A collection of real-life examples of the risks that are faced when using data in advocacy work, along with mitigation strategies to overcome these challenges.

Creating an app for vulnerable communities

Using technology in order to reduce the incidence of violence among criminalised citizens.

Context

The primary organisation works to support and reduce violence against a disproportionately criminalised population–that is, a group who face disproportionate violence and social exclusion, and who are often treated as criminals without reason. For reasons of anonymity, the group they work with will be referred to throughout this case study as a criminalised population.

THEIR AIM: USING TECHNOLOGY TO EMPOWER MEMBERS OF THE CRIMINALISED POPULATION TO SHARE KNOWLEDGE AMONG THEMSELVES, ULTIMATELY REDUCING INCIDENCES OF VIOLENCE.

The primary organisation are working together with a social enterprise technology company to develop an application that members of the criminalised population can use to report incidents of violence. Their report is then sent out to members of the same community, who are in a similar geographic location to where the report originated from, and, if consent is given, the report is also shared with the police, with no details given about who reported it.

This kind of scheme has been happening in an analogue way for a relatively long time, but this is one of the first attempts to bring it into the digital space. It aims to help inform this specific community through **COLLECTIVE INTELLIGENCE**–helping others to inform their peers to keep them safe.

How it works

Currently, they use a system whereby members of the criminalised population can input reports anonymously via their website, then employees of the primary organisation are tasked with summarising these into shorter reports that can be sent out to other affected parties. With the app, they are exploring a new way of sharing this information as a peer to peer service, thus getting rid of the need for summarising and moderating to be done by the primary organisation.

Their partner company is managing the technical requirements of the app, so the primary organisation does not have direct access to the data. Because this is a partnership between two different organisations, with relatively different aims, they are working hard on negotiating an agreement between the two parties that meets both of their expectations and requirements.

Only members of the primary organisation's network have access to the app; and to become a member, they only need to submit their username and email address. This level of "membership" is kept deliberately low to make it as easy as possible for members of the criminalised population to sign up–by not having to put in names, they want to make it easy for them to remain anonymous with the app. They then fill in specified fields through the app to submit their report.

If the person submitting the report gives consent, the report is shared **ANONYMOUSLY** with the local police force, but without giving any further details about the person who submitted the report.

Challenges faced, and how they're being approached

Personally identifiable information

Under UK law, the reports which are sent out **CANNOT** contain personal information about the perpetrator, as at that point they are alleged to have done a crime, but have not yet been proven guilty. There is also a risk that the perpetrator might find out that they have been reported, leaving the person who reported the crime in potential danger. Balancing the reports sent out to be informative enough so that members of the criminalised population in the same area as where the crime was alleged to be committed can identify and avoid dangerous situations is a main challenge.

Planning for future situations

The Primary Organisation is mindful of the risk that potentially, the police or the UK justice system could issue a court order and get access to their data. With that in mind, they are actively practising **data minimisation** to make sure they have the minimum amount of data required.

They have also found that members of the criminalised population are more likely to be deterred from registering if they have to give lots of personal information, so data minimisation as a principle has multiple benefits. Those who are sending the reports do not want to give any information that might potentially be passed on to the police about their places of work, or any other details about their work.

Working in partnership

As the app is the result of a partnership between one topical focused charity organisation, and a tech-focused social enterprise, their aims have been somewhat different during the development. For the Primary Organisation, their main concern is making sure that **no harm** comes to any of the members of the criminalised population. The social enterprise, however, communicates in terms of "percentage risk"; whereas **any percentage risk at all is too much for the Primary Organisation**.

As the social enterprise is more focused on innovative tech solutions, they are keen to develop new tech solutions–this isn't an aim of the Primary Organisation though, who simply wants to focus on empowering members of the criminalised population to stay safe. Balancing between these different priorities has been a challenge, but they are both working with legal experts to make sure that they have clarity over important points in their partnership–such as who 'owns' the data, especially in case of one of the parties ceasing to operate.

The Primary Organisation does not have the in-house tech capacity to manage or develop the app, which is why their partnership is especially useful. But this has difficulties in terms of introducing dependency from the social issue-focused organisation, to the tech-focused social enterprise.

Moderation of content

Up until development and roll out of the application, when the system used was a website, these reports have been written by employees of the Primary Organisation, all of whom have undergone substantial legal training to make sure that they don't release any reports that could have potential legal consequences. However, with the application, a mode of peer-to-peer sharing is being explored, which means that the reports might go out without anyone from the Primary Organisation seeing them.

To mitigate against this, they have put a number of safety guards in place within the 'report' function in the app to ensure that potentially litigious information cannot be

put in; for example, no names of perpetrators can be submitted. They are conscious, though, that should an app user actively try to circumvent these safety guards, it would likely be possible to do so.

They are also exploring how effective these safety guards are in practice, through a pilot phase roll out, and they are mindful of the fact that perhaps this methodology simply won't work. Suggested alternatives to the automatic peer-to-peer report sharing would be reports going first to a moderator who "approves" them before they appear on the app; or a functionality where a moderator can quickly delete the report across all devices, if it proves to be unsuitable for sharing.

LISTENING TO THEIR COMMUNITY

The application was developed through a co-design process, working with members of the criminalised population to figure out the most effective and useful tool for them. The Primary Organisation is proceeding slowly and thoughtfully with the application, trying it out in small areas first, and very clearly putting the focus on their safety throughout, showing willingness to pull functionalities if they could put their community at risk.

Responsible Data Reflection Stories, 2016. This publication is part series found at **https://responsibledata.io**, produced by the engine room Responsible Data Program, 2016.