Location-based data in crisis situations

Case studies

These case studies were developed by The Engine Room, together with the American Association for the Advancement of Science (AAAS). The exact events of these cases are fictitious, but are based upon information about real-life events gathered through desk research and interviews with practitioners. These cases are meant to be used with the accompanying Principles & Guidelines and Decision Trees published by AAAS.

Citizen drone data collection in response to mudslides

Data type: UAV data, including flight logs, geo-located photos and videos
Crisis: disaster, Central America
Key actors: international volunteers
Key principles: Do no harm (1), define your purpose (2A, B), do good science (3C, D)

Heavy rains create mudslides of historical proportions in Central America. Hundreds of people have been killed, with thousands more missing, injured and displaced from their homes. After declaring a state of emergency, one country requests international assistance with search and rescue efforts. There is particular concern about the situation in areas where access has been blocked by the mudslides. A student at a national university shares the call on a forum for enthusiasts of Unmanned Aerial Vehicles (UAVs), commonly known as drones. Deeply affected by the devastating images they see on the news, several international UAV pilots feel they should do something to help.

Some drone pilots have helped in past relief efforts in neighboring countries. Before arriving, they use their connections to get in touch with official search and rescue teams on the ground.

Other volunteer UAV pilots decide to immediately go to the areas they have seen on the news as being the worst affected to try to help. They haven't been trained in data collection for humanitarian relief, and they are unaware of the risks, responsibilities and ethical obligations they face in these contexts. Despite not having contact with organizations on the ground, they start to collect geo-located imagery without an explicit focus, rationalizing that what they collect "might be useful to someone eventually."

Communities in need of assistance are disappointed, frustrated and sometimes scared when they see an often unfamiliar object flying overhead. They had not expected this kind of intervention, nor do they know what might come of it.

The UAV pilots cannot speak Spanish, and have not been able to communicate well with formal search and rescue efforts and local authorities. The unexpected presence of a drone in one region causes the search and rescue operators to ground their helicopter for safety reasons, hampering rescue efforts.

Soon after, the volunteer UAV pilots return to their home countries. In the months after the mudslides, the government faces criticism over the delays in aid provision in the aftermath of the devastating mudslides. In response to the incident that required to grounding of the search and rescue helicopter, new laws are brought in severely restricting the use of UAVs, making it difficult for the small community of local UAV enthusiasts to fly their drones.

Discussion

- What should the UAV pilots have considered before engaging in the crisis response? How was their assessment of risk inadequate and how could it have been made better?"
- What steps could they have taken to better understand the **context**?
- Did the UAV pilots have a **clearly defined objective** for data collection?
- How could the UAV pilots have **collaborated** with the community and **built community capacity**?
- How could the UAV pilots – or others actors involved – have addressed their lack of **training** in crisis situations?

Removing location-based data to reduce risks in conflict

Data: crowd-mapping, GPS coordinates
Crisis: conflict, Middle East
Key actors: international health organization
Key principles: Do no harm (1A, B), define your purpose (2A), do good science (3F), give access to your data (5)

Three years into a conflict, a humanitarian organization has continued to monitor the security situation and begun to fear that its healthcare facilities may be targeted. In the past, they had shared clinics' locations to help patients find them, and because flagging healthcare facilities as humanitarian relief locations had granted them a measure of protection from air strikes. However, as the conflict has evolved, healthcare facilities and humanitarian organizations are increasingly being targeted. Many armed groups in the conflict are technologically sophisticated – they frequently share videos on social media, are known to use satellite imagery, and the government is known to have engaged in cyber warfare.

The organization decides to remove location-based data about their facilities from open source platforms like OpenStreetMap in order to protect the safety of their staff and patients. This prompts the humanitarian organization to review their location-based data collecting and sharing practices more broadly.

As part of this review of their data sharing and holding practices, the humanitarian organization discovers that a software they recently started using for patient health records is configured to automatically gather geolocation data (GPS coordinates).

The discovery prompts a debate within the organization. Some analysts argue that in emergency response contexts, such as rapidly growing refugee camps, GPS is the only information that is useful for location-based analysis of health information, as there are no other shared points of reference for location. This data, combined with patient health records, could help the organization track trends by location and allocate resources more effectively.

The organization has data security protocols in place, however some program managers are still concerned about the potential consequences if there were to be a data breach. Their primary responsibility is to do no harm to their patients, and they fear the potential risks of pinpointing patients' exact locations.

Moreover, the organization is known as a leader in its field and is recognized for the detailed data that they collect. They are committed to doing what they can to keep data confidential, in line with recognized standards of ethical conduct in the medical profession, but are unsure how to share it. Scientists and academics worldwide are interested in this data, and there are some calls to anonymize the data, and make it open and publicly available.

Discussion

- How could the organization **assess risks** related to sharing data about their facilities, particularly in **conflict** settings?
- What location data should the organization **collect** (if any) as part of its patient data records worldwide?
- When they are collecting this data, what should frontline healthcare workers explain to patients to ensure informed and meaningful **consent**?
- What patient data should the organization **share**, and with whom? What risks exist despite efforts at anonymization?

