Image not found or type unknown

Mobile safety

Work with participants to share strategies and tactics for using their mobile phones more safely in situations and contexts where they live. We **highly recommended** that you choose a Learning Path to travel, as these include activities with different levels of depth that should help participants obtain more insight into the covered subjects.

- Introduction and learning objectives
- Learning activities, learning paths and further reading
- Mobiles, intimacy, gendered access and safety [starter activity]
- Making a mobile timeline [starter activity]
- Himalaya trekking [starter activity]
- Collecting phones [starter activity]
- Me and my mobile [starter activity]
- Mobile power - device, account, service, state, policy [deepening activity]
- What is a phone? How does mobile communication work? [deepening activity]
- Debate: Documentation of violence [deepening activity]
- Planning mobile communications for actions/organising [tactical activity]
- Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft [tactical activity]
- Discussion, input + hands-on: Choosing mobile apps [tactical activity]
- Using mobiles for documenting violence: Planning and practicing [tactical activity]
- Reboot your online dating safety [tactical activity]
- Safer sexting [tactical activity]

Introduction and learning objectives

mobile-safety_v2.png

Image not found or type unknown

In this module, we work with participants to share strategies and tactics for using their mobile phones more safely in situations and contexts where they live.

This module offers guides for facilitating conversations about how women's rights and sexual rights activists experience their access to mobile technology and communications differently based on their genders and sexual identities. We'll talk about how we are using our mobile phones for personal and private communications, for public and movement communications, and strategies and tools we are using to managing our mobile communications more safely.

This module includes: group activities for and examining our use of mobiles and how this relates to our genders and sexual identities; hands-on activities for exploring and understanding how mobile phones and mobile communications work; group activities for sharing and practicing safety strategies and tactics in the context of our lives; facilitation guides for trainers to bridge issues of feminist safety and technical security.

Common questions we hear and are trying to address in this module:

- What happens if someone else has my phone? What information is on my phone? How might this affect myself, my colleagues, my movement?
- How do I know if I'm being surveilled by my partner, exes, family members, governments?
- How do I use my phone more safely?
- How can we use our phones to organize?

Learning objectives

By the end of this module, the participants would have:

- an understanding of how mobile access and communications are gendered and intimate;
- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- an understanding of basic concepts of how mobile communications work in order to better understand the risks of mobile communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

image-1605452256072.png
Image not found or type unknown

Learning activities, learning paths and further reading

This page will guide you through the Module's correct use and understanding. Following the Learning Paths, with activities of varying depth, should allow participants to obtain a better grasp of the studied subjects.

Learning paths

For trainers/facilitators who are interested in any specific activity, you can use one or a few in combination. **We recommend beginning with a starter activity to open discussion and sharing by participants about their mobile phone experience and how gender, sexuality, race, class, ability, are related to and impact their experiences.**

Some specific recommendations: For groups who are considering how to use mobiles for **documenting violence** we recommend the deepening activity Documenting violence to open space for debate and discussion about challenges and opportunities of documenting violence and the tactical activity Using mobiles for documenting violence: Planning and practicing.

For groups who want to **use mobiles for communications for actions and organizing** we recommend the tactical activities including Planning mobile comms and Back it up, lock it, delete it.

For **participants using mobiles for online dating and sexting**, we recommend starter activity Collecting phones and tactical activities Reboot your online dating safety and Safer sexting.

Learning activities

Starter activities

image-1605640724450.png
Image not found or type unknown

- Mobiles, intimacy, gendered access and safety
- Making a mobile timeline
- Himalaya trekking
- Collecting phones
- Me and my mobile

Deepening activities

image-1605640735000.png
Image not found or type unknown

- Mobile power - device, account, service, state, policy
- What is a phone? How does mobile communication work?
- Debate: Documenting violence

Tactical activities

image-1605640743110.png
Image not found or type unknown

- Planning mobile communications for actions/organizing
- Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft
- Discussion, input + hands-on: Choosing mobile apps
- Using mobiles for documenting violence: Planning and practicing
- Reboot your online dating safety
- Safer sexting

External and tool-based activities

Where modules include practice and use of specific tools and software, we have linked to external resources. We do this for a few reasons: tool designs and features and security issues change frequently and so it is best for us to link out to resources that are updated frequently.

Special note for mobile safety training

It is very rare that all the participants in your workshop would have the same kind of mobile phone. It is a good idea to do hands-on in smaller groups: for iPhone users, for different versions of

Android, and/or for feature phone users.

Resources | Links | Further reading

- Video for Change guides: https://video4change.org/resource-categories/
- Witness guides: https://witness.org/resources/
- Security in a Box: https://securityinabox.org/en/
- My Shadow resources: https://myshadow.org/ [Training resources are no longer available, but a guide on how to control our data is still available.]
- EFF's Surveillance Self Defense: : https://ssd.eff.org/en

image-1605452256072.png
Image not found or type unknown

Mobiles, intimacy, gendered access and safety [starter activity]

image-1605640366569.png

Image not found for type unknown

This is an **introductory discussion** about the ways that participants are using their mobile devices. Facilitators can use this exercise to introduce concepts about gendered access, to highlight how we manifest many of our identities in this mobile space and how this presents unique possibilities and risks for participants.

We recommend doing this at the start of a workshop about mobile safety.

This activity has 3 stages:

- Pair share
- Pair Reportback
- Facilitator Synthesis of common elements

Learning objectives this activity responds to

- an understanding of how mobile access and communications are gendered and intimate;

Who is this activity for?

This can work for anyone who uses a mobile phone or has used one.

Time required

This activity will require about **30 minutes.**

Resources needed for this activity

- white board or chart paper (if the facilitator chooses to write during the shareback)

Mechanics

Our mobile phones are spaces of intimate interactions. We connect with loved ones, lovers, friends, share calls, messages, images, videos, private conversations and images. And insodoing, we know our mobile phones as personal intimate objects, but they are also a part of a larger context, linked to mobile phone providers, regulated by government policies, subject to getting taken, viewed without our consent.

