Chapter 2
Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts

Rahel Dette

2.1 Introduction

> … which reminds us of the fact that peripheral populations are being subjected to more or less experimental technologies.
>
> Katja Lindskov Jacobsen, The Politics of Humanitarian Technology (2015)

In humanitarian emergencies, information communication technologies (ICTs) such as mobile phones and web-based platforms offer powerful tools for communicating with communities, remote needs assessments and data collection. A quickly growing literature confirms the benefits that ICTs can offer to aid efforts with regards to efficiency, effectiveness and accountability (Raftree and Bamberger 2014; Kalas and Spurk 2011). These promises are especially pronounced in insecure environments, where access constraints hinder aid actors from reaching local populations, such that digital channels could be the only way to send and receive critical information. At the same time, the potential consequences of implementing technology-based projects poorly or overseeing unintended consequences can be detrimental and sometimes lethal.

Recognizing the challenges and risks with technologies can help avoid pitfalls and unintended digital harm. ICTs are known to introduce complications in a number of ways: Digital tools themselves alter the interaction between aid staff and recipients, which can add to and exacerbate crises or conflict dynamics (Jacobsen 2015; Vazquez and Wall 2014; Altay and Labonte 2014). The digitization of communications introduces new security and privacy risks as data transmitted on electronic devices or networks becomes susceptible to third party interception and breaches, sometimes unnoticeably (Internews 2015; Schneier 2015). However, such challenges entangled with using ICT for humanitarian purposes have not been adequately researched or addressed in literature and practice. Although concrete proposals for new ethics and

R. Dette (✉)
The Berlin-Based Global Public Policy Institute (GPPi), Berlin, Germany
e-mail: rdette@gppi.net

S. Hostettler et al. (eds.), *Technologies for Development*,
https://doi.org/10.1007/978-3-319-91068-0_2

conventions to guide technology uses are increasingly considered necessary, they are holding off (Raymond and Card 2015a; Gilman and Baker 2014; Sandvik et al. 2014). While a number of promising initiatives develop guidelines and good practice lessons, they tend to focus on disaster settings, explicitly omit recommendations for complex, man-made emergencies (GSMA 2012; UAViators 2015; Madianou et al. 2015). In conflict zones, aid actors are left to make up rules as they go, or forfeit opportunities by opting against technologies altogether, but these decisions are typically not documented (Raymond et al. 2013; Steets et al. 2015). A better understanding of the perceived and real risks entangled in the use of ICT, as outlined here, can help inform a responsible, sustainable humanitarian technology practice that works in all settings.

This paper draws on finding of the 3-year research project 'Secure Access in Volatile Environments (SAVE)' that was undertaken by Humanitarian Outcomes (HO) and the Global Public Policy Institute (GPPi) with funding from the UK Department for International Development (DFID). Part of the research assessed technologies that aid actors can use for monitoring and evaluation (M&E) in insecure and hard-to-reach areas. The research was undertaken in close collaboration with NGOs and UN agencies in Afghanistan, Somalia, South Sudan and the Syria region with the aim to provide practical contributions. A 'menu of technology options for monitoring' introduces and explains select ICT tools in detail, zooming in on challenges in order to propose effective risk mitigation strategies. The menu and this paper recognize the significant potential technologies offer to humanitarian efforts, but caution against rushed implementation at the risk of overseeing severe challenges and limitations. A risk-aware approach to all new tools, especially those that are digital or data-based, can help aid actors assure they 'do no digital harm.'

2.2 Technology Advantages

ICT in insecure environments

ICT aids communication and can be used in aid efforts. It includes mobile phone, location trackers, software, web-based platforms, digital media and more. Here, we focus on those tools that are already widespread or easily accessible in crisis contexts and thus ready and reliable to use even in precarious situations. The narrow focus on insecurity and conflict settings, where information is often sensitive, makes risks and challenges especially apparent, and can help inform mitigation and best practices that translate to other settings.

In insecure environments, several limitations curtail the selection of ICTs that can be used. Access restrictions, poor infrastructure, budgets constraints and high levels of uncertainty require tools to function without constant electricity supply, across wide distances and without advanced IT support. In close collaboration with aid organizations and technology experts, we identified four technology types that meet these criteria: mobile phone-based feedback mechanisms, handheld devices

Table 2.1 Technological tools for remote monitoring and communication in insecure environments: Types, uses, and challenges