Using Call Detail Records to track a disease outbreak

Data: Call Detail Records
Crisis: disease outbreak, South East Asia
Key actors: mobile network operators, global health organization
Key principles: Do no harm (1), define your purpose (2), consider boundaries (2C), do good science (3B, E)

In South East Asia, there has been a new outbreak of H1N1 flu, otherwise known as swine flu, which is a potentially fatal virus. Fearing a repeat of an earlier worldwide pandemic, a global health organization requests Call Detail Records from mobile network operators in the country to build outbreak prediction models which can be used to channel resources and help prevent the spread of infection.

A Call Detail Record (CDR) is automatically created whenever a call is made or text message sent by mobile phone. Information gathered varies among mobile network operators, and while CDRs don't contain information about the content of the call or SMS, they may log data use, geolocation data, and record the duration and time of calls and the phone numbers attached to the activity. Geolocation data is generated either by triangulating data from cell towers nearest to callers and recipients' phones, or by GPS if a mobile phone subscriber has enabled location tracking on the phone or apps.

Using CDRs, the health organization aims to analyze aggregated population movement and predict the likely spread of disease at the community level. The dataset the mobile network operator shares is anonymized (with names and full phone numbers redacted), given that CDRs contain deeply personal and personally identifiable information.

Some high level staff within the health organization are pushing for the mobile network operator to grant them access to user data for contact tracing, arguing this is in the public interest. If this were to happen, they could combine CDRs with other datasets in order to create lists of individuals and communities at risk of infection. This would allow them to track the infected and potentially to contact them. However, since this data would contain personally identifiable data, some data scientists are concerned about the impacts a data breach could have. The organization goes ahead with the analysis of the anonymized CDR data granted by the operator, but do not get further access to detailed user data.

Months later, a post-response assessment notes that the health organization did not fully account for potential sources of bias within the datasets. Using CDRs in predictive modeling and contact tracing overlooked young children and the elderly, two groups who do not typically have mobile phones. The risk of death is higher for elderly patients, and the risk of contracting the virus is higher for young children.

Discussion

- What were the benefits of using CDRs? Did the benefits of collection and analysis outweigh the risks to individuals and communities?
- What **risks** and potential **harms** existed? How could they have been better identified?
- Could **informed consent** have been obtained from individuals or communities? What could the roles of the mobile network operator and the health organization been in the consent process?
- Given what you know about potential risks and potential sources of **bias**, how would you advise the organization to use (or not use) CDR data in future?

Fundraising video jeopardizes safety of gender-based violence survivors

Data type: video publicly shared on social media, with metadata removed and blurring of people's faces in the video
Crisis: protracted humanitarian crisis, East Africa
Key actors: NGO, refugee GBV survivors
Key principles: Do no harm (1), collaborate and consult (4), give access to your data (5B, E)

A non-governmental organization (NGO) works to tackle gender-based violence (GBV) among refugees fleeing conflict in East Africa through education, training and creation of safe spaces in towns and refugee camps. They rely on grants from institutional donors and donations from individuals to sustain their work, and they decide to refresh their existing communications materials to support a new fundraising campaign. After some preliminary research, the communications team learns that people are more likely to donate when they learn the stories of the GBV survivors that the NGO supports. The team consults with survivors about making a video to share their stories.

Five survivors agree to be in the video, as long as their faces are blurred and their voices are anonymized. The video is shot and edited, and the communications team makes sure that survivors' faces are blurred out, voices are disguised and sensitive video metadata – like creator and location information – is removed. Running late on their deadline, they share the video publicly as soon as it's ready.

The video is seen thousands of times, shared widely on social media, and helps to raise thousands of dollars for the fundraising campaign. The video cuts between interviews with survivors and their daily lives, following them as they walk through some of the NGO's centers and in their communities, including outside their homes. While not immediately obvious, if you pause the video and zoom in, location markers – such as shop signs and well-known community locations – are visible.

One survivor contacted an outreach worker for the NGO sounding upset and frightened. A man in the refugee camp where she lived had identified her home, waiting until she came outside and then following her. He verbally harassed her and referred to having seen the video on Facebook and recognizing her home. As he'd been living in the refugee camp for a few years, he knew the geography of the camp and could work out where she lived from location markers in the video. She managed to stop him from following her with the help of a friend, but is scared that he will continue to harass her, and that he will tell others in the camp.

Fearing for the safety of the survivor who had reported the harassment, and fearing for the safety and re-victimization of other survivors in the video, the NGO activates the contingency plan they have in place. This includes informing the survivors who appeared in the video about what has happened and prioritizing their protection, including finding them new accommodation if they feel unsafe. The NGO withdraws the video from its online communication channels, but it has already been shared thousands of times on social media, and copies may have been made.

Discussion

- How could the NGO have better ensured that they adhered to "**do no harm**"? How could they have foreseen this situation?
- Should they have changed *what* they **shared**, or the *format* in which it was shared?
- Did the NGO effectively **consult with the people represented in the data**? What could they have done differently?

