Vintage 72 | No.. 2 | 2014 | 253-262 | ISSN 0020-577X © University Press | NUPI |
www.idunn.no/ts/ip International Politics | Year 72 | No.. 2 | 2014

"Do no harm": Consent and policy in crisis?

CHRISTOPHER WILSON MA, Knowledge Lead, the engine room
wilson@theengineroom.org

"Do no harm": Consent and privacy in crisis?

Christopher Wilson

MA, Knowledge Lead, the engine room

wilson@theengineroom.org

Given the humanitarian imperative that humanitarian action must not cause damage or expose recipients to risks, see this entry on a specific aspect of digital relief work, namely how to understand the requirements of privacy and consent in emergency situations.

Mobile and web-based information and communication technologies have created new opportunities for both the collection and use of information in humanitarian work. While new tools create new opportunities, creating new challenges.

More and better information can be used for preventive notification, reporting, logistics and coordination and the so-called'spillifisering`. 1 Despite major technological optimism is still uncertain what is information technology's potential and actual contribution to humanitarian crises. At the same time, there is increasing recognition that the real-time exchange of information, large amounts of metadata ("big data") and low capacity to analyze and process information creates unexpected risks and challenges when it comes to personal consent and privacy. Challenges related to privacy, particularly consent and anonymity, is well known from traditional humanitarian aid, and has long been a subject of political debate. New technology brings yet with new issues: information spreads rapidly and uncontrollably, reuse and modification can go on forever, and the digital divide reflects also often part relationships in conflict.

The implications of these issues for privacy and consent has barely been addressed in the humanitarian discourse. One of the main contributors to the influential OCHA report humanitarianism in the Network Age (2013) is that it refers to the important issues that arise around privacy, ethics and safety. But the report does not go so far as to link the issues surrounding the use of digital information to the traditional requirement by humanitarian actors that information must be used ethically and in a manner that maintains the humanitarian actors' protection responsibilities.

This link may be difficult to establish, since the free flow of digital information across stakeholders and platforms complicates the question of ownership, control and responsibility. In humanitarian crises, there is not always a direct relationship between those who communicate and use information and those who have given up knowledge, observations or data, or discussed in reports and messages. In connection with humanitarian crises divided photographic representations of

suffering and desperate pleas for help on social media. Opening of biometric or "big data" for the coordination, support and monitoring human rights violations against third parties. Questions about responsibility and ownership of this type of information is particularly difficult (see Iacucci 2013; Hosein & Freshly 2013).

In most humanitarian crises can be argued that the humanitarian mandate already has a direct responsibility to protect groups and individuals who give up information or contemplated herein. This responsibility has four interrelated sub-areas: 1) identity and anonymity; 2 2) consent; 3) control, 3 and 4) reuse of data and information.

For each of these sub-areas already exists humanitarian guidelines. Of these four, it approval category that is most developed in ethical terms, while the implications for humanitarian practice and responsibility in a digital information landscape is most uncertain. This article will therefore examine this concept and how it is operationalized in the digitized humanitarian work. In the following discussion first, on the basis of health research, how the standards for consent has evolved. Then I examine the current information ecology in humanitarian practice and potential hazards by collecting and using information weighed against the possibility of more effective and targeted relief. The contribution concludes that the need for guidelines and rules for the use of information in emergencies is much needed, and provides some concrete step in this process.

Standards for consent: from health research to "digital crisis map» 4
The term "consent" means in general that those who give consent does so with a minimum of relevant information as possible for "informed consent". Belmont Report (1979), who referred to health research, sharing conditions of consent into five: two concerning the application, and three that apply process:

Consent required in (i) any type of research (ii) in human subjects. For that consent can be said to exist must be the subjects of science (iii) be made aware of the research project's objectives, methods and possible consequences (including risks and damages) and (iv) have a fair opportunity to consider their participation and have an opportunity to ask questions about all aspects of research before they consent. (V) Participation in research must always be voluntary.

Although health research area distinct from humanitarian crises, these terms also relevant here represents a broadly recognized term that also underpins the understanding of consent in a humanitarian context. That leaves the question of how this understanding can be used for digital humanitarian information.

So far it has been developed a few guidelines that are based on new media and information strategies for the use and trying to identify responsibilities and procedures, but does not provide operational guidance. For example, the GSMA's Code of Conduct for Disaster Response (GSMA 2013) aims to improve coordination between telecommunications providers and humanitarian agencies during natural disasters. The document mentions however privacy only once, namely when it determines that information gathering should take place in accordance with national laws and regulations. Furthermore, the document recommends that the SMS information obtained from individuals and other types of "personal data" should not be shared with third parties without consent. However, there is no guidance as to what the requirements are for an "ethical" approval or how consent should be obtained.

