Constructing Consent:

ethical challenges to information innovation in humanitarianism

Christopher Wilson
the engine room, https://theengineroom.org
bit.ly/responsible-data

Argument

① The information systems and affordances produced by ICTs necessitate a conception of direct responsibility for using or collecting information

② The idea of "Consent" is a primary challenge

③ Relevant standards are improving, but still far from operational, and don't account for the contextual pressures and trade-offs of humanitarian action

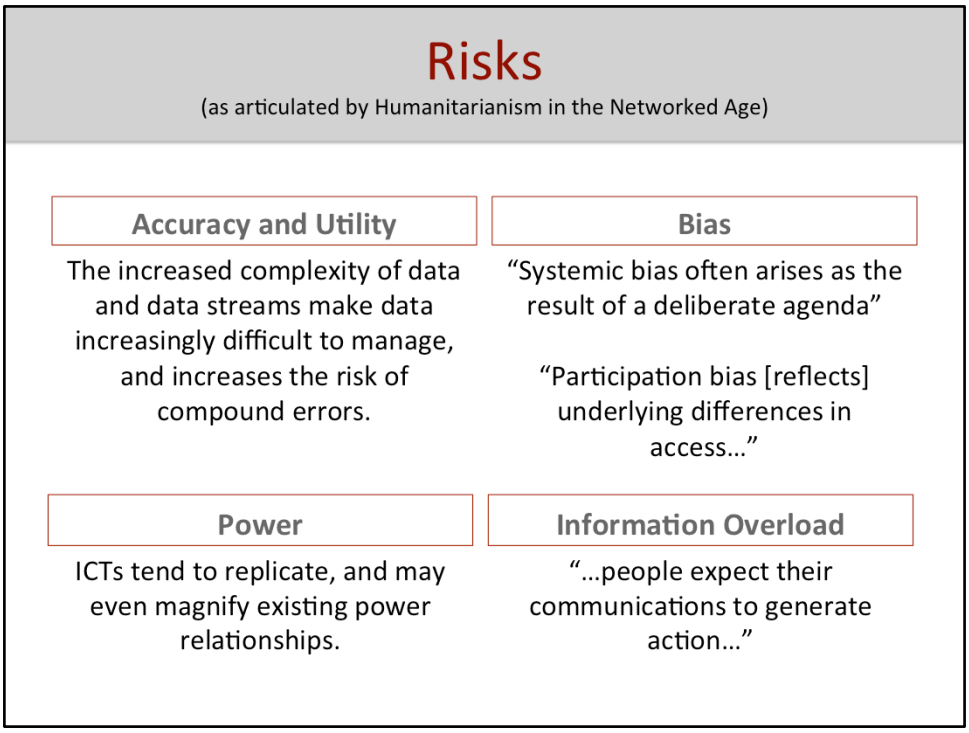
④ We need piloting, documentation and a "user-centric" approach to bridge the gap between standards and praxis

RDP Risks:
Collection effects
Policy Effects (data complexity and accuracy, data dependency, data security)
Misuse (by institutions, by individuals, by 3rd parties[capture])
Data ripples (community effects, policy repercussions)

Promises of

- Efficiency
- Greater impact
- More inclusive


I
DATA



These are all important risks, but they are primarily first-person risks, that is: risks to the initiative considering them.