Phone-based feedback mechanisms and two-way communication	Digital data collection with smartphones and tablet computers	Remote sensing with satellites or UAVs and location tracking (GPS)	Broadcasting and community production of radio shows
Where basic mobile phones are widely spread, they offer reliable channels to reach local communities. Calls, text messages and interactive voice recordings (IVR) can be processed by call centres or specialized software	Aid organizations can use digital data entry linked to electronic databases to replace paper-based survey instruments and create faster, more automatic data analysis. Small handhelds are also more unobtrusive than clipboards	High-resolution geospatial imagery analysed by experts can elucidate context conditions, observable changes and outcomes of interventions, as well as population movement. Radars and sensors can capture unique data	Broadcast radio can spread humanitarian information, conflict or aid delivery updates. To target information, aid staff can stream pre-recorded shows in select locations. Interactive radio shows station can also receive feedback
Complaints and information hotlines Phone-based household surveys Verification calls Focal point reports	Surveys and questionnaires Registration and distribution reporting GPS- and timestamps in surveys	Observation and analysis with satellite UAV imagery for close-up analysis Radar/sensor data Barcode tracking	Outreach, advocacy and engagement Publicize/explain feedback channels Community radio
⊗ Proliferation of parallel hotlines can lead to confusion ⊗ Security and privacy risks to staff and aid recipients ⊗ Risk of bias towards those owning phones (often men) ⊗ Volatility due to poor infrastructure	⊗ Devices can raise the visibility of aid staff and mistrust among authorities and locals ⊗ Competing tools can cause fragmentation ⊗ Privacy/security risks digitizing data: theft, interception, surveillance, etc.	⊗ Lack of guidance/established practice ⊗ Can expose vulnerable groups ⊗ High costs can deter organizations as effect and return are not always clear ⊗ Dependency on image providers, data brokers and experts	⊗ One-way radio broadcasts cannot record feedback ⊗ Difficult to measure impact and identify the audience ⊗ Security risks due to high visibility: interception possible ⊗ Gender bias towards male voices

for digital data collection, remote sensing with satellites or unmanned aerial vehicles (UAVs) and broadcasting with radios. They enable a range of functions to complement communication efforts but also introduce new challenges as summarized in Table 2.1

ICTs in humanitarian action

Aid organizations report a number of advantages with technologies, especially around saving costs and time. In highly insecure settings, ICT increasingly facilitates direct two-way interactions that otherwise could not take place. Where aid access is less restricted, many find that face-to-face time with local communities can be used more efficiently when survey data can be entered directly into digital devices. Because these

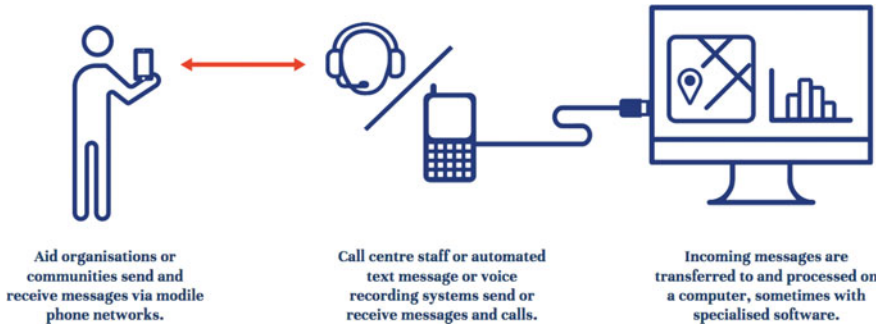

Fig. 2.1 Technology Type 1—Phone-based feedback mechanisms

typically process and upload information directly to databases, the turnaround for data analysis and use increases significantly. ICTs were often praised to be convenient, customizable and very good at handling data efficiently. The devices themselves can be unobtrusive or unnoticeable, which sometimes improved the security for aid staff and recipients. A helpful way to conceptualize such benefits as well as associated shortcomings is what one researcher coined the 'law of amplification' (Toyama 2015). Technology can amplify the intent and capacity of stakeholders, he says, but never substitute for deficiencies. A closer look at how this plays out for different technologies helps lay the ground for afterwards deciphering how problems, too, are amplified—or newly introduced (Fig. 2.1).

Countless studies cite and investigate the 'unprecedented,' 'ubiquitous' spread of basic mobile phone worldwide and the impact their availability and affordability can have in development and humanitarian contexts (Hallow et al. 2012; de Montjoye et al. 2014). Calls or SMS are comparatively cheap and very quick and, importantly, often come naturally to local communities in crisis-affected areas. This makes mobile phones ideal for reaching out to and being reached by more people (Robinson and Obrecht 2016). Aid actors have started integrating phones proactively by offering hotlines for aid recipients, by calling households to collect data, and by inviting comments, complaints or suggestions via SMS (Korenblum 2012). More and more 'hotlines' also are provided via WhatsApp and other online messaging tools that work on smartphones as well as desktops. Powered by mobile data or Internet connection and offering encrypted channels, these started replacing SMS and calls in areas where smartphones are spreading, for example, in Syria. Aid agencies also make use of phones for distributing mobile vouchers and cash directly to people's mobiles or to quickly spread messages with warnings, updates or important information. While regular visits to communities take weeks, SMS updates or survey questions sent to phones take hours or minutes to share and process (Fig. 2.2).

Summing up the significant improvements digital surveys offers data collection, one aid worker said: 'There are no more pregnant men anymore.' Supervisors can programme questionnaires to require specific answers to specific questions, and skip irrelevant questions, such as asking men whether they are pregnant. Spell check and

