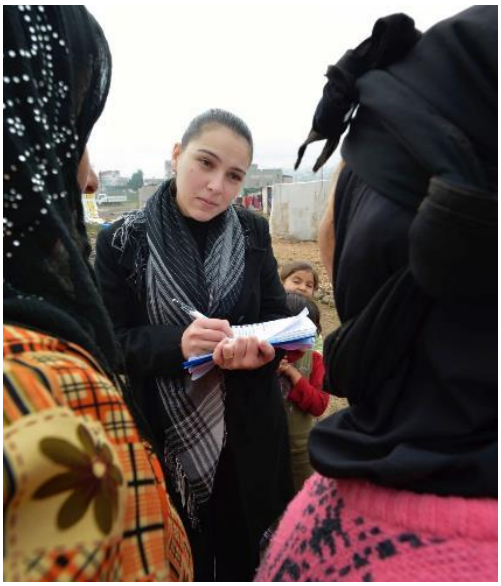
Data, data everywhere, what does it mean for NZ NGOs?

In the first of two short blogs, Nik summarises recent articles about big data in the NGO sector from IRIN (by Ben Parker here and here); researchers from the Harvard Humanitarian Initiative (here); Devex and the World Economic Forum including a piece by Stephen O'Brien (OCHA); looking at the risks of not defining a conscious policy within your organisation (and supporting partners in the field to do the same).

It was nearly 10pm on a December night in an IDP camp, South Darfur. I was wrapping up another long day in my capacity as general gap-filler (Country Director) for a medical INGO. The phone rang, and it was OCHA from Nyala: was my team safe? Was I aware that there was a rebel attack ongoing in the camp, affecting our NGO neighbours? (Yes and no, were my answers…).



© *Paul Jeffrey, Lebanon with Syrian refugees*

Once the incident-management was in hand, I thought of all of the project-level data from clinics we were running: numbers of people treated, drug stocks and training programmes – and patient records. All of the information our donor required before sending the next tranche of funding. All the details of the people we treated.

It was only then, at that moment, did I think to ask my team about data back-up. Because what would happen when the rebels came for our laptops, phones and vehicles?

That was over 10 years ago. I feel slightly sheepish that it took such an extreme event to crystallise the importance of "data protection" for me.

More and more data – so what?

Better tools for monitoring and remote management mean more data than ever is being collected and shared by, about and between, affected people and NGOs. The principle that more is better prevails: it is easy to collect, so why not?

The Grand Bargain, to which NZ is a signatory, includes a work stream on harmonising and simplifying reporting – the antithesis of unchecked data collection.

NGOs (and our donors and the laws we are governed by) are currently being challenged to:

- ***Invest in technology and reporting systems*** to enable better access to information;
- ***Use*** this data to inform decisions;

- ***Enhance the quality of reporting to better capture results***, enable learning and increase the efficiency of reporting and aid itself; and
- ***Handle*** data responsibly.

We NGOs are more conditioned to information scarcity, not overflow, but especially after a disaster, too much information can also paralyse response efforts. Computers, mobile phones, social media, mainstream news, earth-based sensors, and humanitarian and development drones generate vast volumes of data during major disasters. Making sense of this flash flood of information, or **Big Data** requires new skills, systems, and policies (and Digital humanitarians are now a thing!)

In a system with thousands of 'aid entities' supporting communities (local and international NGOs, civil society groups, UN agencies, government and private sector partners), we lack standards and guidelines for collecting, processing, analysing and disseminating data. Added to this problem are contexts marked by poor electricity supplies, intermittent and unreliable communications, limited connectivity, low staff capacity, insecurity, unpredictability and remote access.

Our collective inability to adequately regulate and professionalise NGO information activities threatens our operational sustainability; trust between agencies and the people we seek to serve, and erodes the meaning and value of codes of conduct and core principles of humanity, impartiality, independence, and neutrality.

What's the problem?
Think about this scenario from a WEF blog: You are a humanitarian relief worker, taken to visit a person in need of assistance or protection. Unknown to you, your phone has been hacked, or the metadata generated by your phone is aggregated, allowing its location to be surveilled, your social media activity followed and telecom metadata analysed. The next day, the house you visited is destroyed in a drone strike or the people you met with detained. Suddenly your organisation is viewed locally with **anger and suspicion**, and perception of neutrality of humanitarian action is compromised.

Breaches of platforms and networks, weaponisation of humanitarian data to aid attacks on vulnerable populations, and exploitation of systems against agencies and beneficiaries – may already be occurring, but there are no requirements for reporting, addressing root causes of breaches and mitigating damage caused by such breaches.

In a recent, ugly example shared by the Harvard Humanitarian Initiative, a company competing for the business of hosting a cash-based programme platform hacked into a cloud-based server of **Catholic Relief Services** and accessed names, photographs, family details, PIN numbers, and map coordinates for more than 8,000 families receiving assistance from the NGO in West Africa.

The World Food Programme took a radical step when it released an **internal audit** of WFP beneficiary management (November 2017). The report found extensive data protection failings: lack of proper consent; no assessment of privacy risks; data being exchanged and copied insecurely without encryption and password protection; data being shared with other

organisations without any legal agreements. When beneficiary registration lists are connected to banks and mobile money providers (who may be obliged to share data with national authorities) - another layer of risk can arise depending on local data protection practices. WFP handles huge amounts of personal data (over 82 million people in 2016) and **the audit found** that too much information was being gathered, "without a specified and legitimate purpose", contrary to policy.

Arguably, these issues are relevant in development programmes, and in NGOs' domestic fund raising: databases of individual donors and new opt-in privacy rules for mailing lists could lead to drops in income. (Next week I'll summarise new legislation in the EU, UK and Australia, with some issues for NZ NGOs to consider.)

And that night in Darfur? While team members prayed, cried and called their families, I copied project data to an external hard drive. We were lucky though, our compound was spared. If the laptops had been taken, we would have lost our data, and unknown people may have used it for purposes I could not control. This realisation brought home my individual role in collecting, storing and using data responsibly as well as the need for a guided, organisation-wide system that would function in a dusty, hot and remote IDP camp.

January 28th was International Data Protection Day, raising awareness and promoting privacy and data protection best practices.