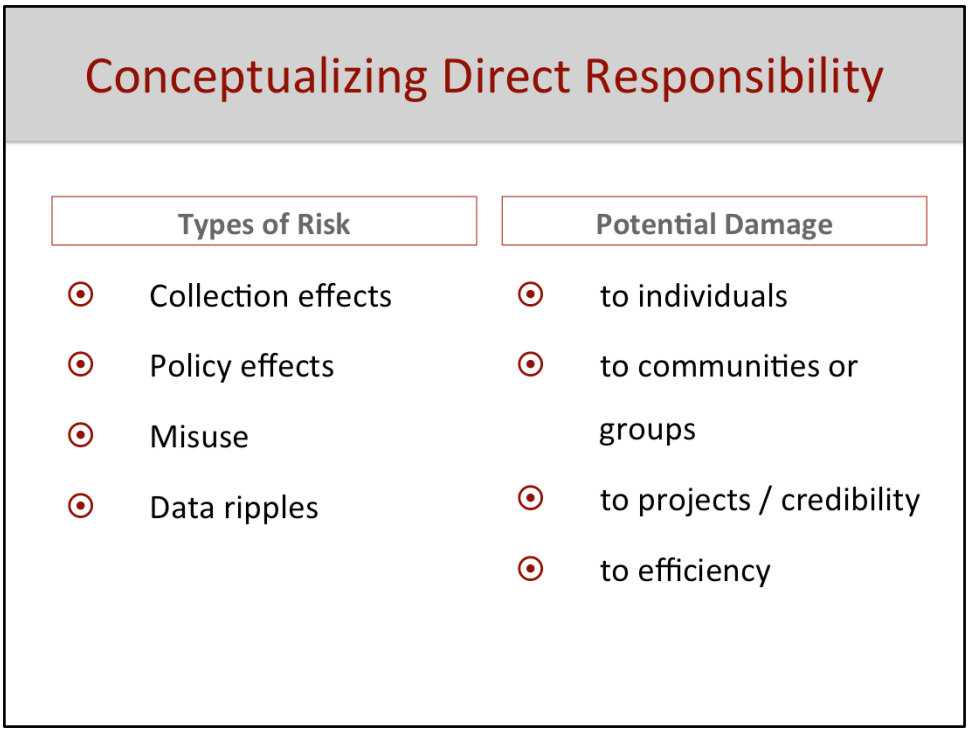
Responsible Data Risks

- Schrödinger effects
- Exacerbation of power imbalance
- Enabling negative actions

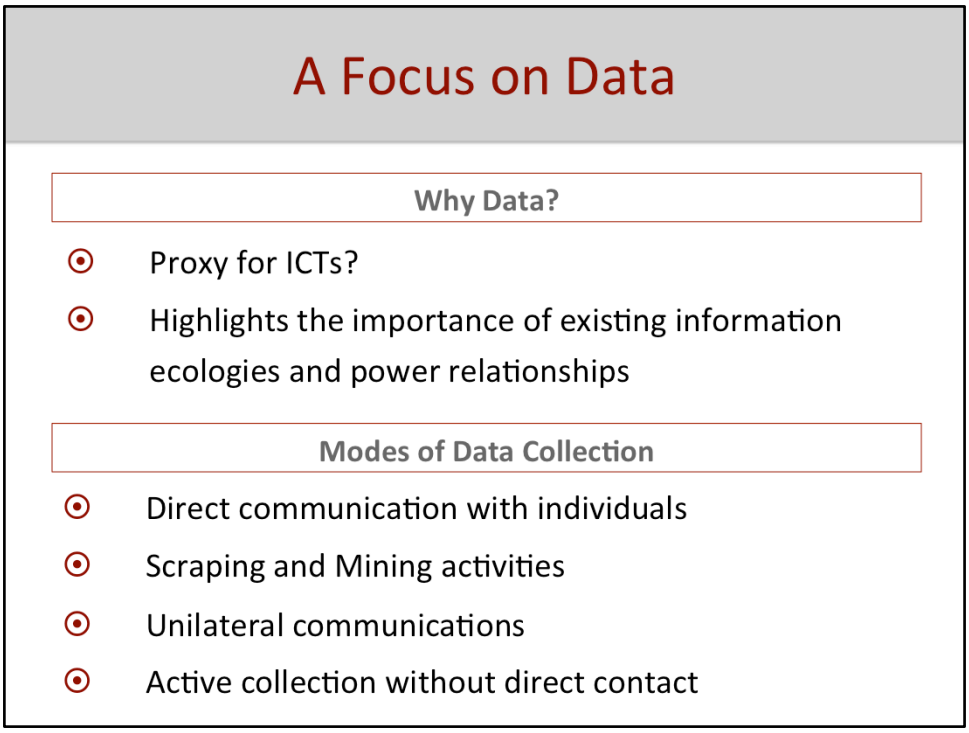
1. By engaging with information from and about individuals and communities, we engage with them. How do we understand and anticipate the impact of that engagement. Do we really want to shoot that cat?
2. Systemic, participation and respondent bias pose threats to more than data quality. When biased data provides the basis for humanitarian decision-making, it threatens to exacerbate exixting imbalances in access to information, international audiences and other resources.
3. Enabling access to information about vulnerable groups can support or enable attacks.

