PRIVACY INTERNATIONAL

Spying on humanitarians: implications for organisations and beneficiaries

Executive Summary

The global communications surveillance mandates of American, British and other Western intelligence agencies leave barely a single individual with a mobile phone or email account untouched or unseen. Humanitarians are no exception to this new reality, the contours of which are only becoming apparent through the ongoing revelations of NSA whistleblower, Edward Snowden. Not only are their communications swept up in mass monitoring, but it is now clear that humanitarian organisations are being specifically targeted by, at the very least, the British Government Communications Headquarters (GCHQ). This dawning era of pervasive digital surveillance has grave implications for humanitarian organisations: it places their staff, partners, beneficiaries or patients under detailed scrutiny by Western intelligence agencies, allowing for their tracking, identification, monitoring and analysis; it impedes their ability to keep highly sensitive information away from malicious actors; it furthers negative perceptions of the organisation's impartiality or ability to shield beneficiaries or patients from retribution or further harm; and it undermines the trust humanitarian organisations build in communities that is so necessary for their work. This paper explores these implications and suggests actions that could be taken by humanitarian organisations to strongly oppose such practices, including legal action against the British government.

Introduction

In December 2013, building upon a series of revelations arising out of NSA documents leaked by whistleblower Edward Snowden from June 2013 onwards, the Guardian reported that British and American intelligence agencies were targeting humanitarian agencies such as UNICEF, UNDEP and Medecins du Monde.[1] The Guardian report relied on a number of GCHQ documents, dated between 2008 and 2011, which established that the surveillance operations were run out of a GCHQ facility in Bude. Each of the organisations named had been allocated a specific ID number in GCHQ's "target knowledge base", indicating that they were deliberately targeted for surveillance, rather than accidentally caught in a dragnet. It is reasonable to assume that this surveillance is on-going. Efforts made by Medecins du Monde to obtain further information from GCHQ about the nature of the surveillance they had been under were met with strict refusal by the intelligence service.

All humanitarian organisations should be seriously concerned by these revelations. In practical terms, being a target of GCHQ surveillance likely means that the British intelligence services (and, by implication, those of its allies, particularly the United States, Canada, Australia and New Zealand) have direct access to all communications sent or received by every employee of every humanitarian organisation, and potentially those of local partner organisations. GCHQ are likely collecting, en masse, copies of emails, phone calls, text messages, and web searches, and also have access to internal files and those stored in external services. They may also possess the ability to remotely control devices associated with the organisation by, for example, turning on the microphone or video camera of a smartphone, without the user's knowledge. These are not outlandish or remote possibilities, but conclusions that can reasonably be drawn from the technical information and descriptions of the GCHQ's capacities and activities outlined in the Snowden documents. Given Medecins du Monde modest size and reach, it is likely that the surveillance activities relating to them were a marginal aspect of a much more significant operation against a larger group of humanitarian organisations; bigger organisations with a greater scope and reach should consider that they are almost certainly the target of surveillance by GCHQ and the NSA. Equally, if large UN agencies such as UNICEF and UNDP are considered fit targets for surveillance, no organisation should consider itself immune to such surveillance.

Yet, the reaction of humanitarian organisations to these shocking revelations has been muted. Whereas Medecins du Monde publicly expressed outrage at the news, no analogous organisation publicly commented, nor did any UN agency. No public action, including litigation, has been taken by any humanitarian organisation, despite there being clear opportunities to do so in the British courts. Spying on humanitarian organisations has not been raised or debated in humanitarian fora or at the United Nations. The humanitarian sector is thus giving its tacit approval to practices which not only undermine the privacy and security of humanitarians and the communities they serve, but which imperil the humanitarian mission.

---

[1] http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

Below, we lay out some of the concerns that the humanitarian sector should have with being under surveillance by Western intelligence agencies. Thereafter, we suggest potential ways in which the sector could begin to turn the tide back against surveillance.