Mobile phone access varies by gender and mobile phone use by women represents a challenge to power – people may enact violence on women using mobile phones; in another context, women may use mobile phones to report abuse.

Pair Discussions - 15 minutes

In pairs to facilitate personal sharing. Ask one partner to share first and the other to listen. Then prompt partners to swap listening and speaking roles. Each person should have about 5-7 minutes to speak. This will depend on how long it takes for pairs to form.

Questions

Write these somewhere visible to everyone or on pieces of paper that the pairs can take with them to their discussions.

- **How do you use your mobile phone? When do you use it?** *If people are stuck, ask them how they use it with different kinds of people: friends, family, colleagues, strangers.*

- **How do you use mobiles for organizing?**
- **When do you feel unsafe using your mobile phone? What do you do to manage in these situations?** *Encourage participants to not discuss possibilities of theft, looking for people to share examples of things like spying housemates, partners, family members; police seizures, etc.*

Full Group Shareback - 15 minutes

Facilitator make notes and synthesize. Are there any strategies in specific that you want to address, situations, scenarios?

image-1605451879726.png
Image not found or type unknown

Making a mobile timeline [starter activity]

image-1605640366569.png

Image not found or type unknown

This is an introductory activity participants share personal experiences with mobile phones and engages people through body movement and storytelling. You can expect participants to speak and hear about each other’s attitudes towards mobile phones and to share ways that they are using and accessing phones that are personal and meaningful to them.

This is similar to the activity, Women's wall of internet firsts, inviting participants to share their experiences of mobile technologies and to relate them to one another along a timeline. Through this activity, the trainer(s) can also become more familiar with the participants' experiences and relationships to mobiles.

Learning objectives this activity responds to

- An understanding of how mobile access and communications are gendered and intimate.

Who is this activity for?

This can work for anyone who uses a mobile phone or has used one.

Time required

This activity will require about 30 minutes.

Resources needed for this activity

Labels to mark a time line with dates in 5-year segments, 1990-2019. This can be numbers written on paper and laid on the ground (ex. 1990, 1995, 2000... etc).

Mechanics

Prepare a timeline in your room. Participants will stand along the timeline at specific dates in response to questions you ask. In a large group, ask participants to move to a time along the timeline in response to the following questions. When the timeline is created, ask what the first and last dates are, if there are clusters of people at certain areas of the timeline, ask them where they are.

Depending on your group size and how much time you have, choose 2 or more questions.

Ask 1-2 participants to respond to the specific questions, for example, "What was it like?"

Questions

- **When did you first have a phone?** What was it like? Did you share it with anyone? How old were you? What did you use it for?
- **When did you have your first smart phone?** What does that mean to you? Did you share it with anyone? What is your favorite app? Why?
- **When did you first connect to the internet using your phone?** What website did you access first? Why?
- **When did you first "retire" a phone?** What did you save from the phone (ie. Media like photos, text logs, hardware)? Why?

Debrief - 5-10 minutes

Ask participants if they have any comments or observations to share. Facilitator, debrief and connect what people have shared to intimacy and gendered access - consider what people have said about their attitudes towards their phones and the ways that they like to use their phones.

Intersectionality Flag: How is mobile access and privacy varying among participants based on their gender, sexuality, race, class?

image-1605451259399.png
Image not found or type unknown

Himalaya trekking [starter activity]

image-1605640366569.png

Image not found or type unknown

This is an **introductory activity** to raise participants' awareness about mobile security and for both participants and facilitators to assess the kinds of safety measures participants are taking and the vulnerabilities that might be the largest priorities to address. We recommend doing this at the start of a workshop about mobile safety.

Learning objectives this activity responds to

- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements.

Who is this activity for?

This can work for anyone who uses a mobile phone or has used one.

Time required

This activity will require about **30 minutes**.

Mechanics

Facilitator ask the participants to stand in a line shoulder to shoulder. Ask questions about mobile security of the participants. Instruct participants to take a step forward if their answer to the question is yes, a step backwards if their answer is no.

Example questions

- Do you have a screen lock?
- Do you use app locks?
- Do you have an unregistered SIM?
- Do you use an alternative email (not your main email account) for your phone?
- Have you set up remote access (Find my phone) on your phone?
- Are location services turned on your phone?
- Do you have a backup of the media on your phone (photos, messages, videos, etc)?
- Do you have an anti-virus on your phone?

Debrief - 5-10 minutes

Ask participants if they have any comments or observations to share. Facilitator, debrief and connect participants' trekking to the agenda for the day or series of sessions you will be together.

image-1605452256072.png
Image not found or type unknown

Collecting phones [starter activity]

image-1605640366569.png
Image not found or type unknown

This is an **introductory activity** to raise participants' feelings about their mobile devices and other people accessing the devices and contents.

Learning objectives this activity responds to

- an understanding of how mobile access and communications are gendered and intimate;
- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications.

Who is this activity for?

This activity works particularly well in the context because their workshop participants experience this often. We recommend this exercise if your participants are experiencing device seizure and want to discuss the impacts on them and their emotional responses.

> **Care note:** We recommend doing this with great **care**. Get participants' clear and emphatic **consent**. This will likely work best in a context where you and your participants have already built **deep trust** with one another.

> **A note about learning pathways:** This is a great starter activity to prepare for discussions and tactical activities around preparing for high-risk situations in which phones may be taken

or lost.

Time required

This activity will require about **30 minutes.**

Mechanics

Activity: Collect participants' mobile and discuss – 15 minutes

Collect participants mobiles in the very beginning, getting their clear and emphatic consent, but without explaining why you are collecting them.

Discussion

Ask:

- How do you feel about not having your phone in your hands?
- What are your immediate feelings?

Activity: Return mobiles and debrief - 5-10 minutes

Return the mobile which was collected from the participant in the very beginning.

