"SECURITY IS COMMUNITY": Lessons from the Panic Button experience

EXECUTIVE SUMMARY

Originally situated within the Security with Human Rights Campaign at Amnesty International (AI), the Panic Button project was born out of a desire to creatively engage with technologists to positively impact on situations of enforced disappearances and unlawful detention. Between November 2011 and January 2012 hundreds of designers, technologists and human rights activists were invited to submit their ideas about how technology could be used to help protect individuals at risk as part of an open innovation challenge AI ran in collaboration with design agency openIDEO.[1] This was the first time AI publically opened up its work to the input and ideas of the technology and design communities to seek new and creative solutions to human rights challenges.

The open innovation challenge, which reaped 360 strong and creative concepts, set AI on the course to design and develop a smartphone alert app for human rights defenders (HRDs) - the Panic Button App.[2] The app aims to quickly and discretely alert an HRD's network of an impending or occurring physical security threat when activated. Following two years of design, development and testing involving more than 150 human rights activists, 25 developers and a strong community of partners and advisers, a beta version of the app for Android was launched on the Google playstore in June 2014.[3] It has since been downloaded and tested by 5,000 users in countries across the world.

From the outset the project was about much more than developing an app. At its centre, the Panic Button project aimed to develop a model for strong peer-to-peer response mechanisms between HRDs and their networks. It did this by collaborating with HRDs to understand and build upon their existing practise and by designing a flexible security framework that would help them prepare for and manage physical security threats. This framework is called the PACT (Prepare-Act) and it was piloted - along with the app - with 120 HRDs from 3 regions (Africa, Asia and Latin America) in a series of workshops and a testing period between March and December 2014.

This evaluation report reflects on the learnings of the Panic Button project since its inception in 2011, documenting AI's methodology and approach and presenting feedback from those it aimed to support. The report is primarily based on qualitative insights gained from 39 HRDs who participated in the pilot workshops and the feedback and testimony they provided in a series of surveys about how they had used the app during the testing period.[4] In

---

[1] OpenIDEO and Amnesty International Open Innovation Challenge, *How can technology help people working to uphold human rights in the face of unlawful detention?,* online at: https://openideo.com/challenge/amnesty/brief
[2] The project was funded with a $120,000 grant from the Ford Foundation followed by a £100,000 from the Google Global Impact Award. The Amnesty Swedish Fund and Amnesty Switzerland also contributed £25,000 to the project's global pilot.
[3] Panic Button App (Beta), Google Playstore, online at: https://play.google.com/store/apps/details?id=org.iilab.pb&hl=en
[4] All surveys were conducted using Survey Monkey. There were three surveys in total over the testing period, in English and

addition, we draw on key insights provided by partners and the feedback of beta testers globally who reported technical bugs to us following the public beta release on the Google playstore in June 2014.

While the data in this report is not statistically representative of the participants who took part in the global pilot, it gives insight into how the HRDs who took part feel about the overall Panic Button project. Throughout the report, suggestions and comments from the pilot participants are incorporated. The evaluation assesses many aspects of the project – from the usability and utility of the app itself to the effectiveness of the PACT framework. We hope that this evaluation will provide useful insights for NGOs and civil society, funders and technology developers interested in how technology can be used to support HRD protection.

The strongly positive response from HRDs who responded to the surveys is notable in light of the technical barriers faced during the pilot. A major technical bug was brought to the attention of AI following the beta release on Google playstore in June 2014. This was the 'false alert' problem whereby the app began to send alert messages without the user having proactively activated the alert. The false alert bug was both frustrating and confusing for users and in some cases actively contributed to fear, as their contacts believed something had happened to them. While the team worked hard to identify the cause of the problem, this was a major and unanticipated technical challenge and its resolution was delayed due to resource and capacity constraints. After putting more resources towards the resolution of the problem, the current version has significantly diminished the problem, emphasizing the importance of sustained technology support to address unforeseen issues and provide improvements long after a technology project is first launched.

Despite this major technical hurdle, every respondent who completed the final survey said they would use Panic Button in the future if the technical problems were fixed.[5] HRDs continued to reiterate its relevancy as a tool in their security plans, even as they noted its limitations. In two cases, for example, HRDs reported that they had faced a threat but were unable to use the Panic Button because of lack of phone signal. Other reported limitations included not having enough time to activate the device and not being able to use the app because their phones ran out of credit. HRDs noted that they often felt at higher risk when working in rural and isolated communities and that poor telecommunication infrastructure represented a challenge to their security. Despite these limitations, respondents emphasized that the app could support them in their work by helping them be more prepared for risks and making them feel confident that their networks would respond rapidly should something happen to them.

"In the dry run, a lawyer who was in my list called me up just few minutes after the button was triggered, my wife provided me with the map of my exact location. So this would be very helpful in real life. If only all HRDs in Basilan were equipped with the

Spanish. Only 39 people out of a total pilot group of 120 answered at least one of the surveys.

[5] 23 participants responded to the final survey in December 2014. This represents 15% of the total participants who took part in the pilot.

system, I could have responded to friends and relatives who just went missing many years ago."

- *HRD, Philippines*

Feedback from participants revealed that the greatest contribution that the Panic Button project had made to their security was the PACT framework and security methodology. According to those who responded to the surveys, creating a PACT has made them, and those close to them, more aware of security concerns, frequently monitoring each other's security, improving communication and enhancing current security protocols. The PACT framework was integrated into HRD networks' security protocols in a number of countries. A participant from the HRDs Network in Uganda commented that "Panic Button reinforced the already existing individual and organizational security mechanisms" and that the PACT "has formed a big part of our security management trainings". In Honduras, a women human rights defenders networkreported that it has integrated the PACT into security protocols at the national level.

"The Panic Button is a fundamental strategy for alerting but also for devising a security plan and articulating this with our contacts so that the plan is strategic and coordinated…The workshop has forced us to sit down and work out what would we do and how to be able to guarantee a greater level of security for women human rights defenders."

- *HRD, Mexico*

A further key learning has been the value of integrating technology within traditional human rights protection approaches. From the beginning of the project, AI were aware that involving HRDs in the design process would be key to ensuring that the app would work for its users. For this reason we engaged in a co-design process where we involved HRDs in designing the project and invested time and resources in testing and feedback throughout. This was a mutual learning process for both AI and the HRDs we worked with, helping everyone gain greater understanding of how technology interacts with security, both supporting HRD protection and also presenting new threats. Several of the participants reported that they has previously found technology alienating, reserved for those with a technology skillset or background. The Panic Button project has helped HRDs to recognize the importance of technology and to take ownership in the development of technologies that can support their own security and protection.

Overall, the varied feedback from our users affirms that the greatest value of the Panic Button project lies in the real-world relationships between HRDs and their trusted contacts, and the ways that these can be strengthened for emergency response when an HRD faces a situation of risk. In this way, the Panic Button project represents a technology-based strategy for planning, mitigation and response to physical attacks on HRDs and not simply a mobile alert tool. As one participant put it, "Security is community. Having a PACT gives you a sense of security."