What surveillance means for humanitarians and beneficiaries

It is a well-established tenant of international human rights law that surveillance, particularly that involving the interception and monitoring of communications, is an interference with the right to privacy, enshrined in Article 12 of the Universal Declaration on Human Rights, and Article 17 of the International Covenant on Civil and Political Rights. The right to privacy is not an absolute right and surveillance, in some circumstances, may be justified. However, in order to accord with human rights standards, communications surveillance must be in accordance with law, reasonable and proportionate.[2] The content and application of these requirements has been detailed in the jurisprudence of the European Court of Human Rights, the UN Human Rights Committee, and various domestic courts, and will not be elaborated on here. In general terms, however, restrictions on the right to privacy must be narrow in scope, explicitly authorised by law and overseen by an independent authority, and subject to strong safeguards against abuse; the benefit gained must outweigh the harmed caused; and the surveillance must be strictly necessary to pursue an explicit, legitimate aim that is necessary in a democratic society.

The surveillance of humanitarian organisations by GCHQ can be said to run afoul of these demands, for a number of reasons:

- It is neither authorised nor regulated by British or European law, nor is it overseen by any rigorous or effective judicial mechanism (that is, the surveillance is neither authorised nor overseen by the courts);
- The harm it causes – undermining the impartiality, independence or neutrality, that many humanitarian organisations are defined by, violating confidential relationships, exposing sensitive data to analysis and dissemination – far outweighs any benefit gained by the intelligence services in carrying out the surveillance;
- It relates not to a specific, narrow threat posed by humanitarian actors, but rather is presumably predicated on a broad assumption that the data collected or transmitted by humanitarian organisations may include data relevant to national security or the economic wellbeing of the United Kingdom (that is, the scope is too broad); and
- The potential for abuse – either by the UK/US intelligence services who collect and access data gained through surveillance, by governments of other countries who might seek access, either lawfully or unlawfully, to that same data, or by non-state actors who might do the same – is huge, given the sensitive contexts in which humanitarian organisations work.

[2] For further information about the content of the right to privacy and the implications of communications surveillance on the protection of the right, see the International Principles on the Application of Human Rights to Communication Surveillance (https://www.necessaryandproportionate.org) and the American Civil Liberties Union's *The Human Right to Privacy in the Digital Age* (https://www.aclu.org/privacyrights).

For these reasons, spying on humanitarian actors must be said to be in conflict with human rights standards, and thus, fundamentally, it is unlawful.

Furthermore, the harm caused by spying on the humanitarian sector goes beyond the violation of the right to privacy. Humanitarian surveillance has correlative implications for both humanitarian actors and the individuals and communities with which they work.

Beneficiaries become vulnerable

Humanitarian organisations collect an extraordinary amount of data about the beneficiaries they assist, from personally identifiable information (name, address, age, gender) to highly sensitive information (political or religious affiliation, ethnicity, combatant status, location). They also often document evidence of human rights abuses and collect victim testimonies. Humanitarian organisations that provide medical services will also inevitably document and keep records of patients' health history, which could include information such as HIV status. Put together, this extremely sensitive information can be hugely valuable to some external actors, and in the wrong hands could create unforeseen and potentially grave threats to the beneficiary. Imagine such information in the hands of repressive governments, rebel groups, opposition forces, or unfriendly intelligence services. The spectre of terrorism haunts the humanitarian world and it is not news to humanitarian actors that the information they collect may be of great interest to governments, among them the United States, in identifying and locating suspected terrorists. Communications surveillance is the easiest, cheapest, fastest means of getting access to that information, which can thereafter be used to locate or target individuals, with potentially life-threatening consequences. For example, there is evidence to suggest that the products of surveillance conducted by GCHQ have been provided to US authorities for subsequent use in drone strikes in Pakistan.[3]

Trust in the humanitarian organisation is undermined

Knowledge – or even the suggestion – that a humanitarian organisation is a target of surveillance by a foreign government can seriously undermine the trust beneficiaries place in the organisation, limiting the access that the organisation might have to individuals or communities, or impeding the free flow of vital information between the organisation and beneficiaries. Beneficiaries may doubt the impartiality, independence or neutrality of the organisations, and not seek their assistance as a result. Additionally, they may withhold sensitive information or fabricate information if they are concerned that their data will not be kept confidential. This would impede the ability of the humanitarian organisation to provide appropriate, tailored, accurate assistance.