Discussion

Ask:

- How did you feel to leave your mobile? Why?
- How do you feel getting your phone back? Why?

- Are there times when your mobile is taken from you? Who is taking it and what is the situation?
- How do you feel in that situation? Why?
- Why is your phone important to you? What does your phone give you access to?
  Encourage participants to be specific about how they relate to their phones, what the phone connects them to, the importance of their phone.

image-1605451879726.png
Image not found or type unknown

Me and my mobile [starter activity]

image-1605640366569.png
Image not found or type unknown

This is an **introductory discussion**. This is designed as a very short activity, to facilitate participants' thinking about how they are using their mobiles in intimate ways and to begin to share practices and concerns around surveillance and privacy related to these.

We recommend doing this at the start of a workshop about mobile safety.

Learning objectives this activity responds to

- an understanding of how mobile access and communications are gendered and intimate.

Who is this activity for?

This can work for anyone who uses a mobile phone or has used one.

Time required

This activity will require about **30 minutes**.

Resources needed for this activity

- white board or chart paper (if the facilitator chooses to write during the shareback)

Mechanics

Pair discussions - 15 minutes

In pairs to facilitate personal sharing. Ask one partner to share first and the other to listen. Then prompt partners to swap listening and speaking roles. Each person should have about 5-7 minutes to speak. This will depend on how long it takes for pairs to form.

Question 1: What are the most personal and private things you do on your mobile phone?

Question 2: What do you do to take care of these interactions, media, these experiences?

Facilitator, give an example or two of what you would share in a pair. For example, nudes that you are taking for your own pleasure and expression of self, sexting or intimate conversations you are having with others.

> **Intersectionality Flag:** How is mobile access and privacy varying among participants based on their gender, sexuality, race, class, disability?

Full group shareback - 15 minutes

Facilitator make notes and synthesize. Ask people to share what they spoke about. Draw out common threads from the conversation. How are people using their phones and in what ways are these uses intimate? How have participants shared that their gender relates to their access to mobile phones, to their privacy? What are people doing to care for their intimate interactions and mobile media? What are people concerned about and how are they relating privacy and gender, sexuality, race, class, disability, age, etc?

image-1605451879726.png
Image not found or type unknown

Mobile power - device, account, service, state, policy [deepening activity]

image-1605640472202.png

Image not found for type unknown

This is a **collaborative mind-mapping activity**. Through a facilitated conversation, the group will discuss how they relate to their phone devices, service accounts, mobile phone providers and a small amount about how corporate and government policies come into play.

We suggest doing this activity at the start of a mobile workshop.

Learning objectives this activity responds to

- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- an understanding of basic concepts of how mobile communications work in order to better understand the risks of mobile communications;

Who is this activity for?

This can work for anyone who uses a mobile phone or has used one.

Time required

This activity will require about **45 minutes** as written. If you want to cover this content faster, you could ask the participants fewer questions and instead share a slide or example mindmap.

Resources needed for this activity

- chart paper
- markers

Mechanics

Ask your participants a series of questions and mind-map their responses. The goal is to try to map the ways participants related to their mobile phones. Participants will discuss mobile power, control and agency as they discuss how they relate to their **mobile devices**, **service accounts**, **mobile phone providers** and **corporate and government policies**.

Suggestions for preparation

- Familiarize yourself with the local carriers;
- Familiarize yourself with the links between the local carriers and the state. ex. are they state run?
- Prepare some local examples of ways that women/gender rights activists are using their mobiles, how this relates to power; how corporations and/or the state react/regulate if applicable;

Draw a mind map in a visible space so people can see as you ask the following guiding questions.

- indicate places where participants speak of choices or decisions that were made for them. ex. type of phone, android/nokia; who else has access to their phone, how they chose it; service provider; plan type; who has access to their plans

example mindmap. click to view it larger.

Mobile_screenshot.png
Image not found or type unknown

Questions to ask

- **About devices**: What kind of phone do you use? How did you get your phone? Do you share it? How and with whom?
- **About your mobile service**: How did you select your mobile carrier? Do you share your plan? Do you manage your plan and if not, who does? Did you choose your plan? How?

Ask/discuss

The relationship between ourselves and our mobile providers. Did you sign terms of service? What did you agree to when you signed your contract? What did you provider agree to?

Note to facilitators: If you know of particular concerns with local carriers, try to find and bring examples of terms of service and/or case studies where people/consumers have engaged with the carrier around safety.

Ask/discuss

The relationship between the mobile providers and the state. Are these state run? Are they international, local, regional companies?

Note to facilitators: You may want to research in advance, state regulations or influences on mobile use. Have there been any recent state shutdowns of service? Are participants familiar with targeted shutting down of individual's lines? Do security forces seize devices?

Additional resources

Case studies: *as WRP continues to use this activity, add links to relevant case studies here*

- A wikipedia page listing mobile carriers by country: https://en.wikipedia.org/wiki/List_of_telephone_operating_companies
- 101: SIM Card Registration: https://privacyinternational.org/explainer/2654/101-sim-card-registration

image_1605451259390.png
Image not found or type unknown

What is a phone? How does mobile communication work? [deepening activity]

image-1605640472202.png

Image not found or type unknown

The purpose of this activity is to deepen knowledge of how mobile communications works in to support participant's ability to assess and plan for risks of mobile communications. Facilitators should include this in any mobile workshop or confirm that all participants are already familiar with the information in this activity. It is the basis of assessing technical mobile risks.

This activity has 2 stages:

- Hands-on phone dissection
- Input: Mobile communication data and risk considerations

Learning objectives this activity responds to

- Understand some basic concepts of how mobile communications work in order to inform ourselves about the potential impacts of using mobile communications;

Who is this activity for?

This activity is for anyone participating in a mobile workshop.

