UNDERSTANDING INTERNET *FREEDOM:*

UGANDA'S
LGBT HUMAN RIGHTS
DEFENDERS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In February 2016, a team from SecondMuse spent time with a group of 14 LGBT human rights defenders as part of a Needfinding engagement in Kampala, Uganda. Prior to landing in Kampala, the team conducted background research and interviews. In Kampala, the team made site visits with two organizations and facilitated a two-day in-person Needfinding session. After the session, SecondMuse led a debrief and learning session with three local organizations who participated in the Needfinding exercise and sought to use these techniques in their own work.

The goals of the engagement were first to understand how the LGBT community in Uganda is communicating, their perceptions of the threats they face while communicating, and the tools and strategies they have developed and employ in order to live a safer, freer existence. Additionally, SecondMuse sought to support and build local capacity to employ Needfinding in the research, advocacy, training and tool development processes already taking place there.

The following report offers insight and provides the context for living as LGBT and/or working to support the LGBT community in Uganda and how this impacts communication, especially regarding privacy and security. This report also gives background on the Needfinding process and offers key learnings and insights from LGBT Human Rights Defenders in Uganda. The intent of the report is to build upon the work already taking place in Uganda, and provide developers, trainers and policymakers with a foundation on which to create interventions targeting this community.

INTRODUCTION

Uganda is a difficult place to be LGBT. Uganda is currently included in an Amnesty International list of 76 countries where homosexuality is considered criminal. While homosexuality is certainly not new in the history of Ugandan culture, the extent to which members of this community are actively persecuted in contemporary Uganda is an atrocity. In colonial times laws that banned homosexual acts existed, but they were rarely enforced. The current situation, however, where sexual minorities and LGBT people are often denied their human rights is a more recent development.

This change has been attributed in part to the arrival of western evangelical anti-gay rhetoric; most notably from Scott Lively who is currently being charged with crimes against humanity in Massachusetts.[1] The status of sexual minorities in Uganda was taken to another, more precarious position with the introduction of the Anti-homosexuality Act in February 2014. The short-lived act gave the state the power to persecute sexual minorities in Uganda for simply living their lives. The legislation decreed that Ugandans found guilty of homosexual acts were punishable by life in prison.

Where Homosexuality is Criminalized
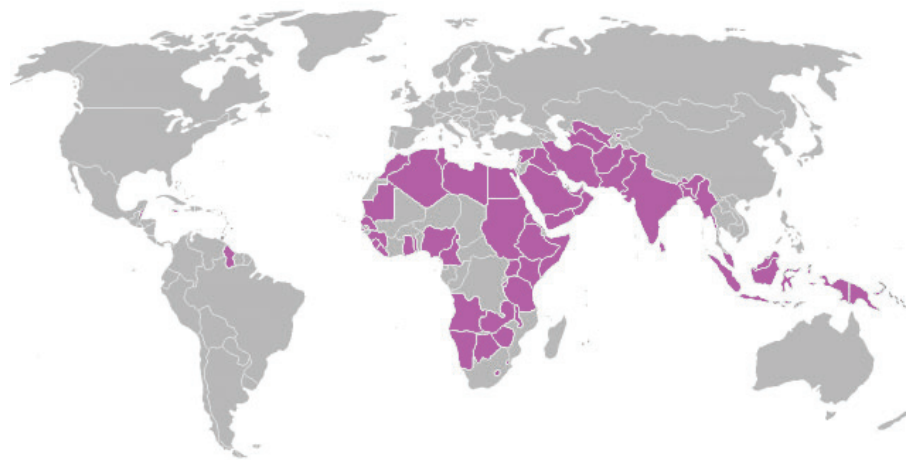
Uganda is one of 76 countries where homosexuality is criminalized. Countries with laws against homosexuality are purple on the map.

Source: 76crimes.com

Activists and human rights defenders mobilized to get the act overturned by Uganda's Constitutional Court less than a year after its enactment, but the fallout, social stigma, and ongoing human rights abuses against the Ugandan LGBT community continue to make Uganda a precarious place to be considered LGBT.

The way in which the LGBT community in Uganda uses the Internet and other communication channels has not been studied sufficiently. This report seeks to provide preliminary understanding and fodder for subsequent inquiry into the threats to and behaviors of the Ugandan LGBT community regarding internet freedom tools (IFTs).

---

1 More information on the timeline of the case can be found here: http://ccrjustice.org/home/what-we-do/our-cases/sexual-minorities-uganda-v-scott-lively

DAILY THREATS

Those in the LGBT community in Uganda face threats to their well-being on a daily basis. These threats come from within the community, from family and friends who are homophobic, and to a lesser extent from the state — by whom they are marginalized and from whom they remain unprotected. Typical threats range from the physical – such as torture, arrest, and "corrective" rape – to the emotional and psychosocial, including blackmail, termination of employment, eviction from home, loss of opportunity and even family banishment.

Those threatened are often left with little recourse because the state has failed to acknowledge and investigate attacks on or threats to LGBT people in Uganda (SMUG, 2016). Through the Needfinding exercise with LGBT activists and human rights defenders, it was evident that many of the threats require not just technological solutions but physical protection as well. Throughout this report, the concerns and strategies regarding physical safety are covered as they inform decision-making and therefore have an impact on the communication safety of the LGBT community in Uganda.

STATE OF CONNECTIVITY

In order to understand the insights and findings shared throughout this document, it is important to understand the broader context of connected life – and especially use of Internet and communication technology – in Uganda. By far the most common method of communicating is by voice, using mobile devices. In the *State of Internet Freedom in East Africa* report,[2] 77% of respondents said phone calls were the most common way in which they communicated; participants in the Needfinding engagement confirmed this finding. The second most common way of communicating is via SMS with 69% reportedly using this method. Of those surveyed in the 2015 CIPESA report, only 10% were familiar with Internet Freedom Tools and those that were tended to be academics or highly technical.

According to the State of Internet Freedom in East Africa 2015 report, the internet penetration rate in Uganda is around 20%, which is significantly lower than the reported 69% penetration rate found in neighboring Kenya. There are a number of factors that impact Ugandans' use of the internet, but speed, access and cost are the most commonly cited barriers:

- In terms of speed, World Bank data shows that of the internet-connected population, only 2% have access to broadband or speeds higher than 4 Mbps.

- In terms of access, electricity penetration rates were cited at 20% of the population in 2012 according to World Bank data, which has clear implications for internet use.

- When it comes to cost, internet is becoming more accessible with the introduction of bundles from telcos and free mobile access to commonly used platforms

such as Facebook or Twitter, but on its own, internet costs are still prohibitively expensive for a significant portion of the population. Monthly unlimited internet fees outside of a bundle can be as much as $100 USD per month - far out of reach for most in a country where the GDP per capita hovers around $700 USD per year.