The problem is that we don't really understand the relational and moral consequences of a new information ecology in which we now operate, which means that even the best of intentions can go terribly wrong.

The ethical issues at play extend far beyond humanitarians' spheres of control and influence.
(The conundrum of digital humanitarianism: when the crowd does harm, http://crisismapper.wordpress.com/2013/11/15/the-conundrum-of-digital-humanitarianism-when-the-crowd-does-harm/)



But this presentation wants to focus on direct responsibility, when informational management occurs within humanitarians' spheres of control and influence. With this focus, we can anticipate a broad spectrum of ways in which managing information can pose risks, and the types of damage irresponsible information management could lead to.



I also want to focus on data, because it provides a useful proxy for ICTs. Doing so also allows us to focus analysis on specific modes of engagement with humanitarian information, as the affordances technologies provide, rather than the technologies themselves.

Direct Effects and Responsible Data

① In situations where ICTs facilitate the accessibility or utility of data for humanitarian programming or interventions

a) (building on established ethical standards

b) and because the scope & immediacy of ICTs present new relational paradigms and challenges):

② the ethical responsibilities owed to individuals or groups

③ when using data they provide, or in which they are reflected.

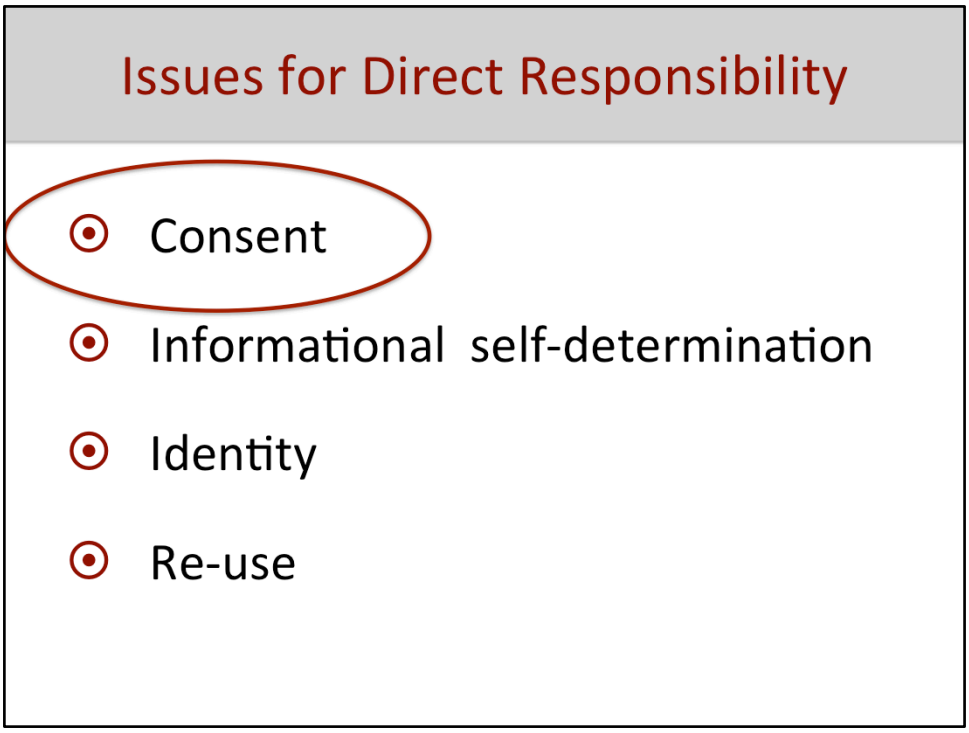
On slide 11, an attempt to define the focus of this presentation: direct responsibility when engaging with information.