Time required

This activity will require about **45 minutes.**

Resources needed for this activity

- some mobile phones to open up and investigate
- A whiteboard, slide, or handout with top level points

Mechanics

Mention or discuss, depending on time, that we will talk about mobile technologies – considering devices that are easily portable in a hand or pocket and have communication capabilities from voice calls and sms to web and data services. Some of this section will apply also to tablets.

Inside our phones - 5 minutes

Take this phone apart. Your phone is a tiny computer. Everyone take your out and locate:

- Parts that listen and project sound: microphones, speakers
- Parts that view and display visuals: cameras, screens
- Parts that send and receive information from other sources: GPS, Antennae, Wifi
- Parts of the computer, hardware: battery, circuitry
- Memory: SD card, other memory built-into the phone
- SIM card slot(s)

Device and SIM identity - 5 minutes

Your phone has all these pieces and it has a few identifying features, in addition to the make, model and OS, it has 2 names - a Device Identifier and a SIM Card identifier. These are important to know about because you can be identified by either one and your phone communicates this information often, especially the IMSI.

- **IMEI** is the name of your device

International Mobile Equipment Identifier (IMEI):
https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** is the name of your SIM card

International Mobile Subscriber Identity (IMSI):
https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

Our phones in communication - 35 minutes

We use our phones to communicate with people: SMS, Messaging, Social Media, Apps, Calls. Our mobiles are also communicating information about our phones and ourselves - not just our messages but metadata, our location, etc, and this can be linked to other information about us like our social networks, our organizing networks, our habits and places of work.

It's good to be aware of these, mostly so that we can understand how our mobile phones use can act as a tracking device in the moment and as a historical record of our activities afterwards.

1. Your phone is chatty

Your phone is calling out to different types of networks and via different types of communication to announce it is near and to connect or check if anyone wants to connect.

Mobile carriers

Mobile carriers have towers and antennae that your phone communicates with. Each antenna can reach a specific area. Your phone checks in with whichever tower(s) you're nearest. It shares **at least your IMSI** to announce which mobile carrier you are using and your number so you can receive messages, calls, and communications to your device. Every time you are near a tower, it is like dropping a pin on a mapped timeline where you are. You mark where you are, when you are there, and what you are doing in that location in terms of using your phone.

GPS

If your GPS feature is on, your phone is communicating with GPS satellites, similarly checking in, which is like dropping pins on a mapped timeline.

Wifi

If your wifi is on, as you pass through Wifi networks, your device may both attempt to connect to those networks, leaving a pin with the wifi network, and also make a record of the network name in your phone.

Bluetooth/NFC

If these are turned on, other devices using Bluetooth and NFC may be able to communicate with your device, attempt to connect, share files. Etc.

Facilitate discussion: Which things you need to have on when? Are records of where you are a risk for you or not?

2. You are chatty

We use our phones to communicate. Different types of communication appear differently while you are communicating and once the messages have been sent.

SMS

Text messages and metadata - in communication and once stored on your device and with your carriers, are sent in cleartext. A useful analogy is that an SMS is like a post card. If someone intercepts it, they could read the entire contents as well as metadata (ex. sender, recipient, time, date).

MMS

Media messages and metadata - in communication, this may or may not be encrypted, so if someone is trying to intercept your communications, it will vary if they can see it. Once it's sent, you and your recipient's mobile providers and devices have a record of the message and so investigation into either might reveal metadata (ex. sender, recipient, time, date) and content.

Calls

Call content and metadata - similarly - calls should be encrypted as they are in progress, but your provider and your recipient's provider will store metadata about the call (ex. sender, recipient, time, date) and if your opponent has access to your providers, they may have access to listen into calls or to record them.

For more information about Apps and Messaging Apps, see:

- Discussion, input + hands-on: Choosing mobile apps

A note about state surveillance: From country to country, state surveillance varies. In some places, governments will have access to any and all data that carriers have -- so with these, you should consider all of your metadata and contents of unencrypted services accessible to governments both in real-time and after the fact if there is an investigation for these records.

Your best defense against surveillance is End-to-End Encryption.

3. A phone is a small computer

Software bug - A phone is a computer and can be infected with malware just like a desktop or a laptop. Individuals and governments alike use software to bug other people's mobile devices. This kind of software often uses parts of the phone to act as a bug or a tracking device, listening in with the microphone or sending location data.

4. The cloud is a file cabinet

Some data that my phone accessess is not on my phone at all, it's on the cloud. The "cloud" is just a term that means "the internet" -- data that is stored somewhere physically on a device that is connected to the internet. Your apps may accessing data that is in the cloud and not actually on your device.

Considerations: Is my data encrypted in transit between myself and the service? Is it encrypted when it's stored by the service? Do I know of any instances when opponents have been able to get access to this information - when, how?

Note to facilitator: As you speak, participants may ask questions about parts of phones or risks associated with communication methods you mention. Take the time to answer questions. If you can, keep a running list of issues and topics that people ask for additional information about -- a

running list on a white board will do. Also keep a running list of issues and topics you will not get to this workshop so that you address it later in the workshop or suggest as follow up after the workshop.

Additional resources

- 7 Ways to find the IMEI or MEID number of your phone: http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- International Mobile Equipment Identifier (IMEI): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- International Mobile Subscriber Identity (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

Tactical Tech's My Shadow site has a number of great training guides to facilitate learning about mobile tech.

- My Shadow downloadable materials: https://myshadow.org/materials
- My Shadow website: https://myshadow.org/

Some videos:

- How does your mobile phone work? This video at nine minutes is likely too long to show during your workshop but can be a reference for participants and for yourself to understand how cell phones work via antennas and mobile switching centers, as well as cell phone generations. https://www.youtube.com/watch?v=1JZG9x_VOwA You might like to find shorter videos that touch on some details and are more appropriate to your specific context once you are familiar with this longer video.

image-1605452256072.png
Image not found or type unknown

Debate: Documentation of violence [deepening activity]

image-1605640472202.png
Image not found or type unknown

This is a deepening **discussion activity** to facilitate discussion around using mobiles to document violence and how this relates to perpetuating violence. This exercise can be used to discuss case studies specifically of activist media aimed at reducing violence to ways in which the same channels and media have been used to perpetuate violence.