"Security is community. Having a PACT gives you a sense of security."

AI has benefitted immensely from working alongside partner organizations who contributed diverse expertise to the design and delivery of the project and who will continue to play an even greater role moving forward. The engine room, which investigates and supports the effective use of technology by civil society, brought both strategic

insights and practical advice during every phase in the project's implementation. Frontline Defenders, an international organization working to protect HRDs at risk, provided input into the development of the app and training methodology and provided a further feedback loop with HRDs they support and train. Finally, iilab (information innovation lab), a small technology social enterprise, played the pivotal role in moving the project to its beta launch and providing the technology management expertise that helped bring together the various dimensions of the project.

For the future of the project, working with partners that see the value in open and user centric methodologies will continue to be key. For instance, one of the avenues to explore is growing the community of open source contributors who will focus their talent and resources to improve Panic Button as a technology base that is capable of serving different needsOur intention is to create a 'modular' codebase so that Panic Button can easily be repurposed and packaged by others.

This evaluation of the Panic Button project charts the development of the project from its inception, initial assumptions made, the development of the mobile app and PACT framework, partnerships with HRD networks and other organizations and the learnings that reshaped the project. We believe the evaluation provides rich insights about:

> Open Source
>
> Panic Button was developed using Open Source licenses, allowing anyone to freely access, use, modify, and share the application technology for any purpose.
>
> This choice has also enabled the building of strong partnerships with other organisations which have adopted these principles.
>
> It has also allowed several technology partners to work in turns on the software development and contributes to the aim of developing a technology community that will continue to improve Panic Button.

- the importance of networking and information sharing in creating robust peer-to-peer and network security mechanisms;
- the role of participatory training methodologies to assist in practical and contextually relevant security planning;
- observations about both the role played by, and limitations of, technology as a tool for HRD protection.
- AI's strengths in relation to this project and the challenges we faced.

We hope that this evaluation will help others who are interested in using technology to support HRDs to develop and implement genuinely impactful projects.

Lessons learned from the Panic Button project:
- There is tremendous value in employing user-led and co-design methodologies when developing technology-based approaches to security and protection within the human rights field. This includes ensuring that there are enough time and resources to work with user communities in a concerted and sustainable manner.
- It is important to focus beyond tools on creating *technology-enabled strategies*. Great efforts must be taken when designing a technology project to facilitate the necessary behavioural change that will support effective use of a tool.
- Relying on mobile (and in particular smartphone) technology will limit the utility of the app for many HRDs who do not have the financial resources to access smartphones and/or live in areas where connectivity and coverage issues render mobile phones ineffective.
- Ensuring that a technology project is well supported with adequate technical and financial resources over time is essential to ensure a high quality and reliable product, and quick response time when something

goes wrong. This is even more crucial when developing a tool on which people's physical and emotional security depends.

- Building technology is hard and even careful planning cannot prevent technical challenges from arising. NGOs play a vital role in bridging software developers and user communities, however they generally lack expertise in product development. It is recommended that NGOs invest in a long-term partnership with an organization with technical expertise and together share ownership of delivery, recognizing that partners with diverse expertise create a stronger end product.

- Mobile technology has inherent security risks, particularly to HRDs and others who may be targeted and monitored by the state. Engaging experts to understand the threat model for your target users is important, as is communicating the risks clearly so that users can take an informed decision before using the technology.

Where next for Panic Button?

Our vision is that by June 2017, hundreds of human rights networks around the world will have integrated Panic Button and the PACT framework into their security protocols, empowering HRDs at risk and their close networks to feel more equipped to respond to physical threats that occur in the course of their work.

June 2015-June 2017, the Panic Button initiative will focus on:

- developing and improving the existing app and PACT materials and increasing their value and relevancy to end-users by facilitating product localization, adaptation and reuse;
- supporting local/national and international partners to deploy the app, by providing materials, advice/mentorship and growing a network of 'Panic Button' trainers regionally
- investing in research and development that will help Panic Button reach more people in remote/rural areas;
- exploring interactivetraining methodologies for HRD security planning and emergency response;
- fostering stronger relationships and knowledge sharing within the sector, including by strengthening support within the open-source community.

OVERVIEW OF THE PANIC BUTTON PROJECT

A PARTNER-DRIVEN PROJECT

Originally situated within the Security with Human Rights Campaign at AI, the Panic Button project was born out of a desire to creatively engage with technologists to positively impact on situations of enforced disappearances. In the three years since its inception, the project has allowed AI to take a firm step into the emerging field of technology and human rights, whilst drawing on the organization's lengthy experience supporting the protection of HRDs.

At the same time, AI has benefitted immensely from the contributions made by partner organizations who contributed diverse expertise to the design and delivery of the project and who will continue to play an even greater role moving forward. The engine room, which investigates and supports the effective use of technology by civil society, brought both strategic insights and practical advice during every phase in the project's implementation.

Frontline Defenders, an organization working to protect HRDs at risk, provided input into the development of the

app and training methodology and provided a feedback loop with HRDs they support, helping AI to identify technical issues and gather new ideas for improvement of the application.

Iilab – information innovation lab - a small technology social enterprise, played a pivotal role in moving the project to its beta launch and providing the technology management expertise that helped coordinate the various dimensions of the project. Partnering with a technical organisation focused on social impact projects that shared AI's vision for the project brought deeper contextual understanding and led to a more robust product. However, the project was delayed due to limited self-funding capacity to address more difficult technical issues that emerged, which presented a challenge when it came to dealing with unanticipated technical issues during the pilot phase. When investigating the 'false alert' bug, AI temporarily contracted ThoughtWorks to increase the team's technical capacity to identify and resolve this problem.

For the future of the project, working with partners that see the value in open and user centric methodologies will continue to be key. For instance, one of the avenues to explore is growing the community of open source contributors who will focus their talent and resources to improve Panic Button as a technology base that is capable of serving different needs (e.g. journalists, citizens at risk of kidnapping in complex security environments, women at risk of sexual and/or domestic violence). Our intention is to create a 'modular' codebase so that Panic Button can easily be repurposed and packaged by others.

Successful open source projects usually succeed in engaging a community of engineers who are themselves in need of the technology solution they contribute to. For Panic Button, involving partners that were committed to the issue we were trying to address was critical. As we move forward, we will continue to engage with open source communities that focus on human rights but maybe more importantly, aim to build relationships with technologists who have deeper contextual knowledge and understanding of users' needs in their country to make the app more relevant and widely available.

The project was funded with a $120,000 grant from the Ford Foundation followed by a £100,000 from the Google Global Impact Award. The Amnesty Swedish Fund and Amnesty Switzerland also contributed £25,000 to the pilot.