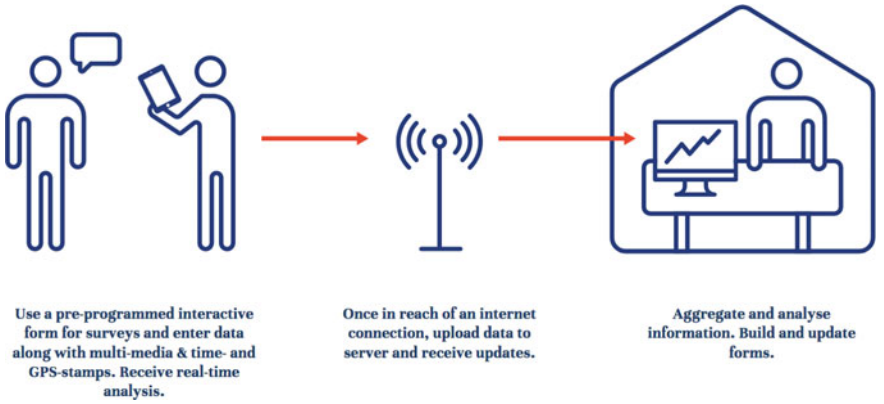

Fig. 2.2 Technology Type 2—Digital data collection

error detection also improve data entries, thereby preventing accidental nonsensical answers. Altogether, running surveys on digital devices rather than paper was largely seen to speed up interviews, sometimes cutting their time in half. Where an Internet connection is available, data transfer from the field or field office to headquarters can be immediate, and makes laborious manual data entry and transfer unnecessary, thus cutting weeks' worth or time down to hours. 'Reporting used to be a headache,' one monitoring officer said. 'With smartphones, it no longer is.' During interviews, smartphones sometimes offered unexpected further benefits, like drawing less attention from members of the community than a flipboard would and sometimes giving survey respondents more in-the-moment privacy by typing rather than saying answers. In addition, field office staff reported that GPS- and timestamps provide certainty that interviews are actually completed at different times with community respondents in different locations. In Somalia, for example, enumerators were suspected to sometimes fill out forms in bulk, inventing answers. Typically, this would happen when it was too difficult or dangerous to reach aid recipients. Because the digital data entries made this trend apparent, aid organizations could address this issue and start constructive conversations with enumerators when and where data collection was too dangerous (Fig. 2.3).

Aerial imagery and geospatial analysis can capture independent and objective information from areas that are too remote or insecure to reach or where larger patterns may not be observable up-close. Where access is restricted, this data can provide valuable insights on infrastructure and shelter, vehicle positions and the effects of disasters including flooding, drought or landslides. Captured repeatedly over time, imagery can help assess project outcomes and, in some contexts such as agricultural intervention, impact. Remote sensing or 'earth observation' information is often visualized on maps or triangulated with other data sets. This is especially beneficial for making sense of complex datasets and putting information in context (Fig. 2.4).

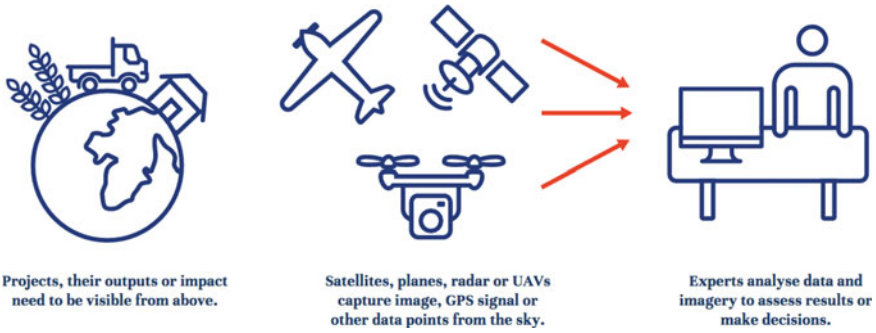

Fig. 2.3 Technology Type 3—Remote sensing and location tracking

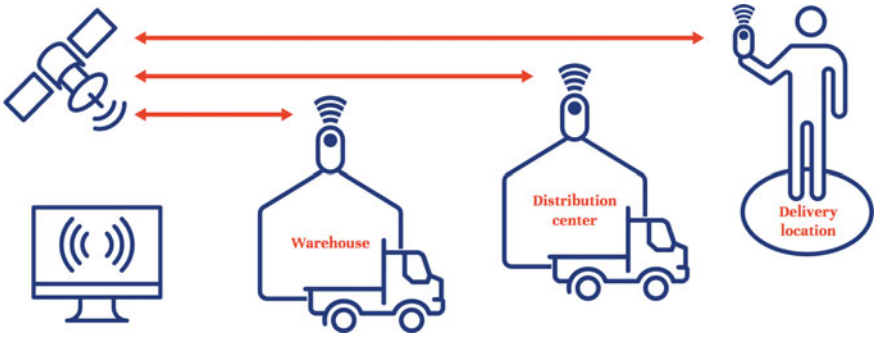

Fig. 2.4 Geolocation

Satellites are also used for location tracking, specifically those two dozen that form the Global Positioning System (GPS) sent to space by the US Department of Defense. Collecting data points at unique places and times can provide aid actors certainty that goods or vehicles have reached certain locations, even when relying on third party deliveries. Some actors already developed 'FedEx-style delivery systems' including low-tech options that use barcodes attached to packages with staff in different locations scan when the item passes them. This data, visualized on maps that are intuitive to understand, is valuable for real-time awareness of where to target which needs and has increased flexible decision-making and adjustments of aid efforts (Fig. 2.5).

