Security Concerns for Libya Crisis Map
Standby Task Force and UN OCHA
March 2011

Given the nature of the crisis in Libya, there are a number of ethical / security concerns relating to the Libya Crisis Map deployment. Below are the risks acknowledged by both the Standby Task Force and UN OCHA, and the actions both partners agree to take in order to mitigate these risks.

In general, both partners are guided by the "Do No Harm" principles. The Standby Task Force is also guided by its code of conduct. The mitigating actions try to balance the benefit of sharing information publicly against the potential harm of information being misused. To this effect, the deployment will operate two sites: one public (visible to anyone on the internet); one private (password protected, visible to SBTF volunteers and to staff approved by UN OCHA)

Categories of information to be made public

RISK: There is concern that making the location of certain reports public may put people in danger, violating do no harm principles. This is particularly relevant to reports on humanitarian operations on the ground.
MITIGATING ACTIONS:

1. The specific location of humanitarian activities reported through the 3Ws are not reported. The GPS locations in the 3W are simply centroid-like points for the cities/borders/places where we know the activities are happening. They do not correspond to the EXACT location of the given activity.
2. Humanitarian activities reported via public means (twitter, media news, etc) will be available on the public site with whatever location was reported publicly

Protecting sensitive information in reports

RISK: Reports may mention the names of people (whether they are involved in the incident, reporting it or verifying it). Source links can also contain personal information (e.g. twitter account feed, videos of people involved). We could be compromising the personal safety of these people.
MITIGATING ACTIONS

1. Reports in the public site will only have the title and location of the report. Sensitive information will be kept in the text of the report and the source link.
2. SBTF volunteers have already gone through existing reports to remove any names from the title of reports and have been instructed to never include names or other sensitive information in the titles

Protecting reporters from Libya

RISK: Reporters based in Libya face particular risks if they are identified.
MITIGATING ACTIONS

1. There will be no reporting via SMS
2. Reporters in Libya will be advised to use only email to report (not the via web form). The following advice will be posted on the public site:

“If you are in Libya and want to share a report, please follow these steps:
1) Go to http://www.hushmail.com and sign up for an email address.
2) From your hushmail account, email us your report to crisismapper@hushmail.com
3) Only the title of your report will be made public: summarize your entire report in the email subject line, but do not include the names of people if it could potentially put anyone in danger. Sensitive information in the text of the email will be kept private. Please include location information as detailed as possible so we can map your report.”

Protecting information in the Ushahidi Libya Crisis Map platform

RISK: Given the mitigating actions above, sensitive information will only be available in the private site. It is therefore crucial to ensure the private site is not accessed by non-authorised people.

MITIGATING ACTIONS:

1. All SBTF volunteers subscribe to the Code of Conduct which states:

“Integrity: I will maintain the confidentiality of all internal communications and information intended solely for TF coordinators and volunteers. I will maintain confidentiality particularly on data relative to:

   1. Personal phone numbers and e-mail addresses of the sources of information
   2. Contacts with NGO, International Organizations and other partners of the TF
   3. Sensitive data related to vulnerable groups like children, women, sick people, elderly, IDPs and refugees.”

2. All SBTF volunteers accessing the backend of the Ushahidi platform will be sent the following:

   “You have just been given a new password to access the Ushahidi site. For security reasons, please make sure that you log out every time you leave your computer. Don't save the password on your computer.

   If you are operating from a hostile environment, it is very important that you install TOR or similar independent security software on your computer (this protects other users from viewing what websites you have accessed). If the main TOR site is blocked, try one of the mirror sites. You can read more about security in hostile environments here: http://blog.standbytaskforce.com/?p=259”