

Voix des Kivus

This case study examines how Voix des Kivus used FrontlineSMS for crowdseeding. It also discusses the associated data protection and security concerns, and actions taken by Voix des Kivus to reduce them.¹

Project Description	Voix des Kivus piloted a crowdseeding approach to assess the feasibility of SMS systems for gathering representative, verifiable information in real time from hard-to-reach areas.
Vulnerabilities	<ul style="list-style-type: none">• Data collection structure
Threats	<ul style="list-style-type: none">• Unrepresentative or incorrect information provided by the cell phone holders
Risks	<ul style="list-style-type: none">• Dissemination of sensitive bulletins to non-approved partners• Safety of cellphone holders and villages due to public knowledge of their participation in the project.
Risk Reduction	<ul style="list-style-type: none">• Crowdseeding system to ensure representative data• Internal validation by comparing multiple reports from same locations.• Limited distribution of sensitive information• Cell phone holders to provide a protection level for each event reported• Close monitoring by field staff

FrontlineSMS and Voix des Kivus

Voix des Kivus piloted a system to gather information about local level events (including acts of violence and atrocities) that took place in Eastern Congo's province of Sud Kivu. The pilot was led by Peter van der Windt and Macartan Humphreys from Columbia University and supported by a grant from USAID.

Events in conflict areas in poor countries often go unreported due to the lack of infrastructure and the danger associated with travel. Representative information is particularly hard to find. Voix des Kivus sought to examine how sourcing information via SMS can overcome these problems, making it possible for international organizations and humanitarian NGOs to respond to these events.

The system worked as follows. Upon entry into a new village Voix des Kivus would convene a village meeting to explain the project. Only with the consent of the village would three members be selected as phone holders: one representing traditional leadership, one representing women's groups and one elected by the community. These three would receive a cellphone, weekly credit and extensive training on how to use the mobile phone to report events. The phone holders were publicly known in the village so that villagers could report events to any of the three holders who would in turn sent an SMS report with this event. A codesheet given to the phone holders mapped a number (00-99) to a possible event (e.g. violence against women, riot or wedding) – meaning that phoneholders had only to send a number to report an event.

¹ Please find more information about Voix des Kivus at the following website:

<http://cu-csds.org/projects/event-mapping-in-congo/>. Note that after 18 months the Voix des Kivus pilot has come to an end on March 31, 2011.



Voix des Kivus used the FrontlineSMS platform to receive SMS reports from villagers. With the use of additional freely-available software, such as R and LaTeX, messages were automatically filtered, coded for content, cleaned, and disseminated through a weekly bulletin. Voix des Kivus was piloted in 18 villages in Congo's Sud Kivu province. During a period of eighteen months the pilot project received almost 5,000 messages of which more than a 1,000 were text messages. At eighteen villages – the first twelve months the project operated with only four villages –Voix des Kivus received around 400 non-empty SMS messages per month.

Data quality concerns

Key to the success of Voix des Kivus was the quality of the messages received. But because of the design of the project – operating in hard-to-reach areas with limited capacity – independently validating all information received from the phoneholders would not be possible. The project faced three major concerns regarding the data. First, phoneholders had to be encouraged to send SMS messages. Second, information received might be unrepresentative. Third, phone holders might send incorrect information.

Security concerns

Perhaps the most important concern for Voix des Kivus was the security of phoneholders. Over the course of eighteen months Voix des Kivus received thousands of messages of which a large number were sensitive. Because of the area in which the pilot project operated it was not uncommon for Voix des Kivus to receive information about sexual abuse and different types of violence perpetrated by different actors. While the project's goal was to share and collect information, dissemination could not be public as this could put the phoneholders at risk. Unlike many crowdsourcing systems there was a close connection between individual holders and the project raising a concern of reprisals against phoneholders for sharing information.

Actions to mitigate data quality concerns

We wanted to make sure that messages were free for senders but also that senders were free to report, or not, depending on their judgement. That is, we wanted to remove financial incentives to report but also financial constraints. Each week Voix des Kivus sent a fixed amount of phone credit to the phone holders that they could use as they saw fit (to call friends, call the hospital, or start a company, etc). In order to receive this credit the holder had to send at least one (possibly empty) SMS per week. In order to ensure that phoneholders could send more, Voix des Kivus reimbursed the phoneholders for all the SMS messages sent; however they did not receive payment per message beyond reimbursement.

The main novelty of Voix des Kivus, however, was the use of “crowd-seeding.” Rather than relying on spontaneous messaging by populations, crowdseeding works by using classic random sampling techniques from survey analysis to pre-identify phone holders who can send information into the system. This crowdseeding has three main advantages for data quality:

1. The data received is representative because the villages can be chosen randomly. This reduces biases that might arise from the fact that different populations might otherwise have different ability or interest in reporting to a system like this.
2. A long term relationship is established between the holder and the Voix des Kivus program thereby decreasing the incentive for phoneholder to send incorrect information.
3. Because more than one holder is selected in each village internal validation is possible.

Actions to mitigate security concerns

By making use of the freely-available software packages R and LaTeX, SMS messages were automatically filtered, coded for content, cleaned to remove duplicates and weekly bulletins were created. These weekly bulletins were generated in two versions. One version contained sensitive information (with village identifiers), the other did not. While the nonsensitive versions were posted publicly online, the sensitive bulletins were disseminated only to organizations and people working in those organizations that were approved by both Voix des Kivus and the cell phone holders. Thus neither the names of individuals, nor participating villages were made public, although the events data was.

In addition, after consultation with the phoneholders, Voix des Kivus added an extra component to the messages that phoneholders could send into the system. It was made possible for the phoneholders to include an extra code (1-3) to a message to indicate the event's level of sensitivity, and thereby with whom it the information was to be shared (only with Voix des Kivus, with Voix des Kivus and its partners, or with the wider world).

Conclusion

Voix des Kivus received around four hundred SMS messages per month reporting on a large number of different events from multiple sources in eighteen randomly selected (representative) areas of South Kivu. The pilot's eighteen months' experience with the crowdseeding system was positive: users were able and willing to use the system consistently and we encountered no security threats to participants of any form. However, although no incidents have occurred with eighteen villages, this might be different when the project is scaled up. On the one hand a project such as Voix des Kivus becomes truly useful when it is implemented at a large scale. However, this will also make it more widely known and could therefore potentially increase the associated vulnerabilities and risks, and make them harder to mitigate.