Radio remains the most widely used technology reaching the largest number of people in remote areas around the world, especially in insecure environments. Broadcasts can be used to circulate important announcements but also to explain aid efforts and feedback mechanisms to crisis-affected communities. Radio programming itself can be used for active two-way engagement, involving or supporting communities in creating their own shows and stations. This can provide interesting forms of gathering feedback in and of itself, which some aid agencies are pioneering. Still, in humanitarian programming and monitoring especially, radio has not received mainstream

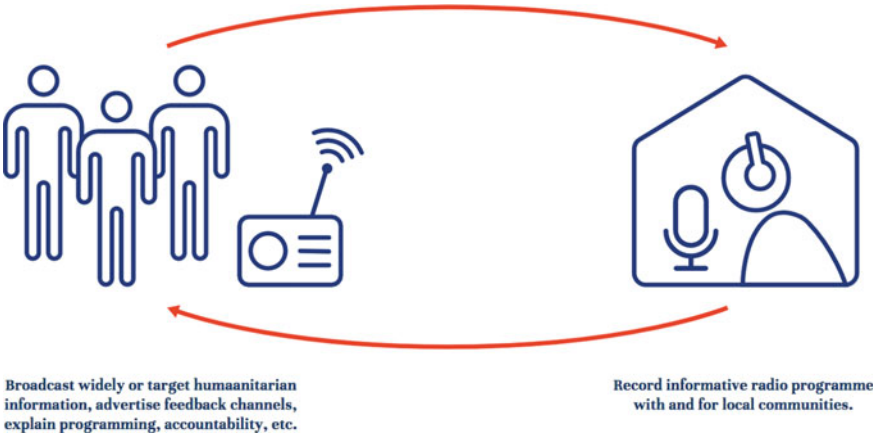

Fig. 2.5 Technology Type 4—Radio

attention. Radio is often seen as a one-way outreach tool, which is not intuitively ideal for M&E. However, a number of projects have shown that radio is easy to use and can complement feedback mechanisms and enable aid actors to seek new forms of input. It offers great potential for aid accountability and community resilience.

Wrapping up with this fourth reliable and likely underestimated tool, the wealth and variety of various technologies, with many news ones yet to come, is evident.

2.3 Digital Disasters

Implementation errors and inherent flaws of ICT

As so often, benefits and opportunities do not come without a dark side. Worse, in insecure environments the risks and challenges technologies introduce can be detrimental, even deathly. A small but growing literature started pointing to shortcomings and problems with advances in technology being brought to humanitarian and conflict contexts. Many of these challenges are surprisingly non-technical: Simply put, technology often fails when introduced too quickly in the wrong setting and for the wrong reasons (Sandvik et al. 2014; Jacobsen 2015). Transplanting what works in one part of the world or even humanitarian programming is no guarantee for success elsewhere. Where new tools are poorly coordinated or not discussed with other actors in the area or sector, proliferation and competition can undermine accountability efforts. Misjudgements of the effort, capacity and time required to maintain and run new systems can lead to mishaps, delays and inconsistencies. Similarly, where technical issues need to be resolved at headquarter level, delays and problems can occur. Finally, technical failures, especially if unanticipated, can severely hamper technology projects. Further yet, these critiques do not address more inherent

challenges entangled with ICT and digitalization, a significant selection of which is described and categorized below.

Challenge 1: Mishaps and mistakes

Serious concerns came up in interviews with 'half-baked' implementation or unanticipated non-technical problems. In one case, aid recipients were given mobile vouchers directly to their phones. The aid organization, however, was not aware that telephone signals in the area were poor, requiring recipients to seek locations, for example, mountains, where their phones could connect to the network. Mountains, then, become perfect target spots for crime and loitering, when individuals would wander off alone in search of mobile connection. Similarly, where enumerators were asked to record GPS-stamps with their surveys, several reported having to wait minutes, sometimes hours, until they could connect to the satellite connection and thus move on to the next question. In another case, aid organizations sent tablets to their field staff but did not consider the number of plugs needed to charge each of them. 'I stayed up all night charging one iPad after the next,' a staff member said. Mobile hotlines, as another example, were sometimes not introduced well enough to fulfil intended purposes, so aid recipients would often call with questions or with praise rather than complaints. An even greater problem was where advertisements outlived hotlines, causing the community to call with nobody responding.

Challenge 2: Negative impact of new devices

Not all staff not always reacted well to new tools, and sometimes rejected change. Local enumerators hired for surveying often required more training than anticipated if they were handling digital devices for the first time, and needed detailed instructions including on the swipe motion to operate smartphones. For data collectors, restrictive digital survey forms and reporting platforms sometimes were a problem: certain answers did not fit. Small answer boxes on small smartphone screens also could cause difficulties with data entry and frustration. Some also critiqued new types of data power dynamics: where data is uploaded to a central database but servers are located at headquarter level and connectivity is poor, it is sometimes impossible or difficult for people in field locations to access the data they submit, either because of access barriers, or simply because the Internet is much too low to dial into the central system. An equally unwelcome inherent technology issue was introducing gender bias. Radio, for instance, is often known to cater more to male than female listeners, a trend that can be hard to break, so the humanitarian intervention could reinforce unequal access. Similarly, men are more likely to hold on or own the phones a household uses, making it difficult for women to use phones anonymously.