The International Red Cross (ICRC) is the one of the major humanitarian actors who have made the most progress in the effort to develop guidelines for the use of digital emergency information. ICRC Professional Standards for Protection Work in 2013 concerning the regulation of sensitive information and presents 15 standards for humanitarian actors to identify and deal with ethical

challenges that come with the use of humanitarian data. 5 This is so far the most detailed and influential contribution of the sector . 6 ICRC Professional Standards for Protection Work includes two standards that are particularly relevant to the question of consent, namely the requirement for risk analysis and informed consent:

40 Protection Actors who systematically set up information retrieval over the Internet or other media must analyze the potential risks that the collection, sharing or public display of information can lead and corresponding customize the way information is collected, controlled, used and shared (ibid .: 86).

48 Protection actors must incorporate the understanding of informed consent when they requested help from the public or individual members of a community to spontaneously send information through SMS, an open web platform, or any other form of communication or when using information already available on the internet (ibid .: 95).

ICRC guidelines cover a number of difficult issues in a very good way. However, the guidelines do not sufficiently clear at the operational level. Who, for example, responsible for setting the guidelines into practice in the field, both at the organizational level and in relation to employees? At the organizational level, lack the resources, the individual lacks capacity. Sees these practical obstacles in the context of the conflict between the ethical responsibility for information protection and the purpose of quick and effective relief, one may question whether these standardization exercises contribute to norm setting - and whether these standards are possible to implement in practice.

New Challenges: when, who and how should consent be given?
Today's information ecology is characterized by easy collection, instant sharing and unlimited reuse of information. In this reality, it is far from easy to study when consent should be obtained. This assessment must necessarily be based on thorough risk assessments, where potential hazards by collecting and using the information to be weighed against the possibility of applying it in an appropriate and efficient manner. For example, establishing a system for SMS reporting to notify and document attacks against civilians. The idea that consent is ethically required from a protection perspective is based on the likelihood that the SMS reports may put individuals at risk when they contribute reports or reports, and because their identity can be traced. Study of consent in such a situation requires both an understanding of the threat and how a potentially threatened local population can understand and access the reports (they can monitor SMS traffic, and is the collaboration with telecommunications providers?), And what information can be used of the various participants. Deep local knowledge is essential to investigate whether consent is needed, but is not necessarily present among humanitarian actors to study the situation.

If one assumes that it is possible to investigate whether consent is required, there remains a number of practical questions of who should give consent and how. Questions about who consented to be hedged is complex: In addition to directly contributing information, one must consider the need for the consent of the parties who are only indirectly affected and third parties. In the text above example, this means that in addition to those sending SMS reports, may also need to obtain consent from the individuals referenced in reports or from groups and stakeholders who may be exposed to reprisals from local groups or governments.

Even when it is clear that consent is ethically required and who should provide it, it can be practical and strategic barriers to ensure that this actually happens properly. Firstly, it can be difficult to identify and connect with individuals and groups you want to get the consent of. If in the previous example appears that those who are sending SMS reports thus being exposed to an unacceptable risk, it is possible that even the seeking consent may entail the same risks. The question is whether

it needed permission to seek consent. When should the decision of acceptable risk lie exclusively with the humanitarian actors? You may find that humanitarian actors build up a reporting system does not have direct contact with other parties that may be described in the reports. Have informants, who often will be the recipients of aid, equal access to the media as humanitarian actors receiving reports? Looks informants humanitarian efforts in a positive light? The same questions can be prepared by third parties that may have economic or security problems after the information has been provided by others. For large groups, it must also be determined whether to seek consent through representatives of the group, or cause to reach out to all potential interested with information about what you intend to do. In such a situation there will again be a question whether consent should be given through active equivalent, or may be deemed to consent exists if the same is not given?

According to Almon & Farkas (2013: 10), these challenges are handled with well worded privacy policies and that informants can be considered to have given consent when they read these guidelines. But this does not help with the question of when consent is required and by whom, nor handling the consent of the second and third parties. There is probably no simple answers to these questions, which require active investigation and knowledge of the context and the kind of technology that will be applied in the specific case.