All this contributes to the fact that an analog mobile phone remains the primary mode Ugandans use to communicate with each other. This is unlikely to change in the near future.

Many of the participants in the Needfinding exercise reported having two mobile devices with two different service providers: a smartphone for web access used only when absolutely needed and an analog phone for the majority of their everyday communication. Having multiple devices enables the price-conscious user to tap into 'deals' from different providers. Many participants, human rights activists and organizers acknowledged that their level of connectivity was not representative of the populations they served or those located outside of urban settings.

This illustrates an important point for trainers and developers alike: the current situation of communication in Uganda is predominantly through non-internet connected mobile platforms. While internet access is predicted to reach a significant portion of the population in the future; this is not the current reality and designing interventions for a future reality means many of the most vulnerable will not be served or helped by web-based solutions and tools.

---

2 This report was completed in 2015 by CIPESA with support from in-country researchers as well as Open Technology Fund (OTF) and Humanist Institution for Co-Operation with Developing Countries (Hivos).

UGANDA'S LGBT COMMUNITY

Throughout the report, the terms LGBT community and sexual minorities are used interchangeably based on feedback from Needfinding participants and reports from activist groups serving this community such as Sexual Minorities Uganda (SMUG) and i Freedom Uganda Network (iFreedom). The community is composed of people who identify as LGBT, allies to this community, and those who are identified externally as LGBT or part of what some in society view as an 'umbrella of immorality.'

The LGBT community is often classified alongside sex workers, but participants in the Needfinding engagement shared that while the two groups do have overlapping members and some shared challenges, they remain distinct in many ways. The most striking distinction is that unlike sex workers, the LGBT community in Uganda still remains in the shadows due to the risk of persecution not just from the state but from widespread homophobia throughout society.

Activist groups are often unregistered or shield their work under a more generic categorization such as human rights. Names and true identities of LGBT individuals are often changed and fluid depending on the level of safety in a particular place or situation. There is a constant threat of being 'outed' or identified as LGBT without having chosen to do so themselves, and a risk of physical attack, disownment and other forms of harassment. Finally, according to participants in the Needfinding, sex workers are less precariously positioned in that they have gained more political power and have organized as a labor group, whereas LGBT remains a persecuted identity.

Tool and program design activities targeting the LGBT community in Uganda are influenced by the cultural, social and technical realities the population faces. Considering this, solutions should take into account two main factors: the
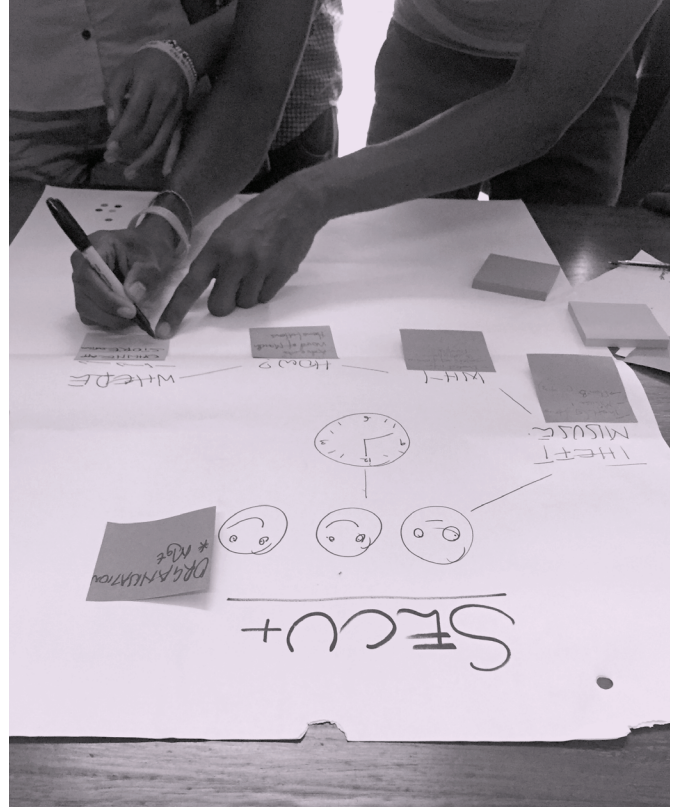
public identity or the level of openness or identification as LGBT, and the technology available.

Participants in the Needfinding talked about the tradeoffs in identifying and living as LGBT. Some participants used a very public persona in order to protect themselves – if something happens, it would have to happen in the public eye – even though that openness typically has painful consequences, including strained relationships with family and limited work opportunities, to name but two. Others remain highly undercover and therefore must navigate a complex path of multiple identities and develop a sophisticated ability to discern where and when to use which identity.

These are two examples on a spectrum with many falling somewhere between, but the common thread is a sense of fear: fear of the unknown, fear of attack, fear of being excluded and violated without recourse. This fear leads individuals and the broader LGBT community to constantly evaluate and vet who and what can be trusted. The following pages seek to shed some light on a population that is under attack, in order to pave the way to more resources for safe, free and fearless communications in the future.

THE NEEDFINDING PROCESS

The Needfinding process by SecondMuse draws on elements of human-centered design, an approach requiring deep understanding of the needs and challenges people face in their everyday environments. This understanding is then used to inform the design of solutions addressing those challenges. SecondMuse's Internet Freedom Needfinding Framework (internetfreedom. secondmuse.com/needfinding) provides a process for building understanding during Internet Freedom tool development through structured engagement with communities around their security-related challenges and behaviors. This Framework is an open process available to anyone interested in better understanding user communities. It continues to be developed iteratively, incorporating new knowledge following each application. To date, SecondMuse has completed Needfinding engagements with the Tibetan exile community, Vietnamese digital activists, Tunisian journalists and now LGBT human rights defenders in Uganda.

DEVELOPING A RESEARCH PLAN

The first step of Needfinding is to establish the research goals, identify specific questions, and design the exercises to gather information. **The following goals guided the Needfinding with the LGBT community in Kampala, Uganda:**

To understand personal experiences, behaviors, motivations, and priorities as it relates to communication and use of those tools.

To understand the perceptions of security and privacy.

To further explore and improve human-centered design practices/approaches to uncover needs and their application to the development and training processes such as:

- Understand what tools and frameworks developers can utilize to better know the needs of users;

- Understand what intermediary organizations can do to better know the needs of users in order to design more effective engagements (training sessions, campaigns, materials);

To be able to speak to, document, and share user experience with Internet Freedom Tools and general communication tools more broadly.

Identify key needs that users have in Kampala, which can lead to better tools for this population.

Following is a list of key questions[3] we sought to answer in order to achieve our research goals:

1. How is the LGBT community identified in Uganda and how do members self identify?

2. What is "meaningful" communication? What are common communication patterns and priorities among Kampala's LGBT community?

   - What are the priorities for an individual when they are communicating?

   - What are the most common use cases of communication technology in which security/privacy may be a concern?