HOW THE APP WORKS

Panic Button is designed to turn a mobile phone into a secret alarm for when an activist is under threat. The app, which is currently on Android only, works by sending an emergency SMS to 3 trusted contacts who are pre-configured by the user. Once it is triggered in an emergency situation, a customized message and the location coordinates will be sent to the user's 3 contacts, who will continue to be updated with the phone's location on a periodic basis (the default is every 5 minutes but this can also be customized). The idea is that an activist's trusted network will be able to respond swiftly if the activist is at risk of arrest or abduction, assisted by ongoing location information to help them identify the last known location of the activist's phone.
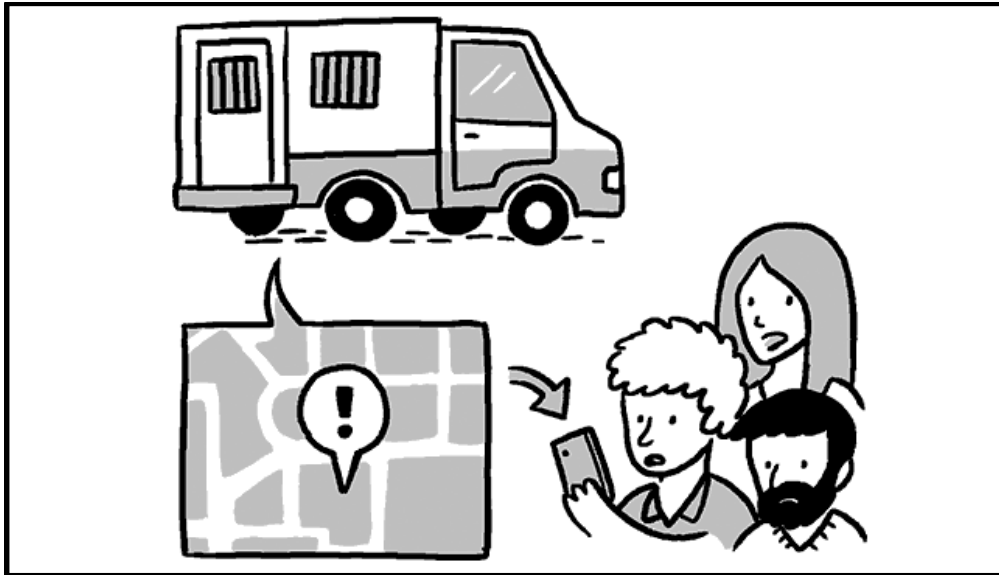
- *Illustration of how Panic Button is designed to work in an emergency. A user's three contacts will receive an SMS and regular updates of their location helping them to act fast.*

The app contains several features that were designed to make it functionally useful for activists at high-risk of arrest or abduction:

1. **Rapid and discreet triggering of the alert by pressing the phone's power button**
   The rationale behind this feature was that it would be too onerous in an emergency to open up a phone and trigger an app from the phone's homescreen. Further delay would be caused if the phone required a pin number to unlock it. The hardware button would be a quicker way to trigger the alerts and would also allow for a degree of discretion if an attacker were close by.

2. **Disguised app façade to mitigate against discovery**
   We designed the app screen as a working calculator app in order to minimize the risk of discovery by an attacker and therefore make it less likely that the alerts and location updates would be easily deactivated. In order to access the deactivation button and contact data of the three recipients, an attacker would need to identify the app, dismiss the calculator façade with a secret gesture on the calculator screen and enter a pin number. While technically sophisticated attackers might be able to identify the app and detect the alert, the design intends to delay this long enough to provide potentially vital information.

3. **Set-up advice and support for making a security plan**
   Throughout the app, security tips and advice are provided so that the user will consider carefully the non-technical elements that are necessary to use their mobile phone securely and to guarantee their contacts will be able to respond in an emergency. This includes tips on selecting appropriate contacts, customizing the alert message, thinking through risk and ensuring the phone is fully prepared with battery and credit when going into a risky situation.

CREATING A 'PACT' WITH YOUR NETWORK

Designing and developing an Android app was only ever one part of the project. From the outset, the larger goal was to build a framework that could form an integral component of security protocols and practices for HRDs, based on and supporting local response mechanisms and resources. This is embodied in the PACT concept, a risk and planning framework that we developed during the course of the Panic Button project to help HRDs think through and create an emergency response plan with their trusted networks.

The PACT is a plan created between an HRD and three contacts who they choose to be their 'first-tier responders' in an emergency. It is a comprehensive security plan that aims to facilitate immediate and effective action when an HRD is under threat. The PACT framework encourages a defender to think through the practical steps that would form part of such a plan. This includes questions such as: once your contact receives an alert, should they try and find you? What risk would this pose to them? Should they contact the police? Would the police be an adversary or an ally? Who else might they want to contact, thinking about the media, local politicians, international NGOs and foreign diplomatic missions in the country? There is no 'ideal' PACT as situations and circumstances can vary greatly; that is why it is important for HRDs and their networks to develop flexible response plans outlining what action may be taken next, what information should be prepared beforehand and who the wider actors are at the local, national and international levels that may be called upon in an emergency.

PILOTING PANIC BUTTON

Between March-May 2014, four regional workshops took place as part of the roll out of the first version of the Panic Button app. These workshops initiated a testing phase until December 2014, during which AI gathered feedback from HRDs on how they were using the app. The workshops were planned and delivered with four networks, directly reaching 120 HRDs from a total of 17 countries.[6] These workshops took place in the Philippines (February 2014), El Salvador (April 2014) and Uganda (May 2014). A number of the HRDs that participated in the global Panic Button pilots did not have Android phones that would allow them to use the Panic Button App. We therefore provided handsets to the participants, both for their own use and to distribute with their networks. In total we provided 234 mobile handsets (100 in the Philippines, 100 in Uganda and 34 in El Salvador). The resources for these handsets were provided by the Swedish Amnesty Fund and AI Switzerland.

In supplying participants with smartphones we identified a number of risks, which we addressed in the project design and training. We were conscious of potentially increasing the risk to HRDs by attracting attention and

---

[6] Pilots took place in partnership with the four networks: Karapatan: Alliance for the Advancement of People's Rights and Philippine Alliance of Human Rights Advocates (PAHRA) in the Philippines; the Mesoamerican Women HRDs Initiative (IM Defensoras) which works in 5 countries in Central American and the East and Horn of Africa HRDs Project (EHAHRDP) which works in 12 countries in Africa.

exposing them to greater scrutiny in communities where smartphones are not common. In addition, we were concerned about the potential threats posed to women HRDs in relation to access and control of their mobile phone by husbands and other family members. Smartphones make it easier for users to remotely track or follow the movement of a phone by installing a simple app or through built-in services designed to help users locate a lost or stolen phone. Women HRDs often hide the nature of their work from their families because of familial or societal pressure that views such work as unacceptable. So being in possession of a smartphone might raise suspicion but also allow family members to secretly track their movement. Smartphones also give governments greater tracking and monitoring powers, such as additional GPS tracking capabilities, which could facilitate greater targeted digital surveillance of some HRDs.