Even when you eventually arrive at appropriate answers to these questions, it may remain a number of challenges related to the information that potential informants could go on. For consent to be informed, those who contribute are given information about the purpose and risks of information-gathering process (process criteria ii and iii) that leads us to a familiar dilemma: the more information about the risk, the less willingness to participate. This is particularly challenging in a situation where informants probably have given insight into the technological information. It is for example difficult for a subsistence farmer with no formal education or access to the internet to understand and assess the likelihood that a militia group will have access to software that will enable it to monitor the cellular network or identify individual contributors. A real assessment of the risks to which participation involves (condition 4), also requires broad knowledge of how the political and legal situation will change over time - how will the balance of power be in five years, how will the requirements for data storage be in ten years? To carry out such assessments are difficult enough for experts. For any informants with broad knowledge, it is not only difficult, but may require the introduction of some possibly frightening information about how technology can be used. To present informants with information they need to give informed consent, you simply lower their motivation to contribute.

The central tension: norms and practices
OCHA report humanitarianism in the Network Age recommends that by 2014 will establish a series of guidelines and standards for the ethical use of data in humanitarian work. Central among these will be a "do no harm" standard for digital Relief:

By 2014 it should be developed 'do no harm' guidelines for ethical use of new types of data, including protocols to safeguard the privacy and security guarantee informants, and develop frameworks to keep players accountable for following ethical and technical standards. It should be ensured that they are addressing the various issues around privacy, liability and security in a clear way (OCHA 2013: 60).

At the same time, the report underlines that "[b] ekymring around information and data may not be a reason to avoid the use of new communication technologies in emergencies" (ibid .: 46).

The basic problem of this article is the question of how to balance efforts to ensure ethical treatment and protection of humanitarian information with the objective of providing rapid and effective

humanitarian assistance. A qualified assessment of whether consent is required, with subsequent efforts to ensure informed consent is resource and time consuming. When it is unclear what is required to secure consent, when the need for consent is not a fact and it is uncertain whether approval will be granted, it may be hard not to prioritize speed and efficiency.

This dilemma has been evident in several humanitarian crises. The dilemmas surrounding the use of SMS to create digital crisis map ("crowdmapping") and coordinating the humanitarian response in the aftermath of the earthquake in Haiti in 2010, is relatively well documented. Over 10,000 SMS messages were collected and mapped by an informal gathering of volunteers, led by Patrick Meier and in collaboration with Fletcher School at Tufts University, Thomson Reuters Foundation, InSTEDD, US State Department and others. SMS messages were surveyed under the name "Ushahidi 4636," 7 and as there was a great demand for data from various stakeholders, including US Marine Corps and U.S. Coast Guard, the volunteers had to weigh the considerations of privacy and the desire to act as soon as possible . Patrick Meier describes the dilemma this way: "... the more open data is, the more likely it is that the information is useful for professional emergency workers, local actors and diaspora - but Goodbye Privacy" (Meier 2013).

Instead thorough risk analysis and assessment of the need for consent on the basis of the current situation, took the leaders of Ushahidi contact with two Western lawyers and asked them for their opinion. Both lawyers argued that consent was implied as individuals had sent information by SMS. On the basis of this Ushahidi opened the 4636 reports they had gathered, and argued for the concept of "implied consent" (ibid.).

Without taking a position on whether this was the right decision or not, it is contemplated that this represents a general perspective among humanitarian actors. Again, as formulated by Patrik Meier:

I will never again spend 24 hours plus to discuss whether time-sensitive life-or-death-SMS may or may not be identified because of the uncertainty surrounding privacy and protection responsibilities - 24 hours during a search and rescue phase will almost certainly make life or death (Meier 2013).

While this is a legitimate argument, it does not remove the imperative to protect individuals as well as groups from danger and harm - even when it comes to risks related to privacy and security. Without specific guidelines for how to identify and weigh competing considerations, the alternative usually win in humanitarian assistance. Unfortunately, it is precisely at this level that the guidelines IRCRs Professional Standards for Protection Work fall short. Charting the responsibilities and possible risks is an important first step, and it is positive that this document presents the assessment criteria that can help humanitarian actors to assess the specific context in which they work. But without more details and guidance on how this balance should be taken, the humanitarian actors without technological expertise and policies and procedures to choose fast and effective action.

Conclusion

This contribution has looked at how consent can be understood and implemented in a humanitarian context characterized by digital media and the free flow of information. Although the concept of consent is broadly recognized in humanitarian work and closely related to the humanitarian protection responsibility, it is unclear how it can or should be implemented in humanitarian crises. Today's digital communication complicates traditional approaches to consent at the strategic and practical levels. This requires deep knowledge and special capabilities that are not present among the majority of humanitarian actors. It also requires assessments and procedures that could be considered competitive with the humanitarian imperative of rapid and effective action. It is far from clear how these tensions should be handled. The discussion on ethics and digital media have slowly started to touch these issues and the development of humanitarian policies have begun to enter the key issues, but does not provide operational guidance necessary to study and implement the consent