Challenge 3: Loss of trust and reputation

Beyond operational difficulties, aid staff observed that the sheer introduction of new devices could have negative effects. Many reported that local communities did not respond well: enumerators with smartphones instead of paper surveys were found to be less friendly, and hotlines were found to be less personal. In fact, respondents were

frequently less willing to discuss sensitive issues over digital media, sometimes for the fear of interception or spying. In Syria, for instance, it was impossible to record GPS-stamps as armed groups would immediately suspect a connection to a foreign military and worry that their armed bases could be revealed. In Somalia, al-Shabaab banned aid actors with smartphones altogether and would threaten those who used them. The negative stigma of digital devices could also affect the quality of survey responses and information passed on via mobile phones. With regards to remote sensing, some governments banned aid agencies from using aerial imagery, fearing that the NGO could reveal data that could harm the government.

Challenge 4: Digital vulnerabilities and digital harm

Further, there are severe risks related to digital security that are far from addressed, let alone known, by both the humanitarian and other sectors. Even though aid practitioners often were aware that digital data can be copied and intercepted without them noticing and that online accounts can be compromised, mobile communications can be tracked and anonymized datasets can be reidentified, many organizations fail to prioritize digital security and even opt against using encryption to secure their data or devices. 'If militants knew how to intercept our communications,' one respondent said, 'then they would build better bombs.' And 'we offer encryption, but aid organisations never want it,' said two different service providers. Increasing digitization, though, means increasing dependency on tools, which both reduce redundancy. Any potential blackout or attack on digital databases or systems will likely become ever more costly. At the same time, it makes attacks more rewarding for attackers as they can get their hands on more information, which can be used against people or passed on to third parties. The potential cost of digital attack was far from meeting with adequate security precautions, typically for a simple reason: as long as no serious incidents are known, aid actors have other worries.

Challenge 5: Privacy risks and irresponsible digital data

Notably, where multiple datasets exist that include information about the same group or individual, for example, census data, food aid distribution charts, caller ID records and online social media accounts, these could allow digital attacker to reidentify a person. Comparing multiple datasets makes it possible to distil accurate revealing information about people. Increasing amounts of digital data, that are increasingly shared with digital communities around the world, for example, in order to 'crowdsource' the analysis of images, can unintentionally increase the risk of data abuse and cross-referencing. All in all, humanitarians' lack of interest in 'cyber' threats is alarming. If aid actors digitize more of their data and communications, they urgently need to increase their digital security efforts. Though some actors are developing promising protective tools, aid organizations overall might be well advised to listen to a quote from IT-security circles: 'There are two types of organizations: those who have been hacked, and those who will be.'

Challenge 6: Increasing inequality and power imbalances

Even those technology implementations that seem seamless and successful can entail problematic power dynamics that disadvantage aid recipients or lead to long-term negative consequences (Jacobsen 2015; Toyama 2015). Technologies affect their surroundings, which can be detrimental in contexts of discrepancy and donor–recipient relationships. In academia, technology has been critiqued as 'deepening the processes of creating inequalities' as those in power who introduce new tools risk undermine the engagement of those in the periphery (Santos 2000).

Challenge 7: Dependence on non-humanitarian actors and sectors

Technology-enabled aid attracts and actively depends on new actors to the field, including computer experts and for-profit businesses. Some of these may not adhere to, or even contradict, the humanitarian principles of neutrality, independence and impartiality (Raymond and Card 2015b). Increasing dependence on the services and expertise of these new actors can compromise the values and objectives of aid efforts (Duffield 2014).

Challenge 8: Double-standards and hypocrisy compromise humanitarian principles

Some controversy has risen where aid efforts relied on tools that were not considered ethical or adequate in other contexts (Hosein and Nyst 2013; Jacobsen 2015: 10). In Europe, for example, public backlash led policymakers to halt the integration of advanced biometrics in citizen registration. In contrast, this is widespread and praised for refugee registration (Hosein and Nyst 2013: 8; Jacobsen 2015). Aid actors often do not have regulatory safeguards for technologies (Duffield 2014: 3). Unless crisis-affected communities understand and object to the risks, subjecting them to digital technologies can introduce new dependencies and inequalities.

2.4 Mitigation Measures

Risk awareness aids responsibility

Oftentimes, the most successful tactics to minimize technology harm are not technical at all, but behavioural such as self-imposed limitations on what information to collect and transmit digitally (Steets et al. 2016; Antin et al. 2014; Internews 2015). When the name or age or even gender of a person is not critically necessary for household nutrition surveys, it may be better not to record it. Similarly, it is good to aggregate and generalize information at the first stage of data collection to prevent reidentification that could lead to harm or problems for individuals (de Montjoye et al. 2014). Security audits can help identify who has access to aid data and how easily staff accounts and emails could be compromised (Shostack 2014; Internews 2015). It is also good to introduce privacy-conscious technology and 'free and open source software (FOSS).' These tools run on code that is published and can be reviewed by anyone, such that

security can be verified. Such tools can also be continued after individual projects may close down. Finally, aid actors should always plan for nondigital alternatives when connectivity or electricity fail, or ICTs cannot be used for other reasons. Sometimes, the best solution may be to opt against technology tools altogether.