   - How do individuals define privacy and security?

   - What are the unmet needs/desires people have for communication in their daily lives?

   - What are the biggest threats? Who are they directed at? What impact do they have on security and communication choices?

   - How are alter egos used when online vs offline?

3. Do individuals utilize Internet Freedom tools? Why or why not? If they do, which ones?

4. What are the security-related behaviors that individuals employ in their daily communication activities? How are these reflected (or not reflected) in the technology they choose to use?

5. What are the things a user considers when making a security-related decision online (even if they do not realize they are making a security-related decision)?

6. What are the most relevant pieces of information that would help a developer build a tool more effectively for the LGBT community in Kampala?

---

3 Participants were not asked these questions directly, but they informed discussions, the visual exercises and the set up of the role play (see appendix for more info).

BACKGROUND RESEARCH AND INTERVIEWS

Prior to fieldwork in Kampala, the research team spent time understanding the challenges and realities of being LGBT in Uganda. We conducted secondary research through reviewing blogs, articles, publications, reports and other reference material to understand the history, cultural and social context, and current events in Uganda. We had background interviews to develop understanding which contributed to the design of the activities, exercises and interview questions for the field engagement. Interview subjects included scholars, human rights organizations, and members of LGBT community in Uganda. The i Freedom Network of Uganda, the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and Defend Defenders provided context for and feedback on design of the Needfinding with LGBT people in Uganda. In parallel, we also conducted interviews with developers to get a sense of their needs in order to better design tools for communities in East Africa. Our on-the-ground partner, CIPESA, worked closely with us to design the engagement and to recruit and vet participants.

NEEDFINDING TOOLS AND TECHNIQUES

During the two-day, on-the-ground engagement, SecondMuse used several types of activities to gain understanding. Facilitating the expression of insights about underlying motivations is an integral part of this process, simply asking direct questions on security threats and software features is often not the best way to learn. The SecondMuse team employed a range of techniques including observation, interaction and discussion. This approach allows participants to express insights in multiple ways, mediums and environments — meeting them where they

are most comfortable. The exercises rely on distinct ways of communicating information from drawing and role plays to creative design exercises — all of which helped answer initial research questions. The combination of these types of techniques allows for more authentic storytelling because they are in the activists' own words and shared in a way that reflects how and when that information is important to them. Needfinding reinforces that the participants are the authorities on their own lives and decision-making processes.

PARTICIPANT DEMOGRAPHICS

Thanks to CIPESA, 9 organizations and 14 individuals participated in the Needfinding engagement. Participants and their organizations reflected a wide variety of services and support needed by LGBT Ugandans, from advocacy to legal to health to general social and community navigational assistance. The group was a mix of self-identified members of the LGBT community and allies or representatives from organizations serving them. Many became human rights defenders based on their own personal experiences living as LGBT and facing the various challenges and threats prevalent in Uganda. Others felt compelled to stand up for the rights of others based on their perceived need for a more fair and just Uganda as a whole. Out of the total number of participants, only a few had participated in a formal digital security training previously. Although the participants all now live in and around Kampala, the vast majority of participants grew up outside of the capital and eventually moved there for studies or were looking for a better life.

BUILDING AN UNDERSTANDING

In the following section, we will outline foundational insights to inform the development of IFTs (Internet Freedom Tools), digital security training, and policy development as they relate to Internet Freedom and the LGBT population of Uganda. These insights emerged from from interviews with human rights activists from or working in Uganda, secondary research including the Open Net Africa Report and a multi-day in-the-field engagement with various members of the LGBT Human Rights Defender community. The following are key learnings from this targeted Needfinding engagement.

SECURITY & PRIVACY BEHAVIORS

If security is about minimizing risk and fear, it is not possible in Uganda.

In order to better design, develop and position tools and training, it is paramount to understand the various ways people view and define the concepts of security and privacy and how they apply these concepts to their everyday reality. Understanding how potential users and trainers of IFTs view these concepts will help ensure that what is designed and what people are asked to learn is in alignment with their own habits and behaviors.

"Security means being able to live your life free from fear and harm."

- Staff Member of LGBT Human Rights Organization

Participants shared the understanding that security isn't an isolated concept and that no matter how much of a security plan an individual may have, security in the LGBT community is inherently tied to and affected by others in the community. Although security "begins with you," there is a need to continually assess and vet the relationships you have in your life or the situation you enter into in order to be secure. Someone who was once trusted, perhaps a former lover, can become a threat to your own security by using knowledge of your identity to harass and exploit you.

As such, there is constant recalibration about personal – and in some cases the broader community's – security that are dependent on whether someone is or is not knowledgeable that you identify with or are an ally to the LGBT community. Ultimately, the LGBT individual's sense of security is all about their relationships, and relationships are central to the concept of security in the LGBT community.

Navigating the world as LGBT means reliance on your gut.

For many participants of the Needfinding engagement, the concept that "security begins with you" influences what platforms and tools they use, the number of accounts they have and what information they share and with whom they share it.
As one participant succinctly put it, security is also about being able to "put distance between yourself and risks." We heard from many participants that they navigate the world based on their 'gut,' which assumes everyone understands the risks that are present in order to put that space or distance between risk and self.

In the physical world, participants talked about how they present themselves to the world in terms of clothing and gender as a conscious decision which is made with security in mind. They also talked about trusted friend and social networks which might be a close group of friends or colleagues who you check in with or check in with you on a regular basis to ensure you are safe. Participants shared how they live in constant threat of attack (both explicit and implicit), which informs the places they choose to spend time and live, awareness of who they spend time with and the way they physically engage with and present to the world.

These choices are often influenced by financial means and therefore those with limited resources often aren't able to 'afford' safety and are forced to live, work and transit precariously.

Multiple accounts and curated groups assure some sense of safety.

The use of multiple email and Facebook accounts was a common tactic, because it allows people to segment their identity, activities and relationships. The segmentation was particularly helpful when it comes to "nosey" family members, neighbors, church members and landlords who may not approve of homosexuality. One participant likened it to living a "divided self" with a separate phone, laptop, email address and Facebook account for those who knew about their identity and those who didn't. If their partner used their phone, they would immediately change the password, because "blackmail is real in the community" and those who were once trusted can use your personal information as a form of attack.

"[Use of multiple accounts for email and Facebook] because of safety. They say security begins with you. I don't want to compromise the community; in terms of sharing issues outside the community [its] separate for those out and not out. I think it's a good practice to separate yourself from LGBT in times of engagement and your work, etc. I was using email for both communities and realized I was sending out info that I just wanted to go to rugby and so I realized I needed to separate out. I have whatsapp group for LGBT work and for rugby."

– Director of LGBT Human Rights Organization

"On your phone don't put an email app just open on the browser so if something happens to your phone they won't' have your email."