on the ground.
For the development of standards and practices, it appears that consent debate follows two parallel tracks. In the field made specific assessments of alternative actions ongoing, and often without any further assessment of risk or privacy. Meanwhile, several international organizations to take seriously that this is the real issues they need to address. Based on the applicability and legitimacy considerations, it is important that efforts to develop guidelines and standards both incorporates a bottom a horizontal perspective, if such guidelines are developed in collaboration with field staff, they are perceived as little more than bureaucratic stumbling blocks and with little chance of to be used in emergency situations on the ground. At the same time, standards must be developed with adequate technical and ethical skills, which help workers possess. In addition, coordination between data experts and aid workers (both professional and volunteer) central - but it is unclear how this cooperation should look like. The first step is a broader dialogue on these issues and better understand how they (can) handle the emergencies in the field.

Literature

Almon, Gabriele & Otto Farkas (2013) Issues and Opportunities for Humanitarian Protection and Accountability in the Digital Age: Working Paper. World Vision.
GSMA (2013) Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters. Available på: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/Towards-a-Code-of-Conduct-SMS-Guidelines.pdf . Reading date: 13/02/2014.
HAP (2010) 2010 HAP Standard in Accountability and Quality Management. Available at: http://www.hapinternational.org/ . Reading date: 13/02/2014.
Hosein, Gus & Carly Freshly (2013) Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. London: Privacy International.

Iacucci, Anahi Ayala (2013) The Conundrum of Digital humanitarianism: When the Crowd Does Harm . Available på: https://crisismapper.wordpress.com/2013/11/15/the-conundrum-of-digital-humanitarianism-when-the-crowd-does-harm/ . Lesedato: 02/13/2014.
ICRC (2013) Professional Standards for Protection Work. Geneva: International Federation of the Red Cross (ICRC).
Meier, Patrick (2013) Launching: SMS Code of Conduct for Disaster Response. Available at: http://irevolution.net/2013/02/25/launching-sms-code-of-conduct/ . Reading Date 13/02/2014.
Mission 4636 (2013) Collaborating Organizations and History. Available at: http://www.mission4636.org/history/ . Reading Date 13/02/2014.
National Commission for the Protection of Human subjects of Biomedical and Behavioral Research (1979) Ethical Principles and Guidelines for the Protection of Human Subject of Research (The Belmont Report). Available at: http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html#xinform . L esedato: 02/13/2014.
National Geographic (2012) How Crisis Mapping Saved Lives in Haiti. Available at: http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/. Reading Date 02/23/2014.
OCHA (2013) humanitarianism in the Network Age. New York: UN humanitarian central coordination unit (OCHA).
Rouvroy, Antoinette & Yves Poullet (2009) The Right to informational self-determination and the value of self-development. Reassessing the Importance of privacy for democracy. In S. Gutwirth, R. Leen, P. De Hert & Y. Poullet (eds.) Reinventing Data Protection. Berlin: Springer.
Zeineddine, Ina (2012) gamification and crowdsourcing as Engagement Techniques of Human Rights Organizations [Thesis]. Gothenburg: University of Gothenburg.

1 "gamification" is a process in which game theory and methods used to solve problems in other sectors (definition based on the gamification Summit 2012, cited in Zeineddine (2012)).
2 Almon & Farkas (2013) presents an overview of the risks associated with identity and confidential information in humanitarian action and any possible response for humanitarian actors.
3 of individuals control over when and how data about them being used or informational self-determination, is considered by many to be an important component of modern democratic rettighetter. See for example Rouvroy and Poullet (2009).
4 Translated from "crowdmapping" in English.
5 Chapter 6: Managing Sensitive Protection information (Standards and Guidelines 36-50).
6 Particularly relevant is Chapter 6, which presents a recommendation that only organizations with the necessary expertise and capacity should gather proprietary information (default 37); the responsibility for assessing the risk lies with participants seeking information and builds systems for information sharing (standards 39, 40, 46); that mechanisms for information security must be present ex ante (default 45); the assessment of informed consent is required for the sharing of information from interviews and "net voluntary" (crowdsourcing, standards 47-48); that individuals and groups should be informed about what information they supplement will be used (default 49); and for the establishment of information systems and security procedures (53).
7 The name comes from "short code" that SMS messages can be sent to Haiti (4636). Cooperation was never formalized, and the website where Ushahidi application was set up (http://4636.Ushahidi.com) is no longer available. The unorganized way volunteers were collected and coordinated has been described as the motivation to create the organization "Standby Volunteer Task Force." For a detailed description of the measure, see National Geographic (2012) and Mission 4636 (2013).