Participants will share examples of how they are using mobiles to document violence and will engage in debates around the impacts of sharing documentation of violence online.

Learning objectives this activity responds to

- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications.

Who is this activity for?

Groups who are currently or considering using mobiles to document violence.

Time required

This activity will require about **60 minutes.**

Resources needed for this activity

- Printed or linked case studies

Mechanics

In plenary - 10 minutes

Ask participants to share ways they are using mobile phones to document violence.

> **Care Note:** People may share incidents that are activating for themselves and others in the room. When you ask for examples, acknowledge any agreements and norms of your space regarding speaking about violence. You may want to acknowledge that the exercise will discuss acts of violence and that people who are sharing are invited to share and to take care of themselves, to share in a way that they do not exceed their own capacity, to ask people to care for themselves if they are feeling activated to stop sharing or to care for themselves how they need.

Ask:

- What are examples of documenting violences and sharing the documentation that have had a positive impact on your work, advocacy, for your communities?
- What were you documenting?
- What happened?
- How did you share?
- Who did you share with and how did you choose these people?
- What was the response?

Facilitators, you may want to prepare examples of recent and local movements using mobiles to document violence and ask participants to share examples of how they are using mobiles to document violence or to share documentation. Examples may include: documenting state violence, forwarding videos of violent acts, live streaming violence, the implications of having possession of this kind of media.

Some examples are linked in the "**Additional resources**" section below. You may choose to use these for your small group case studies or to select examples that are more current or appropriate for your participants.

Explain that this activity is to facilitate space of discussion and debate around this use.

Small group - case studies - 20 minutes

Give each small group a case study to read and discuss. You can find case studies below – choose from and edit case scenarios, blog posts and articles from the news, or choose or write examples that are more relevant for your participants.

- What is the example?
- What are arguments for using mobiles to document violence in this instance?
- What are arguments not to use mobiles to document violence in this instance?
- What are some ways you could reduce negative impacts of this kind of video documenting violence?

Scenarios

These scenarios are examples of one way to write scenarios for your workshop participants. By writing more than 1, you can raise multiple issues that you know participants will want to discuss. The examples here are designed to spark conversations around linking documentation to movement, consent, impact and perpetuation of violence.

Scenario 1

Your community has been facing violence and harassment. You and others have organized to document specific acts and to share some of these on social media platforms with subtitles and text to explain the incidents and the ongoing violence. You link these to resources including a list of demands of your community is making and support resources for people who are experiencing similar violence.

Scenario 2

You witness an act of violence on the street and begin live streaming it to your social media channel where you have thousands of followers. You do not know the people you are filming and

you do not know the context.

Scenario 3

You and your community have been livestreaming footage from demonstrations in order to both show the power of the demonstrations and to document incidences of violence and harm done to demonstrators. You become aware that the footage is being used by local police and by opposition groups to target demonstrators and edited together to create oppositional media about demonstrators that is also being shared on social media.

In plenary - shareback - 30 minutes

The full group shareback is an opportunity for each group to share their case study and to have a full group discussion about current challenges with documenting violence and sharing this documentation online. Allow for ample time for groups to share and for others to engage.

- What is the example?
- What arguments for and against using mobiles to document this instance of violence came up?
- What does this raise for others? Do you encounter this issue? How are you thinking about it? How are you strategising for the best possible impact and how are you reducing likelihood or negative impacts?

Facilitator, as participants shareback, draw out common themes. What are your participants concerned about most in their work – some issues that may come up and that you can facilitate sessions on more specifically later may include tactical issues of how to document, store, share; issues of verification of media, deep fakes; use media to incite violence and the possibility of sharing documentation of violence as perpetuating violence and harm.

Additional resources

Case studies and blog posts about the impacts of documenting violence

Examples of how people are using mobiles in organizing - we suggest gathering local or relevant current examples of how organizers are using mobiles and asking your participants and hosts for examples in preparation for the workshop.

- Migrant workers documenting abuses
  - Centre for Migrant Advocacy´s OFW-SOS

Live streaming violent acts Case Study: The Ethical Challenges of Live Internet Broadcasting, Irie Crenshaw and Justin Pehoski https://mediaengagement.org/research/matters-of-facebook-live-or-death/

- Australia

The world is turning against live streaming, In the aftermath of the Christchurch shooting, Australia is leading the charge against raw, unfiltered video, Casey Newton, April 4, 2019 https://www.theverge.com/interface/2019/4/4/18294951/australia-live-streaming-law-facebook-twitter-periscope

- Brazil examples

Dispatch from Brazil: If killed by police, guilty by default unless there's video?, Priscila Neri https://lab.witness.org/dispatch-from-brazil-if-killed-by-police-guilty-by-default-unless-theres-video/

- Whatsapp and violence in India

WhatsApp will drastically limit forwarding across the globe to stop the spread of fake news, following violence in India and Myanmar, Kurt Wagner Jul 19, 2018 https://www.vox.com/2018/7/19/17594156/whatsapp-limit-forwarding-fake-news-violence-india-myanmar

- USA examples

C-SPAN's viral video moment, Hadas Gold, 6/22/2016 https://www.politico.com/story/2016/06/cspan-house-sitin-democrats-224696 US Congress members livestream a sit-in demanding a vote on gun-control legislation.

image_1605451879726.png
Image not found or type unknown

Planning mobile communications for actions/organising [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

The following are guiding considerations for groups who are organizing and participating in actions and relying on Messaging Apps. Using this guide, you can facilitate discussions to support groups in considering the kinds of communications they are having and to design group management, message and device protocols that meet the safety needs for that communication.