Technology in Peacebuilding

(Laurruri & Kahl, 2013)

	Early Warning	Collaboration	Peaceful Attitudes	Policy Change
Data Processing	U-Shahid Voix des Kivus Uwiano peace platform	CRMA Iraq Monitor		Syria Tracker Satellite Sentinel
Communications	Georgia early warning	#18 days in Egypt	Peace Factory Shoot your identity Umuzi Photoclub PeaceTXT	I paid a bribe
Gamification		Country X	Sambaza peace game Slavery footprint Acts of kindness	
Engagement		Mahallae MasterPeace	Soliya HarrassMap	Turning Tables

This conception of direct responsibility focuses on the engagement with the data of individuals, and would thus apply to all of the types of initiatives referenced here, regardless of whether or not there was direct contact with individuals or groups.



On slide 13 we identify the object of the presentation!

Defining Consent

Application

- "Research"
- Human Subjects

Components

- Participants are presented with purpose, methods and possible outcomes (including risks or harms)
- Provided "sufficient opportunity to consider them and enquire about any aspect of the research prior to granting consent"
- Participate willingly

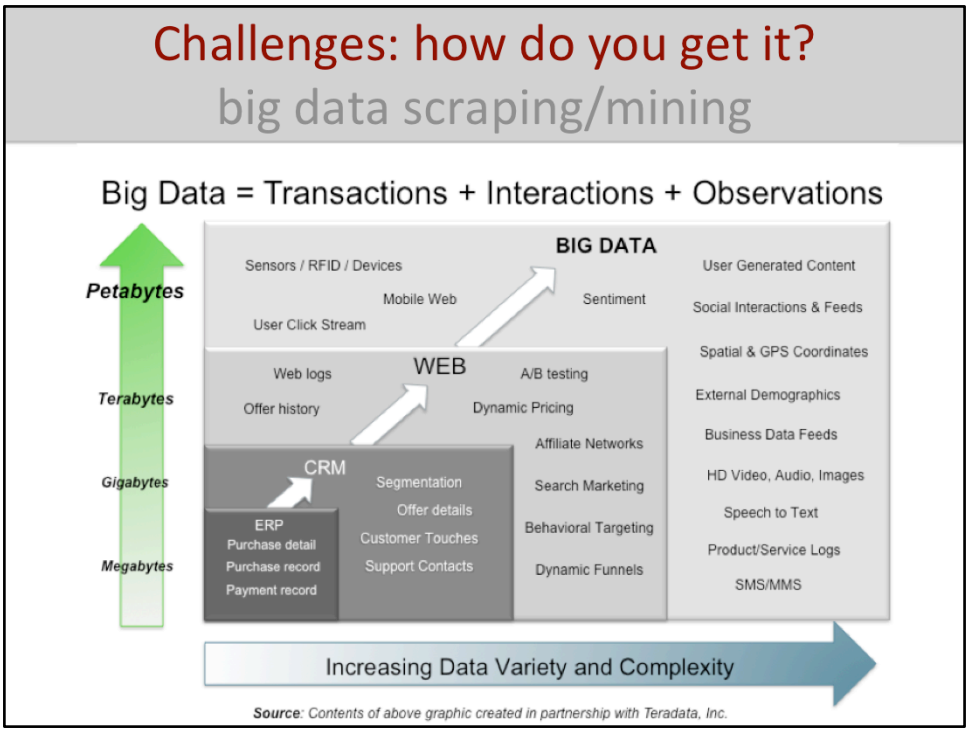
Challenges: whose consent ?
secondary subjects and 3rd parties

Secondary subjects exist when an investigator asks a primary subject, with whom the investigator is directly interacting, to provide information about other individuals.

"A **third party** is an individual (or organization or institution) who is not a researcher or a subject, but who is affected by the relationship between those persons" (Resnik, D. B. & Sharp, R. R. (2006, p. 2).

Directly affected third parties: "are identifiable individuals or organizations whose rights or welfare may be adversely affected by research procedures" (Resnik, D. B. & Sharp, R. R. (2006, p. 2).

Whose consent do you need?



Even if you know whose consent, how do you get it?
Or do you get it? Even if you can reach individuals, how do you consider the ethical implications of delaying assistance by obtaining consent? When is this justified? How do you know if contact will have other negative consequences, such as endangering individuals through association, if the humanitarian initiative is perceived as impartial? Will making contact raise expectations?