– Staff Member of LGBT Human Rights Organization

## *Verification practices are time intensive, but necessary.*

For those running organizations and managing communities where each person has a different level of comfort and desire to be public about their sexual orientation, the way groups are created and monitored is extremely important. Because some people have multiple Facebook accounts, Facebook's 'people you may know' feature has caused problems for some. One participant shared how their false profile where they openly identified as LGBT was suggested to a friend from church who did not know about their homosexual identity.

Verification of members of a group on Facebook or in Whatsapp is complex and even more important because people are careful about what is shared with whom. Just because someone who is asking to join the group knows members that are already in the group doesn't assure they are a safe or welcome member. Current approaches to verify identity and understand the intentions of individuals trying to enter groups is both time consuming and highly subjective. It is difficult to tell who is a "mole" because "not everyone who hits on you is interested in you." Organizations that have had multiple administrators to accounts, groups and pages face a daunting challenge of checking and double checking who was added when and by whom. The safety of the entire group depends on it.

One participant shared how they used to let everyone into an online group they manage, but quickly learned they needed a more robust, considered approach:

> **"We have a strict policy of who is in our group [now]. [Previously] someone that was part of the group that may have been added by a previous admin...this person was added and was homophobic and they would go and look for dirty and degrading videos and put them in the group. If you are in the real group you won't do that. Attention was focused on this person and why would they do the negative if they are LGBT – they are putting anything that is bashing and putting it in the worst light. So I wondered who added them because initially all members could add people. So I had to go back to the drawing board and check everyone, checking their mutual friends even to see if they are really a part of the community and now we see who is in in a strict way."**

> – Staff Member of LGBT Human Rights Organization
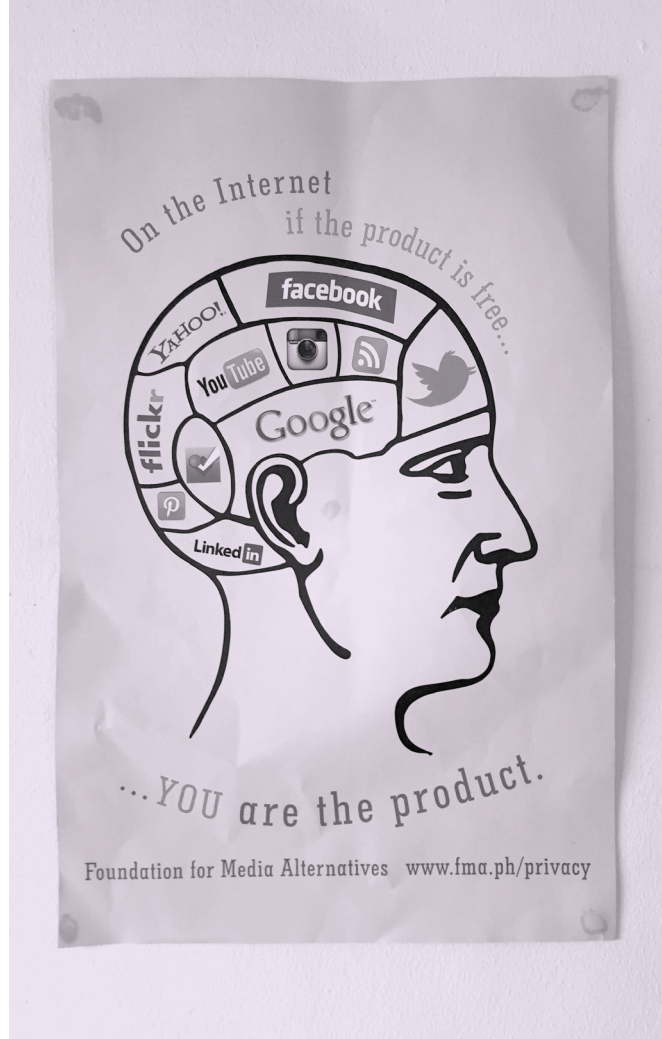
Physical, digital & psychosocial security are always connected.

In the LGBT community, being safe and secure isn't just about the strength of your password (though some people are very aware of the need for strong, frequently changed passwords). Digital, physical and psychosocial aspects of security are all interconnected in the LGBT community. The conversations around security and threats seamlessly went from what type of protection in terms of fences, physical access into work premises and alarm systems your office has, to being mindful of where a boda boda[4] drops you, to passwords on laptops and phones.

> **"Security isn't just about physical. It starts with personal security and you have to protect yourself. Time and again you talk to people and educate them that it's not just about protecting laptops but you can be reported for what you said. Someone would talk to you and get things from you. We teach that personal security starts with you. Be cautious about everything around you. We aren't teaching people to fear, but be responsible."**
>
> – Uganda-based Digital Security Trainer

Although there is an understanding of the connection between the three main aspects of security, that doesn't mean that people have the same level of knowledge, agency or understanding of how to protect themselves and others equally nor how each area relates to the other. We heard from some trainers in the region that they take cues from how their trainees talk about physical threats to know when, where and how to approach digital security topics.

---

4 Boda bodas are motorcycle taxis commonly found in Uganda and are for the most part unregistered.

Everyone has a security plan whether they are conscious about it or not.

The ability to navigate and assess potentially dangerous or compromising situations is a constant for LGBT people in Uganda; sometimes this happens consciously and at other times unconsciously. One person called this internal approach to staying safe a "security plan." As shared earlier these personal security plans encompass physical, digital and psychosocial assessment and tactics. The plan has to be flexible enough that it can be adapted and implemented on a daily basis. It informs everything from which boda boda to take, to where to be dropped-off, to what bar to hang out in.

More often than not, understanding what to watch out for and how to be safe comes from the people with whom you spend the most time. One participant shared that they learned about security based on being around their boss who is someone that is, according to them, "highly security conscious." Over time, the participant said, they can't help but become more aware themselves of their own safety and relevant precautions. As personal "security plans" are being developed, there is the recognition of trade offs – for example, the level of sensitivity needed versus urgency; getting someone the information in a way that works for them but is less secure versus trying to get them to change their behavior in order to communicate; and using technology that is already widely adopted versus what is specific yet appropriate for a particular audience.

These tradeoffs are constantly being navigated throughout people's daily routine. Given the constant threats faced by LGBT people in Uganda, security is sometimes compromised in order to protect or respond to a community member in need or in danger. This tradeoff may address an immediate need but can have negative consequences for personal safety in the future.

THREATS FROM EVERY ANGLE

From the individual to the state, threats are varied but always present.