Notably, mitigation happens at different levels. It can take involve impromptu measures in the field, or standards and good practice can be developed at headquarter level. Some outspoken actors are already seeking to establish shared norms across the field, including the 'digital development principles,' which were developed with about a dozen international and UN organizations and endorsed by many more (https://digitalprinciples.org). In addition, several initiatives emerged around 'responsible data' efforts, crafting principles and practical recommendations on how to assure data security and adequate access (https://responsibledata.io/). And in the UAV community, a code of conduct was authored and agreed (werobotics.org/codeofconduct/). Contributing to this work, Table 2.2 presents nine core ideas on implementing technology tools based on a 'backwards' analysis from risk assessment first to mitigation measures suggestions. This list is not necessarily comprehensive, and specific recommendations would depend on specific technologies and contexts. Yet, this first offering can help start conversations and be further refined with practitioners.

Back to low-tech—and sometimes no-tech

Broadly speaking, there are four types of circumstances when it may be better not to use technologies for humanitarian purposes, as the inherent risk would outweigh or overshadow possible benefits (Table 2.3).

Specifically, the following recommendations apply to the different technology types:

When using mobile phone-based systems, do not…

- *…use phone-based systems to collect sensitive data that could put beneficiaries at risk*. Information related to gender-based violence, the location of persecuted people or financial and health information that could cause stigmatization cannot be reliably secured when transferred through phone networks.
- *…use it for short-term projects or without continuity*. The set-up and familiarization costs only pay off if phone-based systems are used over a long time or for several projects.
- *…create a new mechanism where other, similar mechanisms already exist or are planned*. With too many systems in place, aid recipients can be confused and are less likely to use any.
- *…use it if you do not have the capacity to process feedback and follow-up*. Beneficiaries will expect follow-up when using phone systems. Lack of response can harm trust and reputation.
- *…simply replace other monitoring or feedback approaches*. Phone systems are not sufficient in themselves as phone ownership is biased and network coverage uneven.

Table 2.2 Risk mitigation for humanitarian ICT uses: why and what

1. Study the context before choosing tools	The information and technology ecosystems determine whether a new tool or approach can have a positive impact in the long term. Hotlines, for example, only work where locals have and use phones. Satellite images only make sense when skies are clear and smartphones should only be used in culturally appropriate ways *Be very clear about the information you need to gather or spread. Assess closely what type of information and knowledge travels via which channels in your context. Understand who influences and spreads information and can impact it*
2. Involve all users actively	Any tool or technology is only as effective as those meant to use it understand - and use - it. This involves all: programme staff, supervisors, data collectors, local communities, those processing the data and those making decisions based on it *Work with representatives of the different user groups when inventing, designing and testing the tools. Focus groups or interviews and, as much as possible, collaboration can help assure that ICT is usable and appropriate in all ways, including handling, pricing, language, etc.*
3. Establish informed consent practices	Achieving informed consent is especially difficult when aid actors themselves do not know all the risks involved with technologies and digitization. Because there is currently little best practice, aid actors need to handle recipients' data carefully *Agree on mechanisms and standards by which to explain the risks involved with handling survey responses or phone requests digitally. Do this well before disaster hits*
4. Provide back-up channels and alternatives	Technology-based efforts need to be prepared for the worst cases including energy outages, network disruption, theft of devices, software jams and other complications *Have analogue alternatives in place to turn to when the new tool does not work. Also, assure that every online function has an offline option. And do carry extra batteries*
5. Use security-conscious, free and open source software	With technology, intuition and observation are not enough to know who can gain access to information, as calls and electronically submitted data can be intercepted, often unnoticeably. The responsibility to safeguard personal data and keep it away from third parties lies with the aid organizations, so the choice of technology matters *Use only those tools that independent security experts can review. Such 'free and open source software' (or FOSS) options exist for moth relevant ICT tools*
6. Minimize and self-limit data	Even with the best tools, ensuring digital security is extremely difficult, also for experts. It is safe to assume that every data point that has been digitized can be copied or stolen. Even seemingly harmless datasets can reveal people when combined with other data *Collect only on a 'need to know' basis. Be clear which information gaps you are trying to fill and identify which data points you need to collect. Similarly, define access levels clearly. Who needs to see individual records and where do aggregate numbers suffice?*

(continued)

Table 2.2 (continued)

7. Invest in building acceptance	Local authorities can ban technology tools and restrict aid access. Armed groups could even target them. Local communities may lose trust if they do not trust the technologies *Plan trainings and meetings with local staff, authorities as well as community members. Explain what you are using and let them see and perhaps test the tool themselves*
8. Pool funds and risk	Technology implementations typically take more time and high investments. Running out of budget half-way and halting projects can create inconsistency and further risk trust *Collaborate with other aid actors in the area of relevant private companies. Share the investment in tools and seek agreeable mechanisms for sharing them and the data*
9. Apply humanitarian principles to technology	The humanitarian principles were developed long before the risks affiliated with digital communications were known. Their maintenance in online context must be explored *Safeguard the principles when working with new tools and partners. What does neutrality mean in the context of algorithms that sieve through information? How can you maintain independence when working together with private sector companies? Are biases towards those willing and able to use phones, for example, overshadowing universality?*

Table 2.3 Four scenarios when technology should NOT be used, but low-tech or analogue methodologies are recommended

Data is so sensitive that it could put people at risk	Acceptance is low and could hamper efforts: bans, suspicion, stigma, etc.	Infrastructure makes it impossible or costly: network connectivity, low spread of phones	Capacity constraints mean it cannot be guaranteed in the long term

When implementing digital data entry, do not…

- *…use digital devices, Internet or phone networks if they are in any way banned or compromised in the targeted area*. It is not worth the benefit if carrying the tool could lead to expulsion or mistrust and false accusations.
- *…use smartphones or tablets if they are very uncommon or clash with cultural norms and standards*. If the devices can create distrust or suspicion among local communities, they should not be used. Their stigma could hamper data entry.
- *…use where there is no phone or internet connection and/or electricity at all*. Lack of connectivity which would make it challenging to make the most from the tool.

