Transformative Technology for Migrant Workers

Case Studies

Developed by The Engine Room for Open Society Foundations

THE ENGINE ROOM

Accelerating Social Change

Table of Contents

Colophon

This report was written by The Engine Room from January-March 2018. The responsibility for the information and views expressed in the report lies with The Engine Room.
Researcher: Laura Guzman
Research support: Gabriela Ivens

Samaritians Radar

Launched in October 2014, suspended in November 2014, retired in March 2015

Highlight

The design and implementation of Samaritans Radar[1], which integrated with Twitter to serve its target population[2], was marked by a **lack of user-consultation** and the use of **opt-out (rather than opt-in) policies**. These provoked a strong, negative reaction among users and mental health experts, and the app was suspended nine days after being launched.

Case Study

Samaritans, a UK-based non-profit that provides emotional support to people in times of need, launched the Samaritans Radar, an "online app designed to offer people a second chance to see a tweet from someone they know who might be struggling to cope." Samaritans Radar worked by monitoring the Twitter feed of those that installed Samaritan Radar to see if **anybody followed by the user** had tweeted specific keywords or phrases identified as being commonly used by people who are struggling to cope, such as "I hate myself". If a tweet with those keywords was found, the Samaritan Radar app user (not the profile that sent the tweet in question) would receive an email with a link to that tweet, along with suggested guidance on potential actions that would support the person who had tweeted the message.

The impulse to leverage and integrate social media is strong, especially when opportunities to provide positive support seem to exist. However, response to the application was mixed; some lauded its innovative approach to using social media, but others - notably, many from the mental health community in the UK - reacted strongly against the app. Ultimately, the negative feedback was so strong that Samaritans suspended the app just nine days after the launch and ultimately shut it down. Two key aspects of what made the app problematic were: limited user consultation prior to launch and the use of **opt-out rather than opt-in** policies.

Limited user consultation: In considering the failures of Samaritans Radar, Samaritans explained: "We've learned that we must consult even more widely than we have done in the development of Samaritans Radar and we will continue to respect and better understand the diversity of existing communities and users. To this end, we will be holding a series of consultation events as well as continuing to gather views via an online survey from as wide a range of people as possible."

Opt-out rather than opt-in: Essentially, the app made very visible and explicit anything that someone tweeted publicly with predefined "keywords". Technically, anything tweeted from an open account (ie. as opposed to a "closed" account where the user approves individually anyone who wants to follow their tweets) is indeed public. However, users often think of tweets as 'private', especially users who have very few followers or who expect

[1] More detail on the project can be found here - https://www.samaritans.org/how-we-can-help-you/supporting-someone-online/samaritans-radar

[2] Read more about this project and the responsible data issues here - https://responsibledata.io/reflection-stories/samaritans-radar/

very few people to see their tweets. If an individual tweeted a message flagged by Samaritans Radar, any followers of theirs using the Samaritans Radar app would receive a notification. However, the user who originally tweeted the flagged message would have no knowledge that their tweets were being monitored. Samaritans Radar later added a feature wherein any Twitter user could request to be whitelisted so that their tweets would not be followed. However, this required that Twitter users be aware of the Samaritans Radar app and how it worked, and that they know their tweets could be monitored without consent. This is knowledge and access that not all Twitter users had.

Vulnerable groups app

Highlight

An organisation[3] working with a criminalised population uses **data minimisation** and **partnerships** to maximise the impact of their work and mitigate potential risks. Due to privacy concerns of this organisation they are referred to as ´Primary Organisation´ throughout the case study.

Case Study

Using technology, a Primary Organisation empowers members of a criminalised population[4] to share knowledge among themselves and report incidents of violence, with the aim of reducing this violence. Currently, the Primary Organisation uses a system whereby members of the criminalised population can input reports anonymously via their website. Employees of the primary organisation are then 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.

Partnerships: The Primary Organisation is partnering with a social enterprise to manage the technical requirements of the app. For the Primary Organisation, their main concern is making sure that no harm comes to any of the members of the criminalised population. 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.

Data minimisation: To become a member, users only need to submit their username and email address. This level of "membership" is kept deliberately low for two reasons. First, to make it as easy as possible for members of the criminalised population to sign up. By not requiring users to put in names, it makes it easier for users to remain anonymous. Additionally, the Primary Organisation is aware that the police or national justice system could issue a court order at get access to their data. With that in mind, they are actively practising data minimisation to limit the data that would be exposed if a court order were to be issued.

---

[3] Read the case study here - https://responsibledata.io/reflection-stories/app-vulnerable-communities/

[4] 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.

Medicapt

Launched in April 2012, ongoing

Highlight

Physicians for Human Rights looked extensively at pre-existing technology solutions before beginning development of their own app, and they brought in end-users early in their process in order to create a tool for working with sensitive data.