Threats vary depending on who you work with, what you are doing both personally and professionally, how "out" you are, who you mix with, and a whole host of other factors. There are two main categories of threat that influence each other:

1. Community-based threats (coming from those around you) and

2. State-based threats.

"The umbrella of immorality" – a term used to group LGBT community and sex workers together – sets the context for many threats experienced from the community. The state is considered hostile to this community as evidenced by the Anti-Pornography act which it uses to target LGBT groups and activities; and the Anti-Homosexuality act, which was ruled unconstitutional less than a year after it was enacted. These acts demonstrate how the state has failed to recognize and protect the human rights of LGBT individuals and organizations and is actively antagonistic towards this community. The failure to protect or investigate abuses against this population means that LGBT individuals not only suffer attacks but have no recourse or means to pursue justice once victimized.

At least as concerning as the parlous relationship between the state of Uganda and LGBT communities is the fear that someone who is or was close to you will use your information to attack you. Participants talked about homophobia among friends, family, employers, colleagues, neighbors and landlords. Participants talked about people from their daily lives as posing the biggest threats to their safety. As one participant shared, this is compounded by the "fear of the unknown" – never quite knowing who is safe and when or if someone is going to turn on you. Participants said one can easily identify a sex worker, but this is not the case for LGBT people. The former is a group united by profession and the latter is being marginalized for who they are.

For human rights defenders of the LGBT community and in particular for those that identify as LGBT themselves, physical and psychosocial threats are top of mind, while digital security is secondary. As one digital security trainer in Uganda explained: "In the case an office is broken into, the computer will be stolen and then info is leaked. We help them understand that and introduce the digital security complement to that. So to have digital security you have to have physical security first." Given the breadth of the physical threat to LGBT, the approach is first to focus on the physical and then move into the digital realm.

This connection between different aspects of security influences not only individual choices, but also how people make decisions about helping others. In some respects, physical threats trump digital. If someone is in immediate need (e.g. they are missing or there is a perceived threat of a police raid at the office), getting to people and ensuring their safety is the number one priority, before thinking about securing phones and computers and other documentation. As a result there is a deeper understanding of and reliance on having physical security systems like alarms, fences, signature gate bell rings and knocks.[5] The level of thoughtfulness that is given to precautions against physical harm isn't matched with digital behaviors.

---

5 One participant shared how the office where they work has distinct knocks and ways of ringing the bell for each staff member. That way, when they hear an unfamiliar knock, they take extra precautions before letting the person enter the compound.

Operating from the shadows means greater danger.

Threats are heightened and more difficult to deal with when you aren't recognized by the government or police as individuals or organizations. Activists and LGBT community members are often "invisible" in Ugandan society when it comes to the rights and protections guaranteed to others. It becomes virtually impossible to turn to traditional institutions such as the police or the court system for help when your office has been broken into or someone takes files and other important information.

One of the role play scenarios[6] written during the Needfinding engagement was an LGBT person falsely accused and arrested in a robbery investigation. As the role play went on, it showed that even attorneys coming to assist this person are at risk just because they work with the LGBT community. The lack of formal recognition increases vulnerability and thus forces supportive organizations including human rights defenders, activists, legal aid, health workers to work underground and/or put on a facade that makes them difficult to find by the state but also by those who could potentially benefit from their services. It is important to note that the level of invisibility or visibility may be a choice and can be negotiable depending upon the situation.

Regardless, this constant risk has consequences emotionally, physically and socially that affect the safety and design of these support organizations, the people running them and the people benefiting from their services. One such consequence is that at-risk LGBT community members have to develop and share knowledge about informal legal and health support services, which in many cases operate
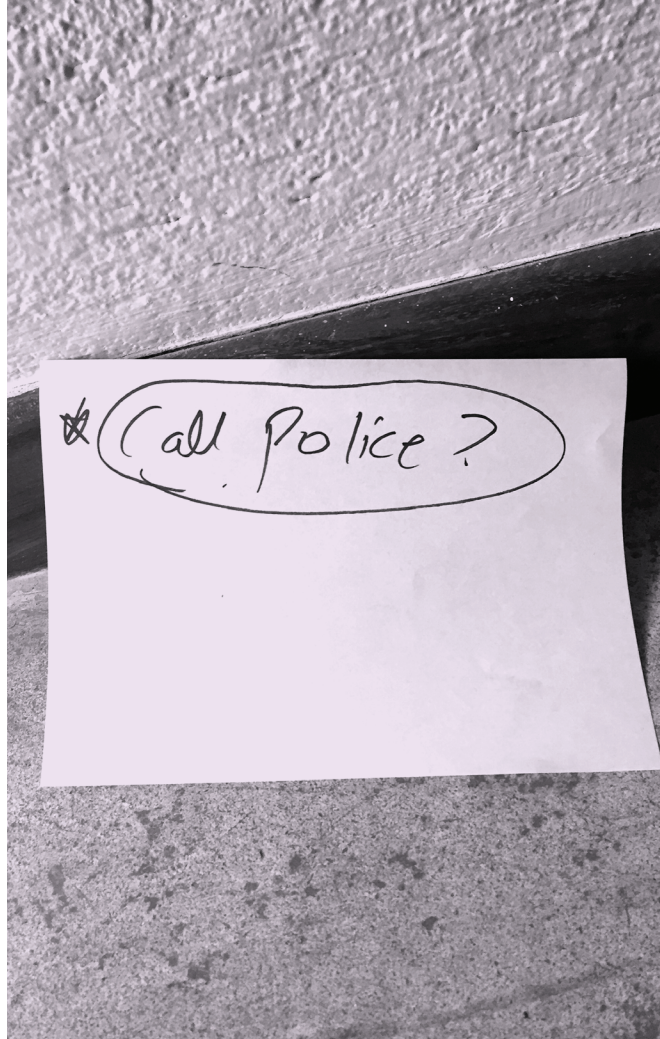
in secrecy. The idea of identity verification applies to those seeking services as much as it is does in the digital realm.

For example, in many of the role plays and stories shared throughout the Needfinding, participants talked about calling a specific friend in an emergency rather than going to a hospital or the police. If someone goes missing or can't be contacted, however, close friends will go to trusted social media channels like Facebook to locate the missing friend. Much of this is "undocumented knowledge" and finding secure and safe ways to verify information, confirm the status of individuals, and share resources more effectively than simply from one individual to the next is a significant challenge.

---

6 Description of the role play exercise is included in the appendix of this report. It was first prototyped in the Tunisia Needfinding engagement and an updated version was employed with this group.

TOOLS USED

The most common "security tools" are those adapted to suit daily reality.

There are many different types of tools that people and organizations are using to protect themselves. Security tools are most often complementary to the physical and psychosocial measures people are already practicing. Some of the practices employed around digital security may not appear to be tools because they aren't recognised digital security tools, but the aim and purpose of their use is to protect and promote safety and privacy.

There is some familiarity with a handful of IFTs. Participants talked about and wanted to learn how to use Signal. They discussed specific approaches for how they use Facebook (including organization accounts and multiple personal accounts). WhatsApp and specifically curated WhatsApp groups within organizations or friend groups were discussed as reliable and secure because people can see when someone opened and read a message.