Challenges: how do they know?
modeling threats and anticipating harm

- Changes in political context
- Limited information
- Changes in data management

What capacity do individuals and groups reflected in humanitarian data have to anticipate changes in context and accurately assess potential risk?
None of these challenges are distinct to humanitarian context, but they are set in stark relief because of the nature of social relationships in humanitarian contexts, and because the consequences can be so extreme.

Relevant Standards (1)

GSMA's SMS Code of Conduct for Disaster Response

7

PERSONAL IDENTIFYING INFORMATION

SHOULD NOT BE MADE PUBLIC UNLESS PRIOR CONSENT IS PROVIDED BY THOSE TEXTING INTO AN SMS INFORMATION SERVICE.

• • •

THE RAW CONTENT OF TEXT MESSAGES SHOULD REMAIN CONFIDENTIAL AND HOSTED ON A SECURE PLATFORM.

RETENTION OF PERSONAL DATA, PARTICULARLY MOBILE USERS' PHONE NUMBERS,

SHOULD BE LIMITED TO A SPECIFIC PERIOD OF TIME FOLLOWING THE DISASTER AND SHOULD NOT BE TRANSFERRED TO THIRD PARTIES WITHOUT PRIOR CONSENT. RECOGNITION OF PREVAILING PRIVACY LAWS IN SPECIFIC COUNTRIES IS IMPORTANT, AS ARE REGULATIONS THAT STIPULATE THAT MOBILE NETWORK OPERATORS PROTECT THEIR CUSTOMER DATA.

• • •

ACHIEVING A MUTUALLY-UNDERSTOOD AGREEMENT

[BETWEEN USERS AND SERVICE PROVIDERS] WHERE IDENTIFYING INFORMATION IS SHARED SHOULD ALWAYS BE DONE IN A WAY WHICH PROTECTS THE INDIVIDUAL [SERVICE USER].

The GMS Code of Conduct mentions privacy only in relationship to national laws. Recommends consent for personal data to be made public or transferred to third parties.

("PII should not be made public unless prior consent is provided by those texting into an SMS information service"
"Retention of personal data […] should not be transferred to third parties without prior consent.)

Relevant Standards (2)

2010 HAP Standard in Accountability and Quality Management

4.3	The organisation shall enable the people it aims to assist to provide feedback and influence or make decisions about the project in a way that is continuously adapted to the context and the intervention. As a minimum, informed consent shall be obtained for the action.	1	Observation, records, and interviews to confirm a process through which the organisation assesses the capacity to participate and decides what is appropriate
		2	Records of informed consent and other participatory activities
		3	Examples and records that input is affecting decisions

The HAP standard makes no mention of data, communications, information sharing or privacy. Recommends consent as a basis for humanitarian intervention generally.

("The organization shall enable the people it aims to assist to provide feedback and influence […] at a minimum, informed consent shall be obtained for the action.")

Relevant Standards (3)

Big Data, Communities and Ethical Resilience: A Framework for Action

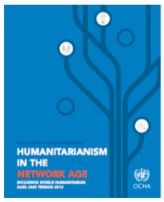
At its core, an ethical framework for data aims to enhance agency: the ability for individuals and communities to be able to make decisions about how, where, why and for how long their data is used.

…

Informed consent goes beyond merely making people aware of the terms of service or that data is being gathered about them, **but a clear articulation of how data might be used, whether third parties will get access to that data, and how people can opt out or limit how much of their data is gathered.**

This framework from the 2013 Poptech Fellows provides strong and articulate arguments for ensuring consent and seeking to support data agency. It does not provide operational guidance, and does not target humanitarian work.