This activity has 3 stages:

- Mapping communications & Assessing risks
- Planning: Design groups and settings
- Installing Apps (optional)
- Implementing (optional)

If groups have not yet chosen the messaging app they want to use, you may want to do the activity Discussion, input + hands-on: Choosing mobile apps

Learning objectives this activity responds to

- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

This activity is for participants with varied levels of experience in using mobile phones. If participants include individuals who will be group admins for messaging groups, plan to implement the designs in the workshop.

Time required

This activity will require about **60 minutes** to map and design and up to **3 hours** if you will be installing messaging apps, mapping and designing, and implementing.

Resources needed for this activity

- Paper for people to draw and complete the Mapping chart

Mechanics

Mapping communications and assessing risk

Consideration: Privacy

Consider that you may have different types of messages to communicate via signal and that some messages can be more public than others. Map the kinds of communications you have and design groups to match your privacy considerations.

What kinds of communication are you doing and what considerations do you have around who has access to communication? Suggest that participants consider these different groups. Ask them if they have more types of information -- for example, is there information that only 2 people should

know, that only one person should know and document and not share?

WHO	EXAMPLE COMMUNICATIONS
1 needs to be kept among a very small circle of people who know each other	*location of lead organizers*

2 is vital for volunteers to know or for small groups to coordinate around	*changes in crowd location*
3 can be shared openly	*rally start time, groups who endorse this action publicly*

PLAN: Design groups and settings

Work with participants to design groups to correspond with the different types of communication.

Guiding suggestions around group design: We suggest starting from these design questions. We have included example suggestions for group management and settings for some common types of

groups. Ask the participants what about this will work and what will not, facilitate the group in modifying the designs to respond to parts that do not work.

Membership

- WHO - Who can join this group?
- HOW - How do people join this group? What is the procedure? Do they need to be vetted, introduced, do they opt-in or sign up?
- ACKNOWLEDGEMENT - How does the group acknowledge when a person joins? Why would you want the group to do this or not?
- COMPLIANCE - What do you do if someone joins without following procedure?
- PERSONAL INFORMATION - with the messaging service you are using, can members of a group can see numbers of other members of a group? If so, for anyone who needs their number to not be known as part of the organizing, they should not join any large groups where the other people don't already know their number and that they do this work.

VERIFICATION: Know who you are talking with

For a type of communication, how will you verify who you are talking to?

- FACE-TO-FACE - will you require that any group member meets the rest of the group face to face in order to join? can a person just be added and vouched for by a member of the group
- SAFETY #s - VERIFY that your Messages are reaching the correct devices. If you are using Signal or Whatsapp, VERIFY SAFETY NUMBERS
- SAFETY WORDS - VERIFY that your calls are reaching the correct devices. If you are using Signal for calls, SPEAK THE SAFETY WORDS to one another. If you are using another calling application, do you want to have a way to check in at the start of a call to verify that a person is who you intended and speaking freely?

Message security - settings

Discuss, based on the sensitivity of the information you are communicating, what agreements do you want to make about how people are using message settings?

- DELETE Messages - How long should group members keep chat logs on their devices?

- DISAPPEAR Messages - In a Signal chat, you can set how long messages will remain before being automatically deleted. Do you want to use this feature? How and why?
- HIDE Messages on your home screen - Set Messaging apps to not preview on your home screen so that if you lose control of your device, people cannot just look at your home screen to see message content
- CODES - For extremely sensitive information, we suggest establishing code words before planning and action. For example, you might substitute words "We're ready for the tea party" instead of "Ready for the protest!"

Common group design templates

1. Small very strictly verified groups for sensitive information

Consideration/Risk: That people will join groups who you don't know and don't want to have access to information that is not okay going public.

- If you have sensitive information that needs to be shared only between a set of known people,
- Very small group, 8 or less, everyone knows each other and has met face to face;
- Only add people when you are face to face;
- VERIFY Identity (on Signal, verify Safety Numbers) in person;
- If anyone's safety numbers change, re-verify in person.
- Don't say more than you need to, don't take unnecessary risks
- DELETE

2. Pods - small groups

Consideration/Risk: That people will join the group and send information that is not useful or intentionally incorrect.

- This manages for the risk of individuals spamming the large group and making it unusable and too noisy;
- 2-20 people, whatever it takes to keep chatter down and have a manageable number of Signal Pods;

- A large group may have multiple pods to keep communication manageable and relevant;
- Pods are connected to one another so that information can flow between. You might consider having one point-person in each pod so they can push information that everyone needs to have;

3. Open group, public Information

Consider information on this channel to be public information in real-time. While information from any of the other groups could be leaked or shared outside of the group, this is a group that you automatically consider to be public.

- If you have any information to share that can be made public, use this!

Device security

If your device is taken, prevent others from pretending to be you and reading your information like signal messages, contact book, email etc. For more detailed facilitation guidance around device security, see the activity: Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft

- Set your lock to immediate/trigger with any button
- Set a strong password
- Encrypt your phone
- Encrypt your SIM card

Power and service

What if people can't use SIGNAL or your chosen App, Phones, Internet, for any reason - power, busy network, shutdown etc. Do you have backup or redundant internet access - a portable wifi hotspot for instance (if it uses cellular data that would also go down)? Is there an offline plan? Will your hub have a power-charging station for volunteers?

Additional resources

- About how to Verify Safety #s and Safety Words - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/

image-1605452256072.png
Image not found or type unknown

Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

In this activity, we plan and prepare for situations where participants and their phones may be at physical risk. Scenarios may include:

- Safety when participating in protests
- Safety at border crossings
- Safety when there is threat of arrest and seizure
- Safety when there is risk of theft and harassment

This activity has 4 stages with optional hands-on activities with installing and preparing devices. The stages include:

- Current practices in caring for ourselves
- Planning and preparing our devices
- Inputs – Optional

Optionally, follow this activity with hands-on exercises to practice the strategies and tactics.

Learning objectives this activity responds to

- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- an understanding of basic concepts of how mobile communications work in order to better understand the risks of mobile communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

This activity is for participants with varied levels of experience in using mobile phones to practice tactical safety with a focus on care and mobile phones.