WhatsApp seemed to be preferred for safe communication because the user has control over who is in groups based on who has your phone number and you can determine who is an administrator. Some had used Jitsi and participated in digital security training where they learned about PGP, HTTPS Everywhere, and one participant mentioned Martus as part of their documentation process, but for the most part the tools people mentioned using the most were social media (Facebook and Twitter), regular phone calls, text messaging and WhatsApp.

People will have Internet via mobile at some point, but right now that is just not the case.

People are currently using phones to call and text their family, friends and loved ones. However many digital security tool developers are no longer considering design for SMS-based phones. The reality now is very different from the future in Uganda, where the Internet is accessible, affordable and reliable via a mobile device. People in the LGBT community need protection now and designing purely for smart devices denies them this opportunity. In addition to limited penetration of smartphones, shared devices are common. There is not a lot of individual ownership of tablets, computers or phones outside of highly professional urban areas. Not only are people managing multiple identities, but they are doing so via one device.

PERSONAS

We have developed these representative fictionalized personas based on the inputs we received from all participants. They represent a multitude of needs and realities described by actual people. They are, however, combined to protect the identity of any one individual and are intended to provide guidance to developers and trainers designing interventions for this community.

JOHN
HEALTH CARE
CENTER DIRECTOR

Occupation

John is the Executive Director of a center that provides health services to the LGBT community in Kampala, and in particular to those who are HIV positive. The center has just celebrated its 3rd anniversary and with the support of a new grant, they have been able to hire staff to support the volunteer doctors and nurses. Because the center isn't recognized by the government, it can be difficult to get supplies and ensure a safe place for patients to receive consistent care. Despite this, the small team of regular volunteers and the newly hired staff are passionate about and committed to the mission, despite the danger of being harassed or attacked for association with LGBT services.

Background

After finishing university with a degree in public health, John started to get more involved in supporting communities affected by HIV/AIDS. As a result he started to learn more about the LGBT community in Kampala and surrounding areas. He noticed that there weren't services being made available for that specific community and it was nearly impossible to go to hospitals and clinics for help. With support from friends and professors from the university he started the center and has recently rented a house to act as headquarters, thanks to a generous donation from a friend of one of his professors.

Motivations

After learning of people not being able to access medication and counseling, John knew he had to provide a safe place where patients and loved ones could seek treatment and support together. A recent trip to London gave him an opportunity to learn more about creative and holistic approaches to running a clinic and he is excited to try them out with his staff and volunteers. John is also the first person in his family to get a degree and he wants to make his family proud even though they don't know explicitly that he is working with the LGBT community.

Challenges

- Since acquiring the house for the clinic, John and his team have had to quickly learn about the types of gates, alarm systems and security guards that are needed to protect the nurses and doctors along with patients coming to the clinic.

- The demand for services has greatly increased and John is looking for additional support staff. Given the secrecy and sensitivity of services he is concerned about how best to recruit and screen applicants.

- John wants to be able to make sure the services the center is providing are helpful and needed. As a result he wants to be able to contact patients once they leave the clinic to know how they are doing and if the awareness and prevention support is working. This has proved difficult especially for patients that are in rural areas.

- Similarly, for John to continue to secure funding he needs to "show impact" which includes tracking who is coming to the clinic and if they are improving. This type of data collection, storage and sharing is challenging for John and his small staff; it is doubly challenging when identities are often made up by patients in order to protect their privacy and security.

Communications

WHO: Current staff and volunteers, doctors and nurses, current and potential donors, the board of the foundation – made up of his former classmates and professors, friends and family from his village, and patients.

WHAT: Supply orders, patient health records and tests, number of patients and services that were provided over various time periods (this is especially important to donors), updates on current and former patients, opportunities to learn more to expand the clinic and services

HOW: Gmail and Google Drive are the primary way to communicate with funders and to store documents, a generic public Facebook page is how people learn about the center, WhatsApp for staff and volunteer communications, smartphone for both personal and center use. John recently learned about Signal and is thinking about getting the staff and volunteers to try it. Jitsi and Skype are used for connecting to other health clinics outside of Kampala that are providing similar services.

Definition of Security

For John, being secure means being able to live your life free from fear and harm. He wants that to be true not only for himself, but also for his staff, volunteers and patients. As a result he knows that the things he has in place to keep everyone safe may not be adequate. He is thinking about changing his behaviors and the tools he uses.

Threat Perception

John and his staff and volunteers are aware that providing health services to the LGBT community exposes everyone to significant risks. Since the center isn't recognized as a nonprofit by the government, if anything would happen to the center they won't be able to file a report with the police or access public funding to provide more medicine. Nosey neighbors or disgruntled former lovers or family members of patients could get them evicted from their new office at any point.

The first space which was close to John's university was broken into and some of the computers were stolen. Luckily none of the records of patients, staff or volunteers were on those computers. He knows of other organizations, like legal clinics, that have been hit by robbers and their information made public; staff was harassed and forced to relocate and start again. John is trying to make sure his staff is not only locking up the building and gates when they leave to ensure physical security, but that they don't bring clinic laptops off premises and they are protected with longer and stronger passwords that they change frequently.

Security Precautions

- Within his staff John has set up a WhatsApp group. He likes that only staff members can be in the group – because those are the people that have your number – and he can specify who is the administrator of the group.

- Personally, John uses Signal. He learned about it from training that was done at his old university. A former professor suggested he attend. He's thinking about having everyone at the center learn about it too.

- He also learned about Jitsi from the same training and now uses it to connect with other health clinics and service providers outside of Kampala to share what he is learning and to get new ideas for funding.

- John's family is deeply religious and likes to stay in touch with their son who is now in the big city. Facebook is the primary way they are in contact. Because of the nature of John's work he has two distinct accounts: one for his family and the other for his friends from university and in Kampala. He does this so that his family doesn't know what community he is providing health services to; he's not sure if they would approve and so he is doing it to protect his patients.

- John takes boda bodas to get to and from work and the center. He tries to make sure he takes different ones and different routes daily. Sometimes that means being dropped off away from the center and walking the rest of the way to arrive.

- Everyone that works or volunteers at the center has a personal knock so they can verify who is coming in.

- There is security at the front gate to meet and vet patients, which adds an additional barrier to those seeking care, but the tradeoff is worth it to keep everyone safe.

LOUISE
LGBT COMMUNITY MEMBER

Occupation

Louise volunteers at an organization that provides basic education services to LGBT and sex workers. She has been volunteering for the past six months because she lost her job as an office assistant after her boss found out she is transgender.

Background

Louise is a transwoman living in Kampala. She is known as Louise to her closest friends but continues to go by Nathan in the village where she is from. She moved to Kampala to attend university and to find work so she could support her younger siblings schooling back home. Louise is considered to be a social butterfly by all of her friends. She loves to dance and go to bars with her friends at night. She recently broke up with her girlfriend and has been enjoying being a single lady in the big city but finds it difficult to approach potential partners in real life.