Relevant Standards (4)



ANNEX A

Further operational recommendations

4. Develop robust ethical guidelines around the use of information

Specific operational recommendations:

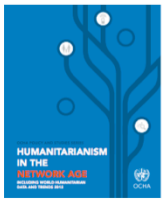
Humanitarian organizations

- No later than 2014, develop "Do No Harm" standards for the ethical use of new forms of data, including protocols for protecting privacy and guaranteeing informants' safety, and develop frameworks to hold practitioners responsible for adherence to ethical and technical standards. Ensure that these clearly address the separate issues of liability, privacy and security.
- Adopt information management principles as a source of guidance for adapting to the network age.
- Ensure that all projects include complaint and accountability mechanisms that can rapidly respond to issues of concern, abuse, exploitation, etc.

OACHA's landmark report recommends that "Do No Harm" standards for the ethical use of new forms of data are developed no later than 2014.

("No later than 2014, develop "Do No Harm" standards for the ethical use of new forms of data, including protocols for protecting privacy and guaranteeing informants' safety, and develop frameworks to hold practitioners responsible for adherence to ethical and technical standards. Ensure that these clearly address the separate issues of liability, privacy and security.")

Relevant Standards (4)

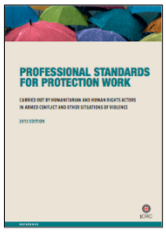


Humanitarianism in the Networked Age (2012)

Concern over the protection of information and data is not a sufficient reason to avoid using new communications technologies in emergencies, but it must be taken into account. To adapt to increased ethical risks, humanitarian responders and partners need explicit guidelines and codes of conduct for managing new data sources. (pg 46)

It also notes the following.

Relevant Standards (5)

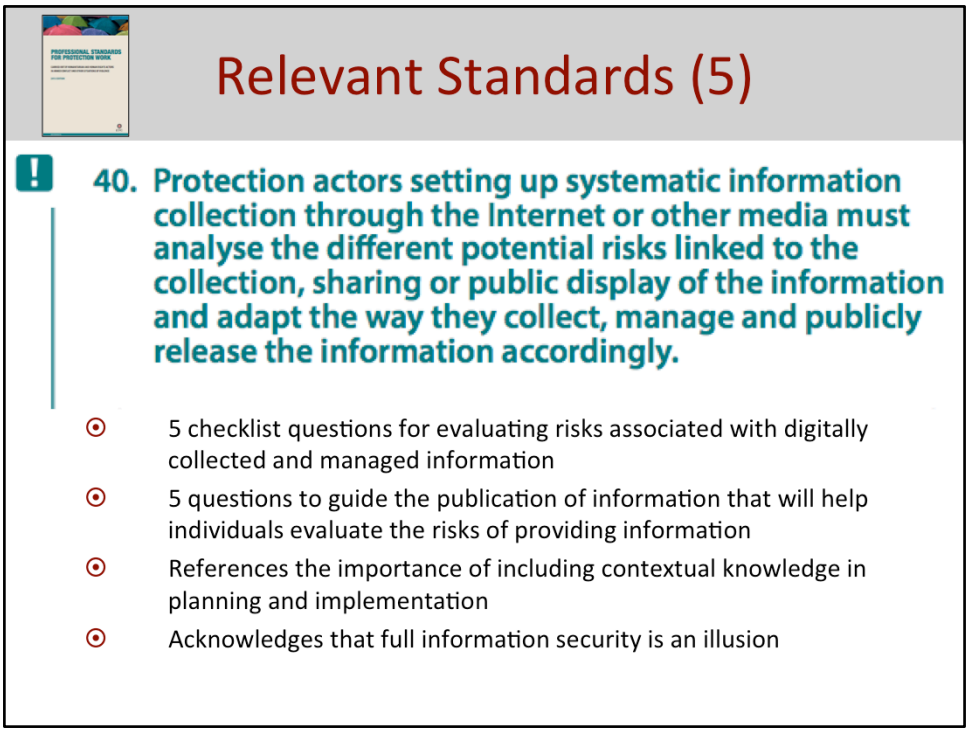


ICRC Professional Standards for Protection Work (2013) By far the most detailed, operational and authoritative standard.

Chapter 6: Managing Sensitive Protection information (Standards and guidelines 36-50)

- Only capable org's should collect sensitive info (37)
- Burden of assessing risk lies w/actors seeking info, building platforms (39, 40, 46)
- Info security safeguards must be in place ex-ante (45)
- Inf. consent for sharing prsnl info from interviews (47), dealing with the crowd (48)
- Inform communities of how information is used (49-G)
- Establishing info management and security procedures (53-G)

The ICRC standards are clearly the gold standard. There are a number of relevant standards listed here. The most relevant for considering consent are 40 & 48.