How should humanitarian organisations respond?

It is crucial that humanitarian organisations begin to consider what steps they can take, both internally and externally, to minimise the threat posed to their employees and

[3] See the British case of *Noor Khan v Secretary of State for Foreign and Commonwealth Affairs,* http://justsecurity.org/wp-content/uploads/2014/01/Noor-Khan-v.-State-UK-Court-of-Appeal-2014.pdf

beneficiaries by surveillance, and to contest their targeting by intelligence agencies. Humanitarian organisations must lead the way in drawing a line in the sand, asserting that spying on humanitarians should never be acceptable. If we are unable to convince Western intelligence agencies that the harm caused by surveillance on humanitarians is so fundamental as to undermine the humanitarian mission, then we have little hope of stemming the tide of spying by emerging malicious powers who are developing increasingly advanced intelligence capabilities.

It is clear that humanitarian actors care greatly about how they may inadvertently be jeopardising their beneficiaries – levels of awareness are high about the need to shred filing cabinets full of documents or destroy hard drives should government agents take control of local offices, for example. Yet, faced with compelling evidence that intelligence agencies are accessing such information (the digital version of filing cabinets and hard drives) en masse, directly, and contemporaneously; storing such information indefinitely; and sharing it with governments who might be using it for a range of nefarious purposes, humanitarian organisations have stood silent. Digital security remains a low priority for many humanitarians. Encryption is a peripheral tool used by the occasional humanitarian actor, rather than part of core organisational policy. Across the humanitarian sector there are low levels of awareness about information security or the vulnerabilities of certain types of technologies or digital tools. Far from showing concern about how using mobile phone or online platforms to transmit information may be placing data inadvertently in the hands of intelligence agencies, many humanitarian organisations are advocating greater use of technologies to record, store, and transmit humanitarian data. More critical reflection is needed in this area.

Beyond digital security, humanitarians need to realise that contesting State surveillance requires far more than small changes; it requires a principled public stance and a call for a normative approach to the issue. To this end, there are a number of public steps that humanitarian organisations could play to draw greater attention, stimulate public outrage, and demand policy change. These include:

1. Taking litigation against British intelligence agencies in the Investigatory Powers Tribunal: The British legal framework governing surveillance allows for individuals who suspect they have been subjected to surveillance to bring a case against the relevant government agency in a specially-constituted court called the Investigatory Powers Tribunal. The IPT has special powers allowing it to hold sessions in closed and examine sensitive material. A humanitarian organisation could bring a case against the British intelligence agency GCHQ in this Tribunal. There is a 'no costs' regime in the Tribunal, meaning that the organisation would not have to fear being made liable for costs should it lose its case. Privacy International has already commenced proceedings in the IPT on its own behalf[4] and would be more than happy to work with an humanitarian organisation to prepare similar litigation.

[4] See https://www.privacyinternational.org/press-releases/privacy-international-files-legal-challenge-against-uk-government-over-mass

2. **Calling for a resolution in the United Nations General Assembly, Security Council or Human Rights Council**: A humanitarian organisation could call upon the UN organs to make a strong statement in support of the notion that humanitarian organisations should not be placed under surveillance. This would be an important symbolic step.

3. **Putting out a joint statement or writing a joint letter:** A coalition of organisations could write to the US and UK governments and put out a joint statement on this issue. In this regard, humanitarian organisations could draw on the recent experience of the public health academics who wrote to the White House about CIA use of vaccination clinics as a front for counter-terrorism activities,[5] which resulted in the successful cancellation of the programme.

Privacy International would be more than happy to assist the sector in taking any and all of these actions.

Privacy International
May 2014

[5] http://www.nytimes.com/2014/05/20/us/us-cites-end-to-cia-ruses-using-vaccines.html?smid=tw-share&_r=1