Time required

This activity will require about **80 minutes**.

Resources needed for this activity

- flip chart paper + markers to document group discussion

Mechanics

This exercise is designed to support activists who are planning to engage in risky situations with their mobile phones. In the end, they will have a map of tools and tactics they can use.

Current practices in caring for ourselves – 20 minutes

> ***Care note**: This activity is a tactical activity to plan and prepare for using mobile phones in situations where people and their devices are at risk. Begin by acknowledging that to prepare for a risky situation, we need to consider first how we care for ourselves before, during and after.*

Begin with grounding and discussion about how people care for themselves in high risk situations.

Ask each individual to begin by working on their own. Hand out paper and ask them to consider these questions and to write their answers:

- What situations do you engage in where you will need to consider the physical safety of yourself and your mobile phone?
- What are you already doing to care for yourself – before, during and after these experiences?

Ask participants to divide their paper in 3 sections: before, during and after. Their paper will look something like this:

Participants' Paper Example		
BEFORE	**DURING**	**AFTER**

As a full group, invite participants to share their practices. Write these on a white board or piece of paper visible to the full group. Leave this up in a place that is visible. Ask people to share practices they do as individuals and with others.

Participants will continue to use this simple method for organizing practices in the next part of the workshop.

Planning and preparing our devices - 45 minutes

If you are working with participants to prepare for a specific event, it is best to work with the actual event. The following are scenarios that you might use in case workshop participants are not preparing for a specific event or your group needs more grounding for any reason. These are examples and we invite you to take these and make them your own.

Scenario 1: Safety when participating in protests

You are about to attend a mass protest. You need to be able to keep the data in your phone safe and to keep yourself from being tracked in the protest, but also be able to use your phone to contact allies for emergency purposes. You are also thinking of using your phone to document the protest and any possible human rights violations that will happen there.

Scenario 2: Safety at (unsafe) border crossings

You are in transit, and are about to cross a border into an unsafe location. You want to be able to use your phone to keep contact with your allies, but not as a personal tracking device. Ask people what their strategies are when they know someone else may have access to their phone. Examples of situations might include border crossings, flight boarding, going to a street protest.

Scenario 3: Safety when there is threat of arrest or seizure

You have heard from a reliable contact that you are being targeted by the state for arrest and seizure of devices because of your activism.

Scenario 4: Safety when there is risk of theft and harassment

You are concerned that someone may steal your phone and use the content to harass you.

Ask participants to document their discussions on paper and to divide their paper in 3 sections: before, during and after. Their paper will look something like this:

Participants' Paper Example		
BEFORE	DURING	AFTER

In small groups, facilitate participants to work through the following sets of questions.

How are people impacted: In this scenario/the event or experience you are preparing for, what are the risks? Who is impacted by this? Consider yourself, people who are on your phone in some way, your organizing/the issue you are working on (if applicable).

You can use the following questions as guiding questions for groups to consider how to reduce the impacts on people from a tactical perspective.

Before: Think about what you will do to prepare your mobile phone for this scenario.

- What files will you delete from your phone? Why?
- What applications will you install? Why?
- Who will you inform about your plans? Do you want to set up a check in system for before and after the experience, is that possible?
- What secure communications set-up will you have with others?
- What other strategies will you and your allies have in place to keep yourselves safe during this experience?
- Location services: Is it safer for you to have location and tracking on or off? Do you want other trusted people to be able to follow your location?
- Remote wipe: Do you want to activate remote deletion in case you lose access to your device?

During: Think about how you will use your phone during the scenario.

- Power: Is power a concern? How will you ensure that people's mobile phones have charge?
- Service: Is service a concern? What will you do if people cannot use their mobile service, apps, or data? Is there an offline plan?
- Who do you want to communicate with during this scenario? How will you communicate with them?
- Are you documenting the protest? If so, are you using any special app for it?
- Who will be able to contact you through your mobile phone?
- Who will you be contacting through your mobile phone?
- If you will need to use a SIM card different from your regular SIM card, how will you choose your carrier? Is there one that is safer than others for your communication? Who will be able to contact you? Who will you contact?

After: Think about what you will do after the scenario.

- Media: If applicable, what will you do with the footage, pictures, audio and other media that you gathered?
- Metadata and records that your mobile makes: What considerations do you need to take about the data your phone is creating during this scenario, consider metadata, records of communication, location of your device.
- In case of seizure: How will you know if you have a spy-ware free phone?
- In case of theft or seizure: What will you do to regain the integrity and safety of your mobile phone?

Give the groups a minimum of 30 minutes to a maximum of 45 minutes to come up with plans, strategies and tactics.

At the end of the group discussion, ask the groups to talk about their plans, strategies and tactics.

Use the results of the report-back to plan your hands-on for mobile safety.

Input (optional) - 15 minutes

Notes for trainer/facilitator Depending on your style and your participants, you may want to deepen and add inputs as groups debrief or as a planned input section. The following are notes that we believe may be useful as you plan this.

Before

- Let people know you will be in a situation where you are concerned about yourself and your personal belongings. Make plans to check in with your trusted friend as you enter and exit this situation. Choose a frequency of checking in that fits the risks you are facing.
- For a very high risk situation: We recommend planning to be in touch as frequently as every 10 minutes. For example, if you are going to be at a high-risk protest or doing a particularly risky border crossing. Plan to communicate every 10 minutes on your approach, while you wait (if possible), and upon crossing.
- For less risky situations: For example you are in a town working with a group of sex workers. You are traveling to and from meetings throughout the day. Make a plan to check in with your trusted partner when you are on your way and when you arrive at each meeting. Check in when you are going to bed, a simple “going to bed” and when you wake up “starting the day.”
- Clean it: What is on your device that you may want to keep private?
- Log out: Log out of any services that you don't need to be logged into. Don't stay logged into services you don't have to be logged into. If someone takes your phone, they will be able to access your accounts, see your activity, act as you on the service if you are logged in.
- Lock and encrypt: You can encrypt your phone, SD card, and SIM card, locking each with its own PIN will mean that if someone else has it, they won't be able to access the information on it or use it on the network without your PIN. *If you are in a situation where you are being threatened for your access information, you may not be able to keep the PINs and passwords private. Discuss with others and consider this as you make your safety plans.*
- Device Copying: Many law enforcement agencies have access to equipment to copy digital devices including mobile phones, laptops, hard drives. If your phone is copied and is encrypted, the person who copied it will need your password to decrypt it. If your phone is not encrypted, the person who copied your phone can access all content via the copy of the phone.

