conduct for the International Committee of the Red Cross and Red Crescent Movement and NGOs in Disaster Relief." International Committee of the Red Cross, February 1996, https://www.icrc.org/eng/resources/documents/misc/code-of-conduct-290296.htm.
[11] Ibid.

Sandvik et al note that, "Technology is not an empty vessel waiting to be imbued with 'humanitarian meaning'; rather, society and technology engage in a mutually constitutive relationship."[12]

Thus, humanitarian practitioners should first agree doctrinal parameters for the appropriate use of technologies, including ICTs, in accordance with foundational humanitarian values. However, the current paradigm is often an effort to deem certain technologies and their uses to be considered "humanitarian".

This paper argues that doctrinal parameters should be defined first before a technology is designed, tested, and/or operationally applied in humanitarian settings. Normative application of core humanitarian principles and values to the potential operational uses of the technologies with affected populations, and an analysis of their possible impacts on affected populations and humanitarian actors, should be the preceding requirement of ICT-supported humanitarian action. At present, this process is almost entirely absent from the use of ICT by humanitarian actors.

This recommended approach contrasts significantly from assuming that the technical creation and social construction of technologies themselves can be considered to somehow be intrinsically "humanitarian". This "humanitarian-ization" of a technology is sometimes claimed by virtue of the design process, intended use or physical characteristics of the software, hardware, platforms, or other products themselves.

In the following sub-sections, current challenges and their potential operational impacts relevant to each of the core four humanitarian principles are presented with pertinent examples, when possible. Suggested critical actions and next steps are suggested when applicable.

The Principle of Humanity

Avoiding Harm from ICT Use

The application of ICTs in a way that is consistent with the principle of "humanity" centrally involves "...assuring respect for the individual" as part of humanitarian action.[13] Pictet's commentary on the principle of "humanity" explains what assuring respect for the individual means as follows: "...do not harm, do not threaten, spare the lives, integrity and the means of existence of others, have regard for their individual personality and dignity".[14]

---

[12] Kristin Bergtora Sandvik et al., "Humanitarian technology: a critical research agenda," *International Review of the Red Cross*, 2014, http://www.humanitarianstudies.no/2014/12/30/humanitarian-technology-a-critical-research-agenda/, 7.

[13] Jean Pictet, "The Fundamental Principles of the Red Cross: Commentary," International Federation of the Red Cross and Red Crescent Societies, https://www.ifrc.org/PageFiles/40669/Pictet%20Commentary.pdf, 17.

[14] Ibid.

In the context of information and communication during crises, the use of ICTs by humanitarian actors, as well as the ability of populations themselves to access and use them, must be implemented in a way that actively avoids additional harm and threats to individuals. This directive to "do no harm" is a clear call for agencies to ensure that their collection and use of both individually identifiable data, as well as non-individually identifiable data that may nonetheless affect individuals, does not further endanger populations.

Additionally, "regard for their individual personality and dignity" can also be interpreted as applicable to the humanitarian use of ICT. For example, data that humanitarian actors collect must both be protected and presented in a way that ensures the privacy, rights, and individuality of crisis affected individuals. The issues of ensuring equitable distribution of ICT assets, capabilities, and programs with respect to gender, cultural, and religious differences are also paramount.

An Absence of Ethical and Technical Standards

The absence of professional codes of ethics and corresponding technical standards for making these operational determinations has impeded the implementation of the principle of humanity in ICT-supported humanitarian work. Without many real world case studies available that show how the humanity principle may have been abrogated in the past, it will be difficult to prevent its violation, however intentional or unintentional, in the future.

Potentially appropriate urgent actions for the humanitarian community to pursue include the development of retrospective case studies documenting incidents where the use of ICT by humanitarian actors may have conflicted with the humanity principle. The goal of these case studies should be to provide a base of evidence for developing technical best practices and ethics codes, including risk assessment procedures and strategies for involving stakeholder communities in project design and management consistent with the Code of Conduct.

The Principle of Neutrality

The principle of neutrality plays a critical role in the humanitarian application of information and communication during crises. Humanitarian actors must ensure that they do not collect data; deploy data collection tools and infrastructure; release data; and engage in programs involving information and communications capabilities that favor one demographic group, political party, or armed actor over another.