Motivations

Louise wants to stay connected to her family and siblings back in the village she is from. She is also active in her village church when she returns to visit. In terms of her life in Kampala, she is eager to date and meet someone and fall in love. She finds volunteering to be rewarding; she meets a lot of new people and feels safe at work with her work family, but she feels a bit lonely being single and so she goes out a lot to the bars hoping to meet "the one."

Challenges

- Louise frequents bars that are LGBT friendly only, but if she is going home late at night, she will change clothes so as not to attract unwanted attention from the wrong person. She has a buddy system in which she and her friends check in with each other to make sure they each arrived home safely.

- After Louise lost her job, she was unable to pay her rent and got evicted. She had to move in with friends because she couldn't find a home in the neighborhood she lived in before and knew was safe.

- Louise is unable to use her former employer as a reference because she was fired after they discovered she was a transwoman, and her employer would likely tell her next employer sabotaging any opportunity she manages to find.

- Louise has a trusted boda boda that she takes to the center every day. The driver drops her at 10 minute walk from the center so he doesn't actually know where she goes.

- Louise has been approached by her mother about her Facebook account with the name "Louise"; Facebook suggested to her mother she was someone she might know because Louise has several cousins who are friends with both accounts.

- After they broke up, Louise's former girlfriend, who didn't want to break up, sent an email to Louise's friends and family outing her. She was able to convince her family that the email was a hack and not from her former girlfriend.

Communications

WHO: Friends, coworkers and other community members in Kampala; her siblings, family and church friends back in her home village.

WHAT: Catching up on family and friend news; checking in with each other to make sure everyone is safe and ok; making general plans to hang out, to go dancing and to parties.

HOW: Louise uses voice call to contact her siblings and family at home. Her youngest brother is just five and is unable to write or read. She uses Facebook to connect to her home community; she posts often about God and all sorts of human rights work (only seldomly LGBT issues) to be true to her passions but also protect her identity. She uses WhatsApp, Facebook messenger and Facebook with her friends and co workers in Kampala.

Definition of Security

For Louise, being safe and secure means she is free to go out in the world dressed as Louise without worry or fear. She knows that as long as society (and her family) view being transgender as an immoral behavior, she will not feel secure.

Threat Perception

Louise is generally a happy-go-lucky person but she is constantly aware – some would even call it paranoid – that she will be publicly harassed or physically attacked. Her natural outgoing attitude is hampered by her uncertainty when meeting new people as to whether they want to do her harm or not. She has found it difficult to find a home because nosey neighbors will tell her landlord and get her evicted if she isn't careful about who she has over and how she dresses when leaving the house.

She knows that her work at the center may have some risks, but she doesn't care because she feels surrounded by people who understand her and she can relax a bit in their company. Louise knows not all men are comfortable with transgender women and so she is particularly paranoid about picking a boda boda off the street; she rides regularly with one boda boda driver to and from work. When going out, especially after dark, she'll only go if she can take a personal car, hire a cab or if she is able to catch a ride with a friend.

Security Precautions

- Louise keeps two Facebook accounts to manage the multiple and distinct identities that her family and friends know her by.

- She has a separate email for the few family members who have email than the one she uses at work or in the Kampala LGBT community.

- She only seeks work at places she feels are LGBT friendly; losing her last job was traumatic and caused a downward spiral in her life.

- She always messages her friends after a night out to report having arrived home, and she expects the same from her friends.

- Louise never shares her personal information (contact, address, etc.) with people seeking services at the center, even if they seem like they could be a great friend;

- She always logs out of her account when using the center laptop at work;

- She never shares her passwords with anyone including her siblings, her ex girlfriend etc.

KEY INSIGHTS
& RECOMMENDATIONS

For those designing tools, training, workshops, etc. for and engaging with the LGBT Human Rights Defenders community in Uganda, please keep the following design principles in mind:

Support the fluidity of multiple identities

Duality of identity is the norm for this community; maintenance is resource intensive; it can be used to both harm and protect, but consider facilitating the following:

- Separation between online and offline identities, relationships and networks

- Separation between personal life, work and activism

- Intentional distinction between human rights work and personal LGBT activism.

Think through how digital intervention addresses or relates to physical and psychosocial security threats

Look for ways to connect psychosocial, digital and physical security to maximize impact and adoption.

Being LGBT and staying secure is expensive

In order to feel safe, participants spoke about going to nicer bars where there were security cameras, taking cars instead of boda bodas and finding homes that were more expensive because there was more privacy and security.

Develop tools in tandem with users and local developers

- There is growing interest in and access to coding skills in Uganda, and this is viewed by many as a great way to make money.

- There were individuals with technical skills in the Needfinding exercise who could provide great support and feedback to developers developing for this context.

- Participants as a whole felt they learned a great deal from each other about how to be more secure both on and offline. Uncovering the needs of the community serves both to inform tool development and also to uncover the community of

tools that have already been developed, and which might be appropriate.

Support verification of identity

- Current practices to verify identity and intentions of those seeking services and/or membership is time intensive and subjective. Many organizations have a person devoted to managing all of this and this puts not just them but their entire network at risk of being attacked if that person is compromised.

- Learning and ideas should be shared on how to support individuals with multiple online identities.

- Current practice in verification is driven by an individual who is testing to see if people are seeking to do harm to the community; it's about evaluating real intentions. Some of the approaches currently employed include asking for information that only that person would know and vetting among a network of already vetted individuals.

- Verification methods require existing online connection for access. They also set up a condition where a person that is truly in need of community feels judged, as they are in the larger society. Is there a way to maintain verification protocols while making sure new individual feel welcome and a part of a community?

Support documentation and connection in remote and rural areas where feature phones (non-smart mobile devices) are available but laptops are not

- It is difficult to find a central repository to safely keep documentation that can be easily accessed.

- Being able to add rich media content (videos and pictures) is essential, and being able to upload and then immediately remove from a personal device is desired.

- Organizations that need documentation have cobbled together different methods that often don't support remote access.

Let people know immediately when their information might have been shared

- Blackmail and break ins are not uncommon and in the immediate aftermath, it is difficult for individuals and organizations to know what has been taken (including names and other identifying information) and distributed without permission.

- Organizations serving this community need to store information about the communities they serve more securely and also have a way to quickly alert

those whose information has been stolen, that it has so
they can take proper precautions from being outed.

Help notify people and connect them to each other

- Physical safety is critical, as is allowing people to know where and with whom others are.

- Community members are looking for secure ways to communicate if someone has been arrested or attacked. Similarly, before things escalate to that level, people are seeking a way to track or "watch your back" especially if they are alone.

- Any intervention should be available on a simple phone (and even better if the phone is powered down) and offline.