We worked with the networks in each country to include a risk assessment in the participant selection process. We also purchased low specification handsets locally to ensure the model would be a widespread, affordable and popular phone in the relevant country/region. Digital security trainers from Tactical Technology Collective and Frontline Defenders co-facilitated each workshop in order to integrate aspects of digital and mobile security awareness into the workshop delivery. We focused on raising awareness of the ways that mobile phones can reveal personal information or be used by the authorities for tracking and identification. The training covered: how mobile phone networks work, understanding GPS, security trade-offs and when to avoid using a mobile phone, alternative ways to communicate sensitive information over SMS (e.g. coded words) and additional mobile apps for secure communication.

EVALUATION DATA

An important part of the global pilot was that the participants agreed to participate in surveys as a mechanism for giving their feedback in the months following the workshops. The participants created the content of the surveys themselves in a participatory session during the workshops focused on monitoring and evaluation. The rationale behind asking the participants to develop their own surveys was that they would be more engaged in the process and therefore more likely to respond to the surveys when the time came. Accordingly, participants were asked to fill in periodic evaluation surveys to give us information about how the app was working for them.

There were three surveys conducted as part of the pilot taken at the beginning, middle and end of the testing period, in December 2014. Participant engagement in the surveys was not as high as we had hoped despite the efforts beforehand to ensure high levels of engagement. 39 people out of the original pilot group of 120 answered at least one of the surveys: 13 from the Uganda workshop, 19 from The Philippines, and 7 from the workshop held in El Salvador. Whenever we refer to feedback from the pilot participants in this report, we are referring to feedback of the 39 participants who responded to at least one of the three surveys.

A large reason for the relatively limited engagement with the surveys was likely because of the 'false alert' problem, which presented a serious technical hurdle for participants and was a barrier to ongoing use of the app. A number of survey respondents explicitly said that they had uninstalled the app because of false alerts. False alerts were also reported by almost a quarter of beta testers who downloaded the app on the Google playstore. The issue was related to the power button trigger interfering with the user's normal phone use and causing the alert to start sending when the user had not intended it to. This issue is referred to as the 'false alert' bug throughout this report and it was a major impediment to adoption and engagement during the pilot period.

EVALUATING THE APP

This section of the report documents the methodology employed during the design phase and the feedback received during the testing period: how user-friendly did the app prove to be, what were some of the main technical issues encountered by users and was the app useful in practise?

INVOLVING USERS IN THE APP DESIGN

From the beginning of the project, we were aware that involving HRDs in the design process would be key to ensuring that the app would work for its users. For this reason we engaged in a co-design process where we involved HRDs in making design decisions about the app. In November 2012, we ran a five day workshop in Nairobi, Kenya including 20 human rights activists from Kenya, Uganda, Nigeria, Pakistan and South Africa and a number of technologists and external experts, with the aim of testing our assumptions about what would make the app most useful for our intended users. We employed several design methods for user research, from a risk mapping exercise to a group brainstorming session, usability tests and surveys based on a prototype of the app.

> "The methodology adopted to pull out the issues and requirements was great and allowed for discussion amongst the group."
>
> *Fatima Bhyat, Association of Progressive Communications*
>
> "Participants discussed extensively, analysing how the present features on the app works. Lots of suggestions were made as to shaping how the app should evolve, the essential features needed to make the app simple to use and effective as well."
>
> *Bryan Nunez, (formerly) WITNESS*

A Panic Button design exercise takes place with human rights defenders in Kenya, Nov 2012

We took the information gathered in this research phase to inform the requirements for the beta version of Panic Button. Many of the experiences recounted to us by HRDs ended up directly informing design features of the app. For example, we learnt from a HRD working with the sex worker community in Uganda that frequent police raids meant she often had to hide her mobile phone inside her long skirt when on field visits. Her experiences helped us to come up with the idea for the power button trigger as this would be something she could reach for without having to bring her mobile phone into plain site of the police. This was then validated by our survey results and feature prioritization exercise where people placed ease and secrecy of activation as the biggest priority for the app, above

features that focused on transmitting evidence (such as video or sound recordings from the phone) and security of the communications (by encrypting the content of the alert messages and ensuring anonymity of the recipients). It was following this co-design week with activists that we were able to sum up the purpose of the panic button app simply as "a secret alarm for when you're in trouble".

Following on from the Nairobi workshop, we invited the participations to form a Panic Button Advisory Council to ensure that we continued to learn from and involve users in the design process. The Council acted as a sounding board for key design decisions. For example, we initiated discussion in an email thread about what would be the optimum number of trusted contacts to receive the alert. The group provided feedback on the merits of users being able to decide for themselves how many recipients to select versus the benefits of focusing on a small group of 'first-tier responders'. The consensus was that the latter was preferred; the rationale being that a small group of well-prepared recipients would be more effective at responding than a long list of recipients who may lack information and be poorly placed to exercise judgement in an emergency. This would also help to make the app secure-by-design in that it would restrict the number of people in a network who could be compromised should the app fall into the wrong hands.

The app design team decided to settle on 3 recipients, which directly fed into the creation of the PACT concept. We understood from our work with HRDs that the app would be of most value to an HRD encountering a situation of risk if it was the trigger to a pre-agreed and well defined security plan. The PACT concept therefore became integral to the design of the app and the information and guidance we provided throughout the app's interface.
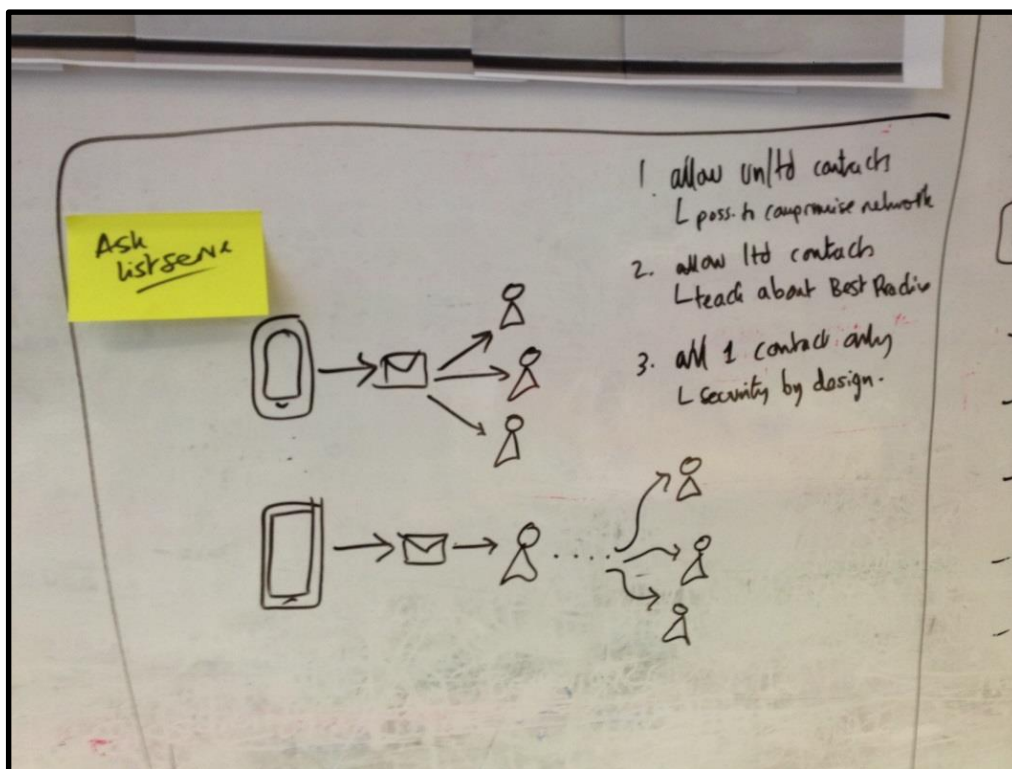
- *A sketch of the design options which we shared with the Panic Button advisory council listserve for input*