Especially in situations of armed conflict, humanitarian actors must ensure that the data and systems they employ do not provide any tactical military or operational advantage to parties engaged in hostilities. As demonstrated by Raymond et al in the case of using satellite imagery for humanitarian early warning in Sudan, the provision of unique, otherwise unavailable assets for situational awareness in an armed conflict environment may increase the volume and quality of actionable information available to alleged perpetrators of human rights abuses:

> Analysts were thus able to better target their collection of imagery to be more relevant to the real time security of vulnerable populations. This move towards prediction forced [Harvard Humanitarian Initiative] researchers to weigh the unintended consequences of publicizing information and images about vulnerable populations when the audience included the parties to the conflict themselves. This task was especially difficult given [Satellite Sentinel Project's] access to near-real time satellite imagery and the ability to rapidly share those images globally through the international and Sudanese domestic media.[15]

This situation, regardless of whether satellite imagery or any other unique data source is being employed, represents both an operational, curricular, and doctrinal challenge to the principle of neutrality that must be addressed. At present, the humanitarian community is potentially engaged in work that may not only inform and assist affected populations, but also parties to hostilities themselves targeting those populations; potentially providing armed actors otherwise unavailable operational and military advantages.

Providing applicable guidance for how to operate (or not operate) in these situations consistent with the neutrality principle is required. In the absence of agreed doctrine, humanitarian actors will likely to continue to engage in ICT-based programs and projects that may not comply, however unintentionally, with the current understood definitions of the principle of neutrality.

The Principle of Impartiality

Presently, it can be argued that the application of ICTs - both for the collection of data and supporting communication by affected populations - is often not applied in a manner consistent with the humanitarian principle of impartiality. Two reasons may contribute to the difficulty of attaining the impartial delivery of information and communication related programs and strategies.

Needs Assessments and Minimum Standards

First, acting impartially depends on determining what regions and populations most urgently require ICT-supported humanitarian assistance. Currently, an evidence-based approach and theory for conducting ICT and data-related needs assessments of affected populations in a tested and accepted way does not exist.

The available literature relevant to the subject of assessing the ICT needs of a population affected by humanitarian crisis largely focuses on identifying crisis-affected populations themselves through the use of ICTs during and after an emergency.[16] While sometimes of value during an initial needs assessment phase, this approach does not address, demonstrate

---

[15] Ibid., 4.

[16] Linus Bengtsson et al., "Improved Response to Disasters and Outbreaks by Tracking Population Movements with Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti," *PLoS Med* 8(8): August 30, 2011, http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001083.

or define what the communications and data needs affected populations, as well as those assisting them, may have in specific crisis contexts in order to better survive and recover from the emergency.

Thus, it is unknown how local actors, governments and agencies should meet those needs. (*See section on "Towards Minimum ICT Standards".)* Relatedly, even when those needs are known, no minimum standards for the provision of interventions exist so that the needs can be met. Realizing the principle of impartiality in this work will be extremely challenging without humanitarian actors having capacities and capabilities in these two underserved areas of practice.

Applying the principle of impartiality in ICT-supported humanitarian responses must be rooted in evidence regarding a population's physical and ambient ICT and data requirements. This approach contrasts with the current de facto approach that often stems from what interventions and approaches are most available and feasible for remotely based, data donor-dependent practitioners.

Data Donor Dependency

This second, critical issue, "data donor dependency", is also impacting the application of the principle of impartiality. Humanitarian actors now often depend on donations of hardware, software, and in some cases, the data itself, such as satellite imagery, to perform basic aspects of their work. These donations of data, assets, and bandwidth often come from private companies and governments supporting ICT-related humanitarian work.[17]

Instead of being able to make needs-based requests for what is required, practitioners are at risk of tailoring their ICT-related work to the specific scenarios in which donors, increasingly private companies, might make data, tools, and partnerships more available. Sandivik et al note:

> ...there is a significant but little understood political economy aspect to the rise of humanitarian technology: both the military industry and the surveillance industry are looking for new markets – and the type of legitimacy that partnership with a humanitarian actor can provide.[18]

The current approach is an understandable reflection of certain operational and economic realities inherent in the unique and relatively recent emergence of the humanitarian ICT space - which depends, in many cases, on "data philanthropy" as a precondition to exist.[19] However,

---

[17] "How Public-Private Partnerships Between Telecommunications and Humanitarian Agencies Can Save Lives," Aid & International Development Forum, March 19, 2015, http://reliefweb.int/report/world/how-public-private-partnerships-between-telecommunications-and-humanitarian-agencies.