Case Study

In conflict zones, those that experience sexual violence rarely report their experiences, facing social stigmas, fear of reprisals, or lack of knowledge on how to report. The Program on Sexual Violence in Conflict Zones – launched by Physicians for Human Rights – aims to help survivors who do come forward increase the likelihood of successful prosecutions by providing tools and trainings to help first responders to more effectively collect, document and preserve forensic evidence of sexual violence to support allegations of these crimes. The project identified the need for a technical solution that could be used to support this process, involving multiple stakeholders, of collecting and preserving forensic evidence. This solution became an application called Medcapt.

Testing pre-existing solutions: Before beginning development of a new application, Physicians for Human Rights undertook a landscape review of existing technology tools that might have been suitable for their needs. They interviewed technologists, privacy specialists and public health workers. Eventually, they tested out the most promising existing technology in the field with seven clinicians from different hospitals. It turned out that putting their standardised forms into the platform resulted in a very cumbersome process for clinicians who had to use it. They learned two major things: that convincing them of the benefits of the technology was not an issue, but that this platform was not a viable way of allowing them to access these benefits.

Consulting end-users: From the very beginning – understanding what the current process of reporting assaults looks like – the project team brought together people with differing roles such as doctors, nurses, police officers, lawyers and judges, so that they could explain their specific roles and responsibilities to each other. They identified existing obstacles — difficulty in transportation, terrible road conditions, costs of paper and printing – and used these to inform their project from the beginning. When beginning development, the team held workshops with potential end-users, asking them what the 'must-haves, should-haves, and could-haves' would be for the technology to be useful. The team user-tested the new platform during development, after development, and returned a year after initial deployment to see what long-term and new users thought about the app and its features.

Panic Button Training Kit

Launched in March 2014 and retired in September 2017

Highlight

The Panic Button app, aimed at supporting the security of human rights defenders, launched a Training Kit that users could consult when setting up and using the app. The Kit **increased user literacy** around digital and physical security and **ensured informed consent** from its users.

Case Study

Panic Button was an Android app devised to help protect human rights defenders (HRDs) by turning their smartphone into a beacon that notifies a trusted group of individuals (called a PACT) of the phone owner's position and situation.

Use of the app required good digital and physical security practices and could itself introduce different variables into how the HRDs should think about their threat models. Because of this, Amnesty International conducted training sessions for Panic Button users from the outset. Eventually, they saw an opportunity to extend the impact of these trainings by creating a Training Kit[5] that could be used by anyone, anywhere.

Increasing user literacy: The Training Kit consisted of a set of training cards and a role-playing game called imPACT. The content was based on Amnesty International methodology, which had been fine-tuned over months of assisting communities at risk to integrate the Panic Button into their work. By providing targeted activities and tools, it increased users' understandings of risks that they faced – both with and without the app – and help them think through them differently. It also helped them consider how using the app could reduce their vulnerabilities.

Ensuring informed consent: By increasing user literacy, the Training Kit also made it possible to ensure informed consent. Through the Training Kit, users of the app could freely explore both the benefits and risks of use and what data might be collected. Then, they were able to consent to using the app, having first assessed not just its policies and technologies, but its impact on their own situations.

Ending an initiative responsibly: When the Panic Button app was shut down, their site[6] made clear that it was no longer supported, and the underlying code was made available with a free software license enabling others to work on it in the future. The team behind the app wrote openly on the reasons why the app was being retired.[7]

[5] Full disclosure: The Engine Room was involved in the development of the Training Kit, in partnership with Amnesty International and Mushon Zer-Aviv. Read more about the process here - https://www.theengineroom.org/from-a-button-to-a-pact-scaling-security-through-design/

[6] https://panicbutton.io/

[7] https://www.theengineroom.org/panic-button-retiring-the-app/

Farmobile

Launched in 2013, ongoing

Highlight

Farmobile[8] enables farmers to collect and sell EFRs (Electronic Field Records i.e. farm data), through their app. Farmobile proposes an **alternative revenue stream** for app users, offers a clear **opt-in data-sharing policy** and ensures **users retain control of their data**.

Case Study

Users of the Farmobile app register for a subscription wherein they are given devices to collect machine and agronomic data constantly. This data is collected by a device that attaches to farm machinery in order to record both the datasets picked up by sensors on the farm equipment itself (e.g. total harvest, rate of spray, number of seeds) and ongoing location data. Farmers can access this data through the Farmobile Dashboard in order to boost efficiency and share field reports with their team. If the farmer wishes to do so, they can opt in to putting their data in the data store, where it can be purchased by third-party buyers.

Opt-in data-sharing policy: By default, farmers' data is not shared to anyone that each user has not specifically approved. Farmers can add specific permissions so that different team members – from fellow farm workers to insurance agents – have access to different datasets. Further, if they wish to place their data on the Farmobile data store, they must opt in to that separately as well.

User control of data: Farmobile has a clear, plain-language data sharing policy that outlines the usage rights related to the data, and it is centers the right of individual farmers to control their data. It is up to the farmer to decide how to use their data, and Farmobile makes it easy to set permissions and agree (or not) to placing the data on the Farmobile data store. Even once the data is in the store, farmers must approve each transaction and are free to reject it.