This standard is 900 words, and includes a significant amount of detail

Relevant Standards (5)

48. Protection actors must integrate the notion of informed consent when calling upon the general public, or members of a community, to spontaneously send them information through SMS, an open Internet platform, or any other means of communication, or when using information already available on the Internet.

- Acknowledges that once information is released publicly, there is no longer any control
- Assigns responsibility to the data collecting party in the event of data sharing and coordination

Relevant Standards (5)

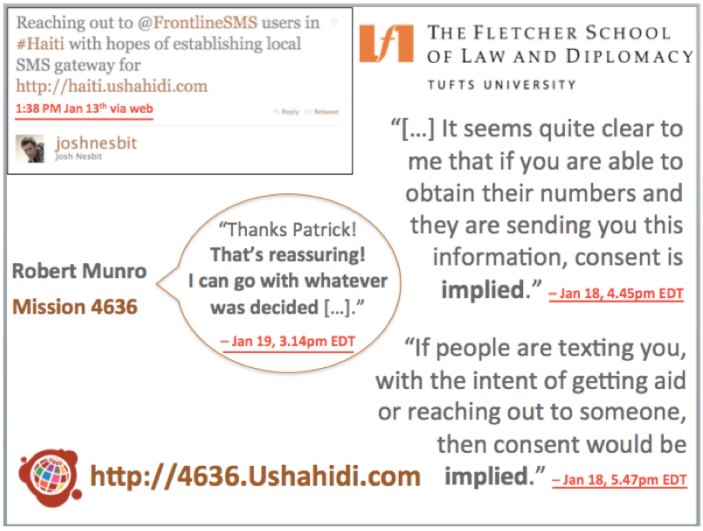
Overarching Questions re the IRCRC standards

- Allocating responsibility
- Time pressure and competing norms of protection and due diligence
- Capacities and resources along the data pipeline

This standard is 900 words, and includes a significant amount of detail

These standards help engage some of the challenges in some of the situations. But their applicability is not crystal clear. The guidelines suggest their relevance for a broad scope of actors, including VTCs, but it is not clear how accessible or operational they are outside of well resourced multilateral organizations. Even in those cases, there remains a significant gap between available guidance and the practical tools necessary to operationalize consent in actual activities in a digital information ecology.

"Implied Consent"



"I, for one, never again want to spend 24+ precious hours debating whether or not urgent life-and-death text messages can or cannot be mapped because of uncertainties over data privacy and protection."

http://irevolution.net/2013/02/25/launching-sms-code-of-conduct/

- And so we are left to make it up as we go. This is description of the Ushahidi response to the Haitian earthquake of 2011, specifically regarding the question of whether sms messages sent to a short code should be shared publicly.
- Tradeoff: "the more open the data, the more widely useable that information is likely to be for professional disaster responders, local communities and the Diaspora—but goodbye privacy."
- 2 "trusted lawyers … opined that consent was implied vis-à-vis the publishing of personal identifying information.

BUT

- Who was it shared with?
- How was it shared?
- What kind of information was included?
- What control mechanisms were in place to monitor these factors?

There may well be good answers to these questions, but they are questions that need to be asked more generally when collecting and managing humanitarian data through the use of ICTs.
They are questions begged by the platitudinal quality of available standards and resources.
They are questions that tell us what needs to happen next.

Moving Forward

- Clear and universal delineation of responsibilities
- Operational tools for specific types of data management processes
- Developed in collaboration with actual users
- Piloted and validated with affected/reflected individuals and communities

RDP Risks:
Collection effects
Policy Effects (data complexity and accuracy, data dependency, data security)
Misuse (by institutions, by individuals, by 3rd parties[capture])
Data ripples (community effects, policy repercussions)

thanks

responsible-data@lists.riseup.net

Christopher Wilson
the engine room, https://theengineroom.org
bit.ly/responsible-data