[18] "Humanitarian technology: a critical research agenda," 17.

[19] Robert Kirkpatrick, "Data Philanthropy is Good for Business," Forbes, September 0, 2011, http://www.forbes.com/sites/oreillymedia/2011/09/20/data-philanthropy-is-good-for-business/.

the prerequisite of humanitarian, needs-based priorities matching government, donor, and corporate ICT priorities for philanthropy is a major issue with profound implications for the field.

While many aspects of humanitarian response beyond ICTs do rely on priority setting and access provided by actors that are not needs based, the humanitarian ICT space is a particularly acute and unique example of this phenomena. Humanitarian reliance on the more formalized structure of “data philanthropy” in order to use ICTs effectively should be viewed as fundamentally inconsistent, in many cases, with the full application of the principle of impartiality.

There are many potential examples of this phenomenom. For example, a common instance includes when a humanitarian agency may need data or ICT assets from a government or private sector entity to support a population and/or region that the donating entity may not politically or economically want to support.

In those moments, it is crucial that humanitarian actors using ICTs do not change their assessment of what data or assets are optimally needed to assist specific affected populations based on their initial professional judgment. Without doctrinal, needs-based and rights-based guidance for practitioners, the principle of impartiality is increasingly endangered by the current “data donor-centric” approach.

Utilizing ICTs in order to provide affected populations access to information and communication during crises is not incompatible with pursuing private sector partnerships. In many contexts, the opposite may be the case. These partnerships can offer otherwise unique and unavailable data and assets that provide the potential significant positive impacts for large groups of people in need.

However, the principle of impartiality, requires humanitarian actors to create “bright lines” to guide these partnerships that currently do not exist. These bright lines must put humanitarian judgments about the needs of the most affected ahead of prospective commercial or political interests, including technology research and development.

Without accepted humanitarian parameters, the principle of impartiality will be difficult to realize within the current political economy in which humanitarians are trying to use data and ICTs. This political economy, as Sandivik et al notes above, is primarily shaped by entities that are not required nor intended to operate on an impartial, needs-based basis like humanitarian actors.

The Principle of Independence

As mentioned in the section above, the rise of governmental and private partnerships as a recurring prerequisite for ICT-supported humanitarian responses is a critical factor shaping the landscape of 21st Century humanitarianism. The principle of independence, in addition to the principle of impartiality, is also challenged by the apparent growing reliance of humanitarian

actors on government and private sector entities for raw data and communications infrastructure.

Access and Consent

Potential challenges to the humanitarian principle of independence in ICT-supported humanitarian work can manifest themselves in some of the same ways that independence can be risked in "analog" humanitarian responses. For example, governments can put restrictions on cyberspace and telecommunications the same as a military checkpoint can block a humanitarian convoy from delivering food to a village. Civilians attempting to call for help can be silenced by having their cellular grid disconnected at crucial moments of impending harm the same as they can be silenced when faced with threats of physical violence from armed militias.

The underlying principle of the "consent" of sovereign states to allow humanitarian aid operations applies to ICT-supported humanitarian action as well. Without the consent of the state or governing power (in cases of occupation), humanitarian actors cannot provide aid to a population.[20] However, in the case of providing consent for ICT-related aid operations, private companies are now part of the consent equation.

Conflicting Loyalties

This new, more ICT-specific version of long standing challenges to the independence principle is expressed well through the concept in medical ethics known as "dual loyalty". Benatar and Upshar provide a helpful definition of dual loyalty in the medical and public health context as the extent to which ethical loyalty is "deflected from a patient to a third-party (e.g., an insurance company or a prison commander)...".[21]

In this case, that definition can be applied to scenarios where a humanitarian actor's primary loyalty to serve those affected by crises, either natural or man-made, is deflected because of power relationships with a third-party rather than the affected population. The potential for this phenomenon to occur in ICT-supported humanitarian response, with real implications for the rights and needs of affected people, is significant.