Striking the right balance between usability and security was always a concern. For instance, good practice in usability would usually be to provide as little "friction" as possible between the user and the interaction. However, given the security risks, it was important to us that we properly inform users about security risks associated with using Panic Button. This translated into designing a setup wizard which guides the user and informs them of important security assessments they need to consider when using the application, while doing so in as few steps as possible to reduce "friction".

Working with technology partners that were committed to use a user centric approach was key to the development of the application. First with Thoughtworks, then iilab, the development process involved making sure that the technologists were taking into account feedback from users and constantly aiming to improve the reliability, security and usability of the app.

Working with human rights defenders to understand their needs was integral to making well informed design decisions. Unfortunately, we did not manage to bring together the app's developers directly with the HRDs that would ultimately be users of the app. This was largely due to financial and time restraints but we suggest that, in future projects, facilitating such interactions would contribute to the mutual learning and understanding of all involved.

EVALUATING USABILITY

In all the workshops we ran we dedicated a session to setting-up the app. While the app has been designed to take only 5-10 minutes for a user to set-up, guided by a set-up wizard, we wanted to have adequate time to observe participants setting-up the app in order to be able to identify 'pain points' and get feedback about how to improve the instructions and user interactions.

This session was difficult to run, especially in large group sizes, given the varying levels of confidence and familiarity with Android handsets and the individual attention many participants required from the trainers. With the exception of the Philippines workshop, the majority of participants in the El Salvador and Uganda workshops had never before used an Android phone. The training team improved ther methodology after every workshop to ensure that participants felt as comfortable as possible learning a new mobile platform. In El Salvador and Uganda, we identified Android users from among the participants to facilitate small set-up groups with their peers who were less confident and familiar with Android phones.

The majority of participants who answered the feedback surveys expressed that they found it easy to understand how to set-up the app, and that they had no issues setting up Panic Button on their phones. However, before the beta release of the app in June 2014, there were numerous updates as we fixed bugs and incorporated user feedback from the workshops. This required users to uninstall old versions and download newer versions on their devices from a private distribution website. According to the survey responses, in general, updating Panic Button was not problematic, but some people mentioned they faced issues when trying to uninstall the oldest version of the app in order to install the updated version. Several users reported having problems installing new versions of the app because they did not have the correct link or the app was not loading on reinstallation. One user specifically said

this was the reason why she was no longer testing the app. Other users experienced problems reinstalling the app due to their very slow internet connection.

Managing new releases of the app was hard to manage without someone present to troubleshoot common user mistakes and identify bugs. In hindsight, it was probably overly ambitious to expect participants to regularly install new versions of the app. After the beta release in June 2014, there was no further public release until April 2015 and updates are now managed automatically through the Google Playstore which is a more user-friendly process.

TECHNICAL ISSUES AND FALSE ALERTS

As with any software product, we anticipated that Panic Button users would encounter technical bugs while piloting the app. During the development process, many of these bugs were identified and fixed by the team. The pilot workshops provided a further opportunity to test, identify and report bugs that were discovered by the participants. Frequently, these related to the compatibility of the app with certain device models or correlated with specific patterns of user behaviour that we were able to replicate and therefore fix in the code.

Unfortunately, a major technical bug was brought to AI's attention following the beta release on Google playstore in June 2014. This was the 'false alert' problem experienced by users whereby the app began to send alert messages without the user having deliberately activated the alert. For six months, our developers tried to establish patterns about what might be causing the false alert. However, without sufficientfinancial resources or access to hardware testing platforms, it was difficult for them to establish and resolve the cause of the false alerts quickly.

The false alert issue was reported in the survey results and was also reported by almost a quarter of beta testers who downloaded the app on the Google playstore. In the end, we began to encourage users who had experienced this problem to uninstall the app while we investigated the issue. This was also reported in the survey feedback from the pilot participants, many of whom uninstalled the app, which was a major limitation to their ongoing engagement and participation in the pilot. After putting more resources towards the resolution of the problem, the current version has significantly diminished the problem, emphasizing the importance of sustained technology support to address unforeseen issues and provide improvements long after a technology project is first launched.

Another technical issue mentioned in the survey feedback related to the phone's GPS location sometimes failing to be sent with the alert message. The location is provided by the GPS signal on the phone, by establishing connection with the mobile network directly or if there is weak signal, by triangulating with the nearest mobile phone towers in range. The GPS location, once detected by the app, is included in the SMS alert as a link to Google maps. Based on respondents' feedback, it seems that the Panic Button app sends the correct information in the majority of cases – including both the SMS customized 'help' message and the GPS link. However, on occasion users reported that the GPS link was missing from the message and in one case the entire message was delayed by a couple of days. Unfortunately, as these were isolated issues we were unable to pinpoint the precise explanation for why this happened but with advice from technical experts believe it may be an issue with local mobile network providers in the localities where it was reported.

> "To alert contacts panic button is useful but the GPS doesn't work in some areas so the accuracy to pinpoint your location maybe unreliable. As for the (Cherry Gem) smartphone, the battery doesn't last for a day, it is suggested to use other smartphone or always bring extra battery."
>
> - *Participant, Philippines*
>
> "I think it can be helpful as it will be able to approximate my location. However, we found some areas where gps signal is weak or there are no network or gps signal at all. Still, it can send SOS signal even without the map link".
>
> - *Participant, Philippines*

USING THE PANIC BUTTON APP IN PRACTISE

Participants reported that they have not made as much use of the app in real-life situations as envisioned. A number of the participants expressly stated that they had no cause to use the app as they had not faced a high risk situation during the pilot period. Furthermore, based on participants' feedback, the communication environment where some of the participants workpresented a number of barriers to adoption of the app. For example, in a couple of cases, HRDs reported that they had faced a threat but were unable to use the Panic Button because of lack of mobile signal. Another reason reported was due to a lack of time to activate the device, followed by the lack of credit on their phones.

The survey responses indicated some concerns from users about the financial costs of sending multiple alert messages when running the app (each alert is the normal price of an SMS message in each country). Equally, participants expressed concern that the app would be of limited use to others in their community because Android phones were prohibitively expensive.