Local volunteers use social media data to rescue flood victims

Data type: social media posts, including publicly shared statuses and locations from Twitter, Facebook and Instagram
Crisis: disaster, United States
Key actors: local volunteers
Key principles: Do no harm (1), do good science (3A, C, E), collaborate and consult (4)

Unusual weather conditions and heavier-than-expected rainfall cause widespread flooding in an urban area. People affected by the floods are tweeting and sharing their situation on social media, hoping to update relatives or reach their local police and fire departments. Emergency services are overwhelmed, so citizen volunteers step in to help communities affected by the flood, though these volunteers do not coordinate with official emergency responders.

The volunteers self-organize, with some people monitoring social media, including Twitter, Facebook and Instagram. The volunteers gather information such as names and locations of those who are stranded in their homes. They then convey this information to other volunteers with boats, who brave the weather conditions to carry out the rescue operations, despite having no formal training. Many of those who are rescued are grateful to the volunteers, but also surprised that strangers are able to know where they are.

A few days into the response, as the volunteer rescue squad becomes better known, they start encountering misinformation and fake cries for help. They have no way to verify the data they are collecting, and continue to respond to calls as they are able. Meanwhile, they face a growing backlash. Critics accuse them of bias and of only helping wealthier communities. The volunteer responders claim that this is false and that they dispatch as quickly as possible when they receive a call for help. However, they have not considered differences in network connectivity and higher smartphone usage among wealthier communities, which inevitably leads to inherent bias in who they offer help to.

A week into the response, the immediate need for rescue efforts has diminished. The volunteers start returning home and go back to their daily lives as there is less need for their assistance. Shortly after, traditional emergency services face heavy criticism for their inadequate capacity and are subjected to an assessment to identify ways to respond to these critiques. However, the informal volunteer network has quickly disbanded and a post-response assessment of their work is impossible. This makes it difficult to evaluate their effectiveness and community concerns of bias.

Discussion

- What potential **harms** face both volunteers and crisis-affected communities in this situation? How should the volunteer rescue squad **respond to and minimize the risks**?
- Have people affected by the floods posting on social media given *meaningful* **consent** for their information to be collected and shared with volunteer rescuers?
- What are the **ethical obligations** of volunteers monitoring social media to gather actionable information and dispatch for volunteer rescue boats? What should they consider as they're **collecting and aggregating** the data?
- How could the volunteers have **collaborated and consulted** with the affected community and other responders during and after the response?

Sharing a live-streamed video from a conflict zone

Data type: public social media livestream, satellite data (including geo-located images)
Crisis: conflict, Eastern Europe
Key actors: human rights organization, content creators
Key principles: Do no harm (1), do good science (3A), give access to your data (5F)

A social media editor working on advocacy and communications at a human rights organization discovers a video being live-streamed on Facebook from Eastern Europe. The video shows armed rebels in a besieged town. They are speaking to a camera, and showing the destruction of the town from a rooftop, which according to them was caused by government shelling overnight. The video seems to share important information that pertains to the human rights violations of civilians in the besieged town. The organization has had difficulty getting on-the-ground access in this conflict, so this kind of first-hand documentation is noteworthy to the social media editor.

The editor decides to begin screen grabbing (in effect 'recording') the video that is being livestreamed and alerts the research lead who is monitoring this conflict. The video is important evidence and advocacy material. The social media editor cannot safely communicate with the video makers to ask for their consent to collect this data, however they thinks that screen grabbing takes into account the needs and interests of the local community whose suffering during the siege has been underreported.

Before they consider using the video as evidence or sharing the video directly to their own social media, the advocacy organization must first verify that it is not fake. They do this by confirming information in the video and looking into its source. They notice location markers in the video, namely a prominent building in the background and a distinctive road. By comparing these markers with recent satellite data, they verify that the video was taken in the same small town that the rebels claim to be in and locate the building from which the rebels are live-streaming the video.

It took the advocacy organization very little time to verify the Facebook live-stream video using satellite imagery. They realize that if they can find the location this quickly, others would be able to as well. Right now, they're among a hundred or so people watching the livestream, but if they decide to amplify the broadcast by sharing the livestream with their large audience of followers, it could potentially reach millions of people, and would likely be noticed by the government. The media-savvy regime has a reputation for ruthlessly attacking rebel targets. The advocacy organization fears that if they re-share or re-broadcast the livestream, the regime would then retaliate against the rebels. However, some of their colleagues argue that the people shooting and livestreaming the video want their story to be told to the world.

With their knowledge of the context – and taking extra caution as it is a conflict environment – the advocacy organization holds a team meeting to evaluate the risks and come to a decision about broadcasting the video.

Discussion

- How familiar are the social media editor and researcher with the ongoing conflict in this country? How does their **knowledge of the context** influence the decision on whether to collect and share data?
- What tools could they use to **assess risks** and support their decision-making process?
- What recommendations would you make to the organization about **sharing** the video, and why? What steps could they take to mitigate the risks and minimize harm?