Alternative revenue stream: Farmers who choose to opt-in to the Farmobile store receive compensation for their data, which can add an extra layer of security to their potentially volatile yearly earnings. Farmobile states, "You own the data, so you should profit."

[8] https://www.farmobile.com/

Extended Case Study: Contratatos

Launched in 2014

Highlight

Contratados, developed by Centro del los Derechos del Migrante (CDM), is an online platform where migrant workers in Mexico and the USA can rate and review employers and recruiters. In developing and maintaining this platform, CDM have made a number of important trade offs, balancing the imperative to protect the security and privacy of its users, with the desire to increase the utility and potential impact of the platform. A number of these decisions are explored below.

Case Study

CDM considered the opportunity that Contratados could provide to engage and empower migrant workers with targeted information. For example, if the platform gathered location data from users, migrant workers could be presented with location specific information, such as the contact details of local advocacy services and support, which could facilitate their access to justice. However, gathering information about users' locations could put workers at risk if there were a data breach of some kind. CDM decided not to gather this information, and to forgo the opportunity to provide targeted information to users of their platform.

CDM integrated voice and SMS messaging into their platform, to open it up to a wider group of workers for whom literacy or access to the internet could be a barrier to access. Although this functionality was built into the platform, on balance, they decided that they would need to make significant improvements in security before they could integrate this data into the publicly available database. For example, they would need to find ways to obscure people's voices, and to better integrate voice review content into the narrative reviews. This would require resources and development time that CDM do not have at this point, so they are no longer soliciting voice and SMS reviews. CDM felt that the utility of the information when compared with the potential risk to users was not great enough to justify promoting its use.

> "Without fixes and changes, and better integration into the other components of the platform… It would be really nice - it would be great to do, but given where we are, we would rather spend resources on other fixes, and dissemination."

Verification of reviews was another decision point for CDM. As a rate and review platform, they felt that the value comes from the quantity of reviews – a critical mass that allows other migrant workers to discern which organisations they can trust, and which they should avoid. But for the platform to have an impact, people need to trust the content. Outside of verifying the identities of workers leaving reviews, which would pose obvious security risks, CDM have considered other ways of highlighting the credibility of reviews. This could include allowing users to "up vote" or comment on reviews, so that those reviews which other users find most helpful, or agree with, rise to the top.

This feedback mechanism could also boost engagement with the platform. For platforms

such as Contratados, whose goal is to prevent fraud or harmful behaviour, communicating the impact of taking part to workers, and encouraging repeat engagement with the platform can be challenging.

> "[Users] expect that as a result of their reviews, other workers will be more informed, and they will therefore prevent other workers from falling victim to the same abuses. They expect to support other workers to defend their rights, rather than receive personal remediation."

Providing workers with a sense of how many people read their review, or find it helpful could act as a very simple feedback mechanism for reviewers, showing that their contribution has been useful to the community, whilst also highlighting the credibility of the reviews. However, CDM do not currently have the resources to implement this feature.

> "There is a whole host of things you could do to make this tool more effective in the long run. Without sufficient resources to make sure that you're constantly monitoring security… you don't want to add things that could potentially put people in a difficult situation. We've gone down the more low tech route to avoid these risks."

Responsible data practices

There are huge risks for workers leaving reviews and sharing information about their workplace experiences on a public platform. There is the possibility for retaliation from employers or recruiters, including risks to workers' physical safety. CDM have attempted to mitigate these risks, and risks to the organisation's security in a number of ways.

> "A lot of the reasons that we have adopted the practices we have is based on a Risk analysis of the specific context that we're working in. It may be different for other organisations."

Data minimisation: The only personally identifiable information that is collected about anonymous users of the platform is their IP address

Data retention: CDM only store IP addresses for 90 days, at which point they are deleted from their servers. 90 days was deemed long enough to see patterns in use and utility, and to analyse potential security issues. One of CDM's main concerns is being served a subpoena to identify people who leave negative reviews. By flushing the data they have every 90 days, they reduce the risk of this happening, as they don't have access to that information.

Server location: To add another barrier to people trying to access this data through subpoenas, they store the data on servers outside of the USA and Mexico.

Data security review: CDM engaged with Benetech, who conducted a full security review of the site.

Open source tools: CDM use an open source platform for analytics and open source servers for storing data.

Anonymous users: The vast majority of migrant workers use Contratados anonymously, meaning they do not provide their names, addresses or other personal data to CDM in order to use the platform.

Organisational security: In order to maintain their eligibility for exemption from defamation laws and others, CDM do not help people to complete reviews, nor do they write any reviews themselves, or edit reviews that are submitted.

Updating practices: CDM regularly review and update their policies and practices around data privacy and security, and are currently reviewing their data retention policies with regards for how they apply to social media content.

> "We need to continue thinking about how our new practices are impacting how people use the site and what data we're collecting. It's about making data security and digital security part of your institution's culture"