There also seemed to be ongoing misunderstanding about whether the app also required the user to pay for Internet data. While Internet access does correlate with more accurate GPS from the network provider, this is not a requirement for the app. While this was explained in workshops and in the Help material on the Panic Button website, some of the feedback indicated misunderstandings about this, exacerbating concerns that the app was costly to run.

> "Limited range of app usage because of the cost of android smart phones for many HRDs."
>
> - *Participant, Tanzania*
>
> "It needs to be improved in a way that it can be useful even in remote areas where there are no signals."
>
> - *Participant, Philippines*

We knew from feedback during the design phase that developing Panic Button as an Android app would prevent challenges to adoption for many HRDs, especially those working in rural areas where mobile signal is often unreliable and few people are familiar with smartphones. We anticipated these challenges and aimed to mitigate some of the barriers to use by providing Android handsets and in-person training. However, ultimately the app proved to be more useful in urban environments and was mainly adopted and passed on by users in contexts where HRDs were already accustomed to using Android phones.

We learnt that a great part of the risky work done by HRDs who participated in the Panic Button pilot was in rural and isolated communities and that poor telecommunication infrastructure in these places represents a big challenge for their own security. The fact that it is precisely in these areas that the app has been least reliable and useful points to the need for more investment in Android alternatives for emergency communications for HRDs working in remote areas.

> "(Panic Button) will significantly speed up the process of alerting relevant people who are in the best position to come up with a quick response plan. However, my field works are done mostly in communities where mobile phone signals are weak & unstable."
>
> - *Participant, Philippines*
>
> "The application may not be user friendly to our communities in rural areas since they may not find the smart phone easy to use. And because the application usage is pegged with a fee, it will be quite challenging for some of our users."
>
> - *Participant, Tanzania*

.

A final challenge was related to language localization. At the time of the workshops the app had been translated into English, French and Spanish. After June 2014, volunteers also translated it into Portuguese and German. While all of the pilot participants spoke one of these languages they found this was a barrier when training others in their communities as the set-up advice, security tips and settings screens were not in local languages, such as Somali or Amharic. While the alert message could be customized by the user, the interface itself was only in a limited number of languages and this presented confusion for the users. The team is working now to scale the number of languages that the app is available in.

> "Language problem: cause of the app setting were in English so it was little difficult for one of them to get the process from the first time. They keep sending me a lot of message so we set other small training to fix this problem".
>
> - *Participant, Sudan*

Survey participants noted that the app could be particularly useful to support specific individuals in the communities where they were working. For example, one participant explained that she had not personally used the app for situations of high-risk but she was considering providing it as a protection tool for witnesses who testify in high-profile cases against the military in Guatemala and face the threat of reprisals as a result. Another mentioned that the tool would be relevant during the run-up to the elections in Uganda where attacks against democracy activists and journalists were anticipated to increase.

> "(It would be useful) to alert contacts of potential attacks we are monitoring, specifically when witnesses give testimony in hearings or in witness relocation following accusations of crimes of sexual violence during the internal armed conflict in Guatemala."
>
> *- Participant, Guatemala*
>
> "As we head to the 2016 elections back here in Uganda, the Panic Button will be a key tool to secure pro-democracy activists and journalists."
>
> *- Participant, Uganda*

Despite the clear challenges to adoption and use of the app, there remains a general consensus from participants that the functionality of the app can be useful for real-life situations. The participants considered the application to be a supporting mechanism to alert their colleagues and security networks if they face a situation of risk. This helps defenders and activists working on the ground to feel safer in harsh working environments. However, the participants also expressed an awareness of the limitation of the app given the range and scale of the threats they face and the poor infrastructure in remote areas that decrease phone and GPS signals. Despite this, respondents reported that the app is a tool that could support them in their work in order to be more prepared for risks and make them feel confident that their networks could respond rapidly should something happen to them.

> "In the dry run, a lawyer who was in my list called me up just few minutes after the button was triggered, my wife provided me with the map of my exact location. So this would be very helpful in real life. If only all HRDs in Basilan were equipped with the system, I could have responded to friends and relatives who just went missing many years ago."
>
> - *Participant, Philippines*

FUTURE DEVELOPMENT OF PANIC BUTTON

Based on the evaluation, we will to continue to invest in and improve the existing version of the Panic Button app for Android users. Our priority is to focus on making the core Android app and training methodology as high quality and accessible as possible. This involves making sure the app is stable and functions well a wide a range of Android devices and that it is available in more languages.

In addition, 20% of our teams' development capacity will focus on research and development, including feature improvements to the existing app and investigation into how a 'Panic system' could be developed for non-smartphone users. Advice from a range of technical experts we've consulted to date suggests that replicating Panic Button features while maintaining some security for non-smartphone users may be complex to implement as well as costly. This is something that requires further technical investigation. We are also exploring ways to circumvent some of the SMS connectivity problems experienced in rural areas. AI would welcome input from technical experts and programmers to assist in investigating some of the possible solutions.

EVALUATING THE PACT

This section of the report evaluate the aspects of the project that go beyond the application itself, particularly the PACT framework and the training methodology that was developed to assist HRDs in delivering trainings to others.

TRAINING ON THE PACT

An important part of the Panic Button pilot was that participants were introduced to the concept of having a personal PACT, a framework to help them to develop their security plans, individually and within their support networks. This was something that formed a core part of the discussion, learning and sharing during the Panic Button pilot workshops. Training on the PACT centred on a number of facilitated exercises.

To begin with, each participant was given space to reflect on their own risks and to visualize this in a map showing where and when they feel most vulnerable, identifying the 'panic' situations where they may require the app. The idea was to take discussion about security and risk to a granular level where they could reflect on their existing security practices, share past experiences of occasions when they have felt under threat and what they did to respond in those circumstances. This helped to ground use of the Panic Button App in a practical, lived experience of security where defenders could turn their attention away from placing security in the Panic Button App to considering security in their daily practices, networks and communities.
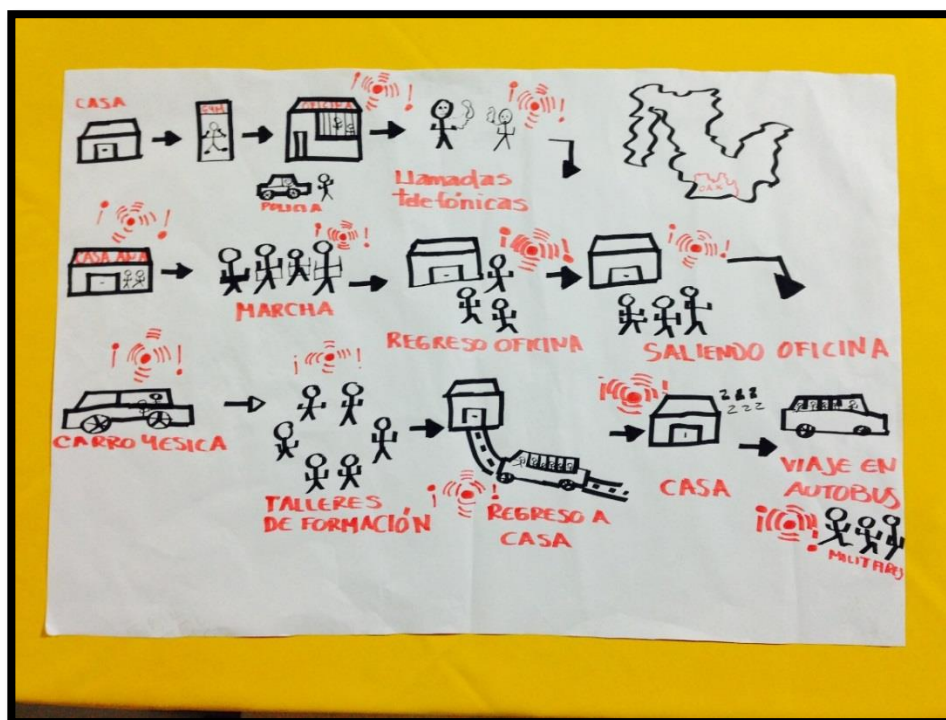
- *Example risk map created by a Woman HRD from Oaxaca, Mexico. Red vibration and exclamation marks reveal 'panic moments' in her daily routine.*