When working with satellite imagery or geo-location tracking, do not…

- *…use satellite or UAV imagery and GPS-tracking if no guidelines on their use are in place and the potential risks to local communities are high or unclear*. Records of the location of vulnerable, persecuted or starving populations or of food delivery trucks and critical infrastructure can seriously endanger people and individuals if in the hands of their enemies.

- *…work with UAVs or other remote sensing technologies if local stakeholders seriously object to their use.* Remote sensing technologies can be associated with spying. Using them against the will of local authorities or communities can erode trust and put operations and staff at risk.
- *…invest in technologies where weather or context conditions are prohibitive and projects and their effects cannot be seen from the sky*. Satellites cannot see through clouds and in some instances regulation might inhibit use. Similarly, where projects can be seen, but there is no clear idea what visually observable impact would be expected, remote sensing may not be a worthwhile investment.
- *…commit to remote sensing when costs for images and analysis are disproportionate to the overall budget*. As of yet, evidence for overall gains or improved decision-making thanks to satellite use remains limited. Until then, their use should only be considered where costs are proportionate to overall project budgets and the expected gains.

When broadcasting information via *radio, do not…*

- *…broadcast information on radio when it reveals the location of vulnerable populations*.
- *…set up new radio programmes when you cannot guarantee long-term commitment to cater to the need of your listeners*. It is not worthwhile to build and audience if the show soon ends.
- *…use radio to support monitoring efforts when you cannot combine it with other tools* and approaches to receive responses to issues raised and questions asked in the shows.
- *…invest in independent radio stations or shows when you cannot engage local communities*. Their help in designing and running radio programmes is critical to assure local interest and relevance.

2.5 Looking Ahead

Scrutiny on using ICT in conflict settings can shed light and insight relevant to the broader field of working with technologies for humanitarian, development and human right purposes. However, the field of practice and literature on technologies used for humanitarian purposes and to communicate with local communities needs to be expanded to examine and address risks and mitigation measures. The particular focus on ICT for monitoring aid in access-constrained insecure settings in this paper provided a lens to view some of the practical and ethical concerns with using technologies to handle data of vulnerable populations. Other technologies relevant to humanitarian action include hardware (such as 3D printers and biometric ATMs), medical research (such as genetically modified food and new vaccines), social media (particularly platforms, messaging apps, and so-called ‘big data’) and a range of applications for coordinating, planning and implementing aid delivery. Many of the concerns around digital and physical risks outlined here similarly apply

to these technologies. In the future, findings from the research underlying this paper as well as alerts and suggestions from other sources should be investigated further both through analysis and cross-comparisons with other fields and through practical sessions, workshops and discussions. These can contribute to the growing field of a responsible and sustainable use of technology for the benefit of conflict- and disaster-affected communities. They can inform aid efforts that safeguard the humanitarian principles and in their work 'do no harm' and do no digital harm either.

References

Altay, N., & Labonte, M. (2014). Challenges in humanitarian information management and exchange: Evidence from Haiti. *Disasters, 38*(Suppl. 1), S1–S23. https://doi.org/10.1111/disa.12052.

Antin, K., Byrne, R., Geber, T., van Geffen, S., Hoffmann, J., Jayaram, M., et al. (2014). *Shooting our hard drive into space and other ways to practice responsible development data*. Book Sprints.

Belden, C., Surya, P., Goyal, A., Pruuden, P., Etulain, T., Bothwell, C., et al. (2013). *ICT for data collection and monitoring and evaluation: opportunities and guidance on mobile applications for forest and agricultural sectors*.

Demombynes, G., Gubbins, P., & Romeo, A. (2013). *Challenges and opportunities of mobile phone-based data collection: Evidence from South Sudan*. Policy Research Working Paper No. 6321. The World Bank.

de Montjoye, Y. -A., Kendall, J., & Kerry, C. F. (2014). Enabling humanitarian use of mobile phone data. *The Journal of the American College of Dentists*. Retrieved from http://www.brookings.edu/research/papers/2014/11/12-enabling-humanitarian-use-mobile-phone-data.

Dette, R., Steets, J., & Sagmeister, E. (2016). *Technologies for monitoring in insecure environments*. Available at: http://www.gppi.net/fileadmin/user_upload/media/pub/2016/SAVE__2016__Toolkit_on_Technologies_for_Monitoring_in_Insecure_Environments.pdf.

DFID. (2013). *DFID's anti-corruption strategy for Somalia*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213926/anti-corruption-strategy-so.pdf. Last accessed January 12, 2016.

Duffield, M. (2013). *Disaster-resilience in the network age access-denial and the rise of cyber-humanitarianism*. DIIS Working Paper 2013: 23.