Awareness of IFTs in this community are currently limited

- While participants expressed interest in being trained on Signal at the end of the Needfinding session, the awareness of other IFTs was limited.

- People are using and adapting their behaviors to leverage platforms that are widely adopted and accessible, such as Facebook, WhatsApp and voice calls for trying to reach a family member who is online less frequently.

- Computer literacy is low for the most vulnerable LGBT populations; digital security training reaching these individuals must include or start with basic computer literacy.

Guidance on designing for mobile

- Although smartphones are prevalent in the community, there are still many people who use or share non-smart phones. There is discussion, and has been for some time, about smart phones and web service becoming more affordable and universally available, but this is not currently the case.

- Access to wifi and data plans heavily influence what devices and tools people use and whether they decide to use a more secure tool or approach. If it appears that the tool will use more data, it is often passed over.

There is a tension between making something flexible and appropriate in your context versus making something that – while it might solve a problem technically – is difficult for people to understand. Participants in the Needfinding engagement appreciated being included in the discussion and having an opportunity to learn from each other about security practices. People understanding how apps work and having input into the development process increases trust, but there is a fine line between trust and acceptance on one hand, and overwhelming people with technical information and detail on the other.

CONCLUSION

The threats that the LGBT community faces are vast and varied in Uganda, especially given the fact that threats often emerge directly from people they have close relationships with - such as bosses, friends, family members, landlords or former lovers. The community's resilient spirit and the approaches already put into maintaining personal "security plans" are an excellent starting point for the larger Internet Freedom community to build upon. Similarly, the connection between digital, psychosocial and physical security point to an opportunity for collaboration. Solutions and tools should be developed in tandem with the community and should consider more than just digital threats in order to have a more comprehensive approach to safety and security. A concern about security is that it is purchased and expensive, which leaves those without financial resources in a particularly vulnerable state.

The LGBT community in Uganda needs the IF community — both trainers and developers alike — to support groups already working in the space. Poised and ready to engage with the broader IF community are local groups working on issues of digital security and inclusion such as i Freedom Network of Uganda and Defend Defenders. These groups have existing expertise that position them to guide and support tool development and training indigenously. The findings and recommendations in this report provide a foundation for developers, designers, trainers and the larger Internet Freedom community. The knowledge contained herewithin and shared by LGBT human rights defenders is critical to improve existing interventions – i.e. tools and approaches – and to develop new ones that support human rights of a population currently at risk.

APPENDIX

ROLE PLAY

In the course of the Tunis Needfinding engagement and the Uganda LGBT Human Rights Defenders engagement we developed a new component for the Internet Freedom Needfinding Framework: Role Play. This new exercise was designed to help participants tell their stories more authentically and to help others have a deeper understanding of their experiences.

DEFINITION

Role Play: A group exercise that uses principles of drama and analysis to articulate and think through a security threat or risk. Small groups develop a scenario (which we refer to as a skit), act it out in front of others and – as a larger group – reflect on what just happened and how to prevent and/or solve the threat that was shared.

OVERVIEW

Storytelling takes lots of different formats. Giving participants an opportunity to explore an important experience that they, or people they know, have had, and then analyze their actions and what they could do in the future is a powerful way to understand not only risks and threats, but also mindsets and decision-making processes.

Being able to embody and walk-through the steps of a security threat helps identify key points where specific tools can be designed or altered to meet the challenges at hand, as well as provide guidance on how training can be structured to reflect the journey users go through in their lives.

WHY

Instead of recalling an incident, role plays create space to further explore issues as a community. Identifying the scenario, thinking about how it can be explained to someone that wasn't there, witnessing a re-enactment and reflecting on decisions made and courses of action taken provides fruitful insights for developing a deeper understanding of what is happening in communities.

This activity is often followed by a "Design Your Ideal Communication Tool" activity. Thus priming participants to think about solutions more holistically and have a point of view going into the design process.

HOW

1. **Pre-role play exercise**

   The role play exercise typically takes place after participants have visualized communication priorities and their threats. This ensures everyone is in a similar headspace, able to share experiences, and receptive to listening to the experiences of others. In some ways this helps to prime/identify risks that they can act out.

2. **Developing the skit**

   The amount of time needed for the exercise depends on how much time you've allotted for your entire session and the number of participant groups. The following is a basic breakdown to guide you when you have 1.5–2 hours:

   In groups of 3–4 people, think of a security threat or risk scenario and develop a skit to share with the larger group. This could be at a march, election rally, meeting up with a friend, traveling, etc.

   Participants are encouraged to use scenarios from earlier discussions. Each scenario should include:

   - a specific communication need: be very clear about what you are trying to achieve

   - articulation of a risk or threat related to that communication

   Demonstrate how that scenario plays out:

   - **Who** - People that are involved

   - **Communication Need(s)** - What are you trying to do?

   - **Risk(s)/Threat(s)** - What happened?

   - **Action(s)** - What did you do? What did you use (tool, person, org, reference, etc...)?

Remind participants that the scenario they choose to use for the skit does not have to be their own, it could come from a combination of things that have happened to them, something they read about or heard about from a friend or colleague.

Each skit should be between 3 and 5 minutes. Give teams 30-45 mins to choose, prepare and practice their skit. Identify who on each team will be the primary facilitator for this exercise. Check in on them throughout this section of the exercise to make sure they are on track.

Provide basic materials to use as props and scenery, such as markers, post-its, flip chart paper and pieces of cloth. Encourage groups to use things that they have brought themselves like backpacks, laptops, phones, sunglasses, etc.

3. **Show time**

   Secure a place that can serve as the "stage" and provide seating for the rest of the participants and yourself. Make sure that the main facilitator for this section and a note taker are in a place where they can see each other as well as what is happening on stage and in the audience. Remind teams of how much time they have for their skit and discussion.

Documenting skits

Please follow whatever security and privacy guidance you have established for the entire engagement. It may be tempting to record video of these with your phone or you may see other participants wanting to do so. Please remind everyone again before the skits start what security environment you all have agreed to as it relates to documenting and sharing.

4. **Debriefing**

   At the end of each skit "performance" leave time for the "actors" and "audience" to talk through what just happened. This is the time to ask them to summarize the skit and start diving into what they were thinking, what tools they were using, who they turned to for help, etc. You can also open this up to the audience to understand what struck them that was interesting or what they would do if they were in a similar situation.

Just like in other components of the Needfinding framework ask questions that seek to better understand the motivation of the participants that means use their own words and have them define concepts in their own words. Similarly take notes in the actual words that participants are using. For more guidance take a look at Conducting Interviews component of the framework.

At the end of all of the skits, pull out key takeaways from the experience including patterns – things that were similar or different in the way that participants were handling threats or risks. Similar to the debrief at the end of each skit, open this time up for others to share their takeaways and observations from the entire exercise.

We'll be updating the Needfinding website to include this new component.