We used a mix of role-play and facilitated group discussion to help participants think through the most important elements of a strong PACT. Firstly, we asked what makes a suitable Panic Button contact. This brought up valuable debate about the difference between choosing personal/familial contacts and colleagues/institutional contacts. On the one hand a family member may know the HRD most intimately and be equipped to respond quickest. On the other hand, they may have a more emotional response and could face direct risk that they are not aware of and prepared for. Participants challenged one another to consider how reliable their chosen contacts would be in an emergency situation and to focus on preparation so that their chosen contacts would know what to expect and what would be expected of them in an emergency. We also discussed the importance of regularly updating the chosen contacts for different situations, so that there would always be someone close at hand to respond to a situation of potential risk.

Secondly, the group focused discussion on the response plan between an HRD and their three trusted contacts. It was important to think about this at a practical and not just theoretical level, and we did this through group discussion using hypothetical scenarios developed from the participants' risk maps. This included questions such as: once your contact receives an alert, should they try and find you? Would they be close enough to get there quickly? What risk would this pose to them? Should they contact the police? Would the police be an adversary or an ally? Who else might they want to contact, thinking about the media, local politicians, international NGOs and foreign diplomatic missions in the country? In every case, the groups arrived at the conclusion that there was no 'ideal' response plan as situations and circumstances can vary greatly. The conclusion of these discussions was that it was very important to develop flexible response plans outlining what action a contact should take, what information they need and who they should contact. Regularly 'checking in' and updating trusted contacts was also identified by the group as an important part of a strong PACT.

Thirdly, we asked participants to discuss what information their contacts would require in order to be prepared. It was recommended that each contact keep a folder with information that would be critical in an emergency. Personal details such as date of birth, national ID number and a photograph were considered key information to pass on to the authorities or to international NGOs and institutions. Participants also reflected on the value of keeping background information related to the HRD's work including a history of previous threats that would help provide key context, whether issuing a press statement, urgent appeal or lobbying relevant officials. Finally, each contact should have an agreed contact list through which to escalate the response.

In order to practice putting their PACTs into action, the Panic Button trainers created a game simulation of an emergency situation. Teams were composed of one person playing the role of an HRD at risk and three people playing the role of their trusted contacts. Each team had to work together to develop a PACT based on a series of character cards we gave them. A series of 'unlikely situations' then acted as unique triggers for the person playing the role of the HRD at risk who had to activate the Panic Button alert as discretely as possible. As soon as their 3 contacts received the alert each then had to complete a task and gather evidence related to their task. Each task required the responders to put into action the PACT they had previously created by getting information to/from specific game characters who were playing roles such as the 'prison warden', 'IT coordinator', 'coalition head', 'media' and 'EU mission representative'. The game was a fun way to get people to learn by practising. A debrief afterwards allowed the group to come together and reflect on what had worked and not worked in their team. The

groups then consolidated their learning into a Panic Button 'checklist' to ensure they were prepared to use the app in a real emergency.

We have since named this game 'imPACT' and have developed the instructions and game cards into a stand-alone training package that will be available on the Panic Button website. The hope is that this kind of interaction learning through Live Action Role Playing (LARP) will be of value in security planning discussions even outside the context of the Panic Button app.

The participative methods employed during the Panic Button workshops helped to ensure that participants left with a good understanding of the Panic Button App - but most importantly an awareness of the limitations of the app as a security tool when operating without the human response mechanisms to underpin it.

> Panic Button, in the days we have been testing it, has proven to be a potent tool. Always wary of its limitations, the workshop organizers have been quick to remind us that it can work for some situations and not others. Especially when our work requires constant visits to far flung areas where access to telecommunications are scarce, we cannot solely trust our security to an app. Of course, with suggestions and inputs from testers, I can say that the possibilities for the Panic Button to be useful to HRDs in the Philippines are huge.
>
> *- Participant blog post, written during the Philippines workshop in February 2012*

EVALUATING THE PACT

Overall, the positive feedback of the participants on the PACT framework affirms that the greatest value of the Panic Button project lies in the real-world relationships between HRDs and their trusted contacts, and the ways that these can be strengthened for emergency response when an HRD faces a situation of risk. In this way, the Panic Button framework represents a technology-based strategy for planning, mitigation and response to physical attacks on HRDs and not simply a mobile alert tool. As one participant put it, "Security is community. Having a PACT gives you a sense of security."

According to the participants, creating a PACT has made themselves, and those around them, more aware of security concerns, frequently monitoring each other's security, improving communication and enhancing current security protocols. Having a PACT increases their confidence, gives them a sense of security and helps to bring peace of mind to those working in potentially dangerous environments.

> "The way in which it helped me most was in the initial phase of building a strategy and defining the actions and contacts in case of an emergency. This was further strengthened the habit of updating the alert and always keeping battery and credit on the phone."
>
> *- Participant, El Salvador*
>
> "Security is community. Having a PACT gives you a sense of security."
>
> *- Participant, Philippines*
>
> "It has served as a guarantee that if at any time something happens to me there will be companions who will know what they can do in that situation of risk."
>
> *- Participant, Mexico*
>
> "Somehow the panic button application provides me an assurance that I will be directly connected or be traced by my PACT whenever I am in danger at work."
>
> *- Participant, Philippines*

All of the respondents who answered the final survey (23 in total) said that the Panic Button has impacted/influenced the improvement of "security best practices" within their work and their organizations. A participant from the HRDs Network in Uganda commented that "Panic Button reinforced the already existing individual and organizational security mechanisms" and that the PACT "has formed a big part of our security management trainings. In Honduras, a women human rights defenders network reported that it has integrated the PACT into security protocols at the national level.