Duffield, M. (2014). *Cyber-intelligence in humanitarian emergencies: A critical exploration*. Notes. http://www.iss.nl/fileadmin/ASSETS/iss/Research_and_projects/GGSJ/Crisis_Speaker_photos/Speakers_Papers/Duffield.docx. Accessed November 20, 2015.

Gilman, D., & Baker, L. (2014). *Humanitarianism in the age of cyber-warfare: Towards the principles and secure use of information in humanitarian emergencies*. OCHA Policy and Studies Series 011. UN OCHA.

GSMA (2012). *Disaster response: Guidelines for establishing effective collaboration between mobile network operators and government agencies*. Resource document. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Guidelines-for-Establishing-Effective-Collaboration.pdf. Accessed November 20, 2015.

Hallow, D., Mitchell, J., Gladwell, C., & Aggiss, R. (2012). *Mobile technology in emergencies: Efficient cash transfer mechanisms and effective two-way communication with disaster-affected communities using mobile phone technology*. Retrieved from http://www.alnap.org/resource/10619.

Hosein, G., & Nyst, C. (2013). *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*. London: Privacy International.

Hussain, H. (2013). *Dialing down risks: mobile privacy and information security in global development projects*. Washington, D.C.: New America Foundation.

Jacobsen, K. L. (2015). *The politics of humanitarian technology: Good intentions, unintended consequences and insecurity*. Abingdon: Routledge.

Kalas, P., & Spurk, C. (2011). *Deepening participation and improving aid effectiveness through media and ICTs*.

Korenblum, J. (2012). *Mobile phones and crisis zones: How text messaging can help streamline humanitarian aid delivery*. Available at: http://odihpn.org/magazine/mobile-phones-and-crisis-zones-how-text-messaging-can-help-streamline-humanitarian-aid-delivery/.

Madianou, M., Longboan, L., & Ong, J. C. (2015). Finding a voice through humanitarian technologies? Communication technologies and participation in disaster recovery. *International Journal of Communication, 9*(S.l.), 19. ISSN 1932-8036. Accessed November 20, 2015.

Maxwell, D., et al. (2014). *Lessons learned from the Somalia famine and the greater horn of Africa crisis 2011–2012: Desk review of literature*. Feinstein International Center. Available at: fic.tufts.edu/assets/Desk-Review-Somalia-GHA-Crisis-2011-2012.pdf. Last accessed January 12, 2016.

Raftree, L., & Bamberger, M. (2014). *Emerging opportunities: Monitoring and evaluation in a tech-enabled world*. New York: Rockefeller Foundation.

Raymond, N. A, & Card, B. L. (2015a). What is "humanitarian communication"? Towards standard definitions and protections for the humanitarian use of ICTs. Signal Program on Human Security and Technology, Harvard Humanitarian Initiative.

Raymond, N. A., & Card, B. L. (2015b). Applying humanitarian principles to current uses of information communication technologies: Gaps in doctrine and challenges to practice. Signal Program on Human Security and Technology, Harvard Humanitarian Initiative.

Raymond, N. A., Davies, B. I., Card, B. L., Achkar, Z. Al, & Baker, I. L. (2013). While we watched: Assessing the impact of the satellite sentinel project. *Science & Technology*, 1–13.

Robinson, A., & Obrecht, A. (2016). *Using mobile voice technology to improve the collection of food security data: WFP's mobile vulnerability analysis and mapping*. Available at: http://www.alnap.org/resource/21596.

Sandvik, K. B., Wilson, C., Karlsrud, J. (2014). A humanitarian technology policy agenda for 2016. Blogpost. Humanitarian Academy at Harvard (ATHA). http://www.atha.se/content/humanitarian-technology-policy-agenda-2016. Accessed November 20, 2015.

Shostack, A. (2014). *Threat modeling: designing for security*. Indianapolis, IN: Wiley.

Steets, J., Sagmeister, E., & Ruppert, L. (2016). *Eyes and ears on the ground: Monitoring in insecure environments*. Available at: http://www.gppi.net/fileadmin/user_upload/media/pub/2016/SAVE__2016__Monitoring_aid_in_insecure_environments.pdf.

Thakkar, M., Floretta, J., Dhar, D., Wilmink, N., Sen, S., Keleher, N., et al. (2013*). Mobile-based technology for monitoring & evaluation*. Retrieved from http://www.theclearinitiative.org/mobile-basedtechnology.html.

Toyama, K. (2015). *Geek Heresy: Rescuing social change from the cult of technology*. New York, NY: PublicAffairs.

UAViators. (2015). *Humanitarian UAV code of conduct & guidelines*. Resource document. Humanitarian UAV Network. https://docs.google.com/document/d/1Uez75_qmIVMxY35OzqMd_HPzSf-Ey43lJ_mye-kEEpQ/edit?pli=1. Accessed November 20, 2015.

Van de Walle, B., & Comes, T. (2015). On the nature of information management in complex and natural disasters. *Procedia Engineering, 107,* 403–411. https://doi.org/10.1016/j.proeng.2015.06.098.

Vazquez, L. R., & Wall, I. (Eds). (2014). *Communications technology and humanitarian delivery*. European Interagency Security Forum (EISF).

Woods, A. K. (2014). *Do civil society's data practices call for new ethical guidelines?*. Stanford: Ethics of Data in Civil Society.