Humanitarian actors engaged in ICT work often rely directly on governments and private sector enterprise (who receive their licenses to operate from national governments) to provide direct access, not only to data, but also to the telecommunications infrastructure used by affected populations themselves. The Groupe Speciale Mobile Association (GSMA), which represents the interests of the global mobile telecommunications industry, has tried to respond proactively

---

[20] Cedric Ryngaert, "Humanitarian Assistance and the Conundrum of Consent: A Legal Perspective," Amsterdam Law Forum, 2013, http://amsterdamlawforum.org/article/viewFile/298/483, 1.

[21] Solomon R. Benatar and Ross E. G. Upshur, "Dual Loyalty of Physicians in the Military and in Civilian Life," *American Journal of Public Health* 98(12), December 2008, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2636540/.

to some of the challenges related to granting humanitarian access to this infrastructure with a 2015 "Humanitarian Connectivity Charter".[22]

While an important first step towards providing some form of principles-based structure to this work, the GSMA Charter is neither based on humanitarian principles, nor does it comprehensively address how telecom companies should respond consistently to different types of crises, such as armed conflict and government crackdowns on protests. Humanitarian actors are increasingly having to maintain their independence in operational, ICT-specific spaces shaped by guild level charters and inter-corporate codes of conduct that define what access they may or may not have to ICT data and systems.

The potential for "dual loyalty" scenarios and the emerging challenge of corporate consent for data and systems access related to ICTs is critical. However, commercial and governmental efforts at shaping and structuring the process of consent and provision for ICT-related action during crises is important and should be generally welcomed.

Humanitarian actors are not yet equipped doctrinally to manage ICT-specific dynamics that have the potential to "deflect" their loyalty from affected populations when negotiating "consent to access" with those that control crucial data and systems. Preserving the independence of humanitarian actors engaged in ICT work is directly linked to their ability to operationalize how to put affected people first in these complex contexts. Developing a rights-based framework for information and communications during crises will be an essential first step in this process.

Conclusion: Minimum ICT Standards is the First Step Forward

Operationalizing the four humanitarian principles above in the networked age depends not only on applying traditional humanitarian doctrine to the new operational and organizational challenge of ICT-supported humanitarian action. It also depends centrally on the agreement of minimum "Sphere"-type standards for its assessment, provision, delivery and support.

These minimum standards, which should be grounded in the core four humanitarian principles, are required for measuring realization of the right to information and communications in crises, in addition to attempting to meet the basic humanitarian need. While this paper does not intend to fully identify and frame these minimum standards, there are six main areas that require broad minimum standards.

These areas requiring minimum standards are presented below with illustrative examples of some of the specific issues relevant to each area:

- *ICT and data access and capability needs assessments:* Humanitarian actors, local communities and governments should have commonly agreed standards for assessing

[22] "GSMA Launches Humanitarian Connectivity Charter," GSMA Press Release, March 2, 2015, http://www.gsma.com/newsroom/press-release/gsma-launches-humanitarian-connectivity-charter/.

the ICT and data access and capability needs of affected populations across crisis contexts.

- *Network access, data storage, charging, and hardware:* Minimum standards should be agreed for what level of mobile network access and coverage is optimal, safe, and required in different humanitarian scenarios, including displaced population camps, transitional housing, and host community settings. These standards should include recommended standards on providing phone charging infrastructure, cloud storage per person for individual and family documents, basic mobile device requirements when included in NFI (non-food item distribution) packages, and access to phone cards and money transfer resources in camp settings.

- *Protection standards for vulnerable populations involved in ICT programs:* Minimum standards, including the security of individually identifiable information, are needed for those providing ICT services that affect vulnerable populations, including women, children, and those of ethnic, religious, and political minorities that may be targeted by armed actors.

- *Technical standards for collection, release, presentation, and security of humanitarian data:* There must be common standards for what information is collected and released through multiple types of ICTs, including satellite imagery, mobile and text-based crowdsourcing platforms, and others. These standards should include basic security guidelines, annotation and presentation standards, and identify best practices for analysis.

- *Standards for negotiating, soliciting, accepting, and using in-kind ICT and data contributions:* Humanitarian actors need minimum standards consistent with core humanitarian principles for how to appropriately review and process in-kind and monetary donations related to ICT access and data analysis programming.

- *Guidelines for use of ICTs in early warning and community communication activities:* General approaches should be identified for using various forms of data and ICT to provide early warning to communities at risk. Also, best practices and minimum standards for centrally involving local partners and communities in ICT-related programming design and deployment decisions, including issues of consent and responding to critical incidents such as security breaches.