> "While I wasn't able to use it in an emergency situation, it provided me and my organization a framework on digital security and inputs on enhancing security protocols."
>
> *- Participant, Philippines*
>
> Once you have established a PACT, it's not the technical tool but the PACT that is most valuable".
>
> *- Participant, Honduras*

Respondents to the survey stated that throughout this project they have valued being able to share experiences of security with one another and learn from other HRDs in their region. For instance, they have become more aware that they all share similar security concerns, and that it is important to keep good communications across their networks in order to learn from one another's security and safety practices. They reported that while sometimes they (and their colleagues) do not feel emotionally prepared to face a risky situation, the Panic Button, and more specifically the PACT, reminds them about the value of their networks and how to build trust and resilience in these networks when it comes to security.

> "It is more powerful to share experiences with others, because we learn from each other security plans and get the chance to develop our own plans."
>
> Their interest with the app showed their equal concern for their own safety (…) At least I found out I'm not the only one concerned about that."

HRDs who participated in the Panic Button workshops reported that it was useful not only to learn about Panic Button, but also to get to know other tools and strategies for security. Participants valued the information provided by the trainers that related to safer digital communication, data encryption, networking and the creation of a PACT as part of their security strategies. Numerous participants reported that mapping out the risks they face visually was a helpful exercise.

> "I see that technology has a huge link to human rights and that link is sustainable. We have seen after the Edward Snowden case many Journalists take crash courses in technology and security so I see it's a vital and necessary linkage. Therefore in days to come this linkage needs to be harnessed and popularised."
>
> *- Participant, Uganda*
>
> "Now I know that I can use technology in so many other ways as a defender apart from advocacy or capacity building, it's now a security tool as well."
>
> *- Participant, Tanzania*
>
> "Learning how the tool worked the tool and its usefulness alongside other strategies that should accompany it has helped me to position myself differently in my work and daily life."
>
> *- Participant, El Salvador*
>
> "It has been an incentive to learn more about technology and apply it in performing my role as a defender."
>
> *- Participant, Guatemala*

SUPPORTING PARTICIPANTS BECOME TRAINERS

Two of the Panic Button pilot workshops followed a training of trainers (ToT) model – with the aim for participants to train others in their networks and thus help the app reach others working in their communities. As part of the Panic Button pilot workshops, participants were asked to practice leading a short session for other participants in the group. This allowed us to give feedback on the training methodologies each individual participant proposed. In El Salvador, this was an incredibly effective model with participants adapting and building upon many of our participatory methodologies to develop their own versions of the training.

At least ten additional trainings of Panic Button have been conducted by participants since May 2014, some of these in more formal training settings than others. Other participants reported helping set-up their colleagues with

the app one-on-one or in small groups. The East and Horn of Africa HRDs (EAHRDP) project trained HRDs in the region of East and Horn of Africa on security management and digital security, and included a new training component on Panic Button and the PACT framework. They reported that after the trainings, participants mentioned in their evaluations that the app is very useful for HRDs' security, especially those who work in hostile environments such as Sudan and Somalia or those who work on issues such as LGBTI and women rights.

Where participants reported that they attempted to run Panic Button workshops in contexts with limited access to smartphones, they still found that the concept of the PACT was useful and helped to develop peer-to-peer security measures that instilled a sense of mutual protection and support between those they trained.

Some participants emphasized that manuals, or some sort of short tutorial handbooks, would have been helpful for those delivering Panic Button workshops. Some also mentioned that short videos (in numerous languages) showing how to install the Panic Button application would be useful.

> "We worked directly with women defenders who are at risk in specific areas over the course of 5-6 hours. Until now no one has been in a situation of such risk that they've had cause to use the app. But the personal PACT has been useful to them as a form of relief because it guarantees that their contacts will know if something happens to them. "
>
> - *Participant, Guatemala*
>
> "As a trainer, I have been using some training methodologies and skills which I acquired during the workshop, the HRDs map of risks from Latin America"
>
> - *Participant, Uganda*

CONCLUSION

The Panic Button project has always been about more than developing a smartphone application. The larger goal from the outset has been to build a methodology, or framework, that could become an integral component of security protocols and practices for HRDs, based in, and supporting local response mechanisms and resources. This pilot phase has allowed AI to test assumptions and develop a framework that's responsive to the needs of HRDs.

The feedback from the pilot participants is that Panic Button has helped them to develop an understanding of the possible benefits of using and interacting with technology for their security. For many of the participants the link between technology, security and human rights work was previously a foreign concept reserved for those with a technology skillset or background. The Panic Button framework has helped HRDs to acknowledge the importance of technology and to take ownership in the development of technologies that can support

> "(The project) was helpful to reflect on the need to establish trust and support networks for mutual protection between defenders. It generated reflection on the need to improve communication mechanisms."
>
> - *Participant, El Salvador*
>
> "To establish allies within one's family as part of the pact has been an interesting topic because often we attempt to remove our family from the risk we face thinking that not involving them will be more secure, however we must consider a strategy starting also within (the family)"
>
> - *Participant, Guatemala*

their own security and protection.

At the same time, during the pilot phase the participants experienced the limitations of Panic Button as a mobile tool, expressing concern and sometimes frustration, at the technical and environmental barriers. In some cases, the stability and performance of the beta app made it an unreliable tool, triggering 'false alerts' between a HRD and their network. In other cases, even when the app worked as expected, weak mobile phone signal in isolated or rural areas limited its value to HRDs. However, despite these recognized challenges during the pilot phase, HRDs who participated in the pilot still expressed that overall, the Panic Button app was a useful tool and repeatedly made the case for a non-smartphone version that would be more easily integrated into their communities. Equally, in urban environments and in communities accustomed to using smartphones, the app seemed to work well with fewer challenges reported by the participants.

Participants also inherently recognized the pitfalls of placing trust for their security in a mobile phone app. As a participant in the Philippines put it, "a reminder for all of us using mobile phones for advocacy: 'Security is a people problem'. Even with the Panic Button, we should always keep this in mind." For this reason, the PACT was especially well-valued among the participants, who reported that it made them more aware of security concerns, frequently monitoring each other's security, improving communication and enhancing existing security practices. In this way, the Panic Button framework has enabled a space for reflection and analysis on the importance of creating and strengthening trust and support networks for mutual protection between HRDs and their close contacts.

Ultimately, the initial phase of Panic Button has contributed to increased capacity amongst the participants in relation to using technology within their security protocols, but also as a technology-based approach to improving security planning and communication within their networks.

The next phase will aim to resolve some key barriers to the use of the Panic Button app, localize the Panic Button app and framework so it can be accessible to more HRDs in different languages, and reach out to support dozens more HRD networks integrate the Panic Button framework into their security protocols and daily practices.

"The Panic Button is a fundamental strategy for alerting but also for devising a security plan and articulating this with our contacts so that the plan is strategic and coordinated…The workshop has forced us to sit down and work out what would we do and how to be able to guarantee a greater level of security for women human rights defenders."

- Human rights defender, Mexico