- Be quiet: turn off notification sounds and graphics, keep it on mute
- Remote wipe: You may or may not want to enable remote wipe. In some situations, you may want to prepare for remote wipe and ensure that you and a trusted colleague have the ability to remotely delete the content of your phone if someone has taken it or you have lost it.
- SIM cards and devices: Our mobile phones are devices that create and broadcast a lot of information, from messages and calls that we make and send, to data sent to apps, to location and time stamps communicated frequently with mobile phone carriers. Assess if you want to carry your personal device into a risky situation. If you do, this device may be linked to you by opponents and tracked ongoing. You may instead, choose to leave your device at home or to use a “burner” device, a device that you intend to use only for this action or event, that you expect will be linked to your activity during the action or event, and that you can and will discard afterwards. Note, you will need to have both a phone and SIM card in order for this to work. Both your phone and the SIM have an ID. If you use your regular phone and a burner SIM, and replace your regular SIM after the action, you will still be known by the ID of your phone. *This is an expensive option and keeping a phone and SIM from being tracked to you will take a lot of planning and the ability to stop using and destroy the device. If you are unable to discard the device, you might still think of carrying an alternative phone into risky situations, but the more you use it, the more easily it will be linked to you.*
- Removing SIM cards: If you find yourself entering a risky situation without having planned, you may want to remove sensitive parts of your phone like your SIM card and memory card (if possible). *Note: in some situations this may be used as an excuse by aggressors to escalate harm.*

During

- Remote wipe
- PixelKnot for encrypted messaging
- Firechat for protests and network shutdowns

After your phone has been out of your control

- Clean it or get a new device: Our best recommendation is to factory reinstall. If you can afford it, replace the device; do not reset your first device, instead send it to someone

who can analyze it.

- Your services: Reset passwords to all of your services.
- Let people know: If your phone has been out of your control, let your contacts and people you had active communications with know and what the implications may be for them.

Additional resources

- EFF Surveillance Self Defense - Encrypt your iPhone - https://ssd.eff.org/en/module/how-encrypt-your-iphone
- EFF Surveillance Self Defense - Using Signal on an iPhone - https://ssd.eff.org/en/module/how-use-signal-ios
- EFF Surveillance Self Defense - Using Signal on an Android - https://ssd.eff.org/en/module/how-use-signal-android
- EFF Surveillance Self Defense - Using Whatsapp on an iPhone - https://ssd.eff.org/en/module/how-use-whatsapp-ios
- EFF Surveillance Self Defense - Using Whatsapp on an Android - https://ssd.eff.org/en/module/how-use-whatsapp-android

image_1605451259399.png
Image not found or type unknown

Discussion, input + hands-on: Choosing mobile apps [tactical activity]

tactical_activ_circular_200px-withte



This is discussion and input activity that will focus on enabling the participants to choose mobile apps for themselves, especially after the workshop.

This activity has 3 stages:

- Discussion: What are you using and why?
- Input: Best practices for choosing apps
- Hands-on Activity: Assessing Messaging Apps **OR** Hands-on Activity: Assessing Popular Apps

Learning objective this activity responds to

- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

This session may apply to anyone who has ever used a mobile phone, and wants to have a better handle on how to choose apps.

> **Intersectionality flag:** this activity is designed as practice with assessing safety of mobile apps, specifically messaging apps. Other types of apps that may be more relevant for your participants might include the following:

- menstrual/fertility apps and the data they collect and birth control solutions they might offer
- dating apps
- messaging apps, and immediate erasure /flash apps
- safety apps, esp. for women and what they reveal, what can be turned on and off, if there is remote access,
- gaming or other apps with interactive component
- performative apps like tiktok

Time required

This requires about **60 minutes.**

Resources needed for this activity

- paper for small groups to write notes
- White board or large paper for recording shared notes
- some mobile phones with data and app store capability

Mechanics

Discussion: What are you using and why? - 10 minutes

In plenary, ask: What are 5 apps you use the most? What do you use them for? Get everyone to contribute to the discussion.

- list down the apps as participants mention them, ask who else uses the apps and mark down the # of users of the app in the room
- list down their reason for using the app

Then ask: How did you choose them?

- write down the responses to how they choose the apps and

To synthesise, summarise the reasons and go into the input.

Input: Best practices for choosing apps - 5 minutes

- Research! Learn about options, learn about which is a trustworthy app. Ask participants to share their methods of research – you could read about it somewhere online/offlline, ask a friend who you know likes to research. Read positive and negative comments in the download center.
- How do you begin to make sure that it´s a secure app? Who develops it? What is their privacy policy? Is it open source? Has there been incidents of the app being used to get access to systems?
- Understanding the permissions that apps require. For example, why might a game app need access to your camera or contacts?
- What makes you feel more secure/confident using the app – can you control the permissions? Do you know where it stores information about you or that you generate with the app? / Do you know where stuff goes?
- If this is a social app, how do you want to engage with people on this app? What can you choose about who you are visible to, what is visible to people, how people can interact with you and you can interact with them? What are the default settings, what do they reveal about yourself, who do they connect you to? Do you know of any safety issues on this tool? Are there reporting mechanisms that you can use? That could be used against you?

Hands-on activity: Assessing popular apps - 15 minutes

Go into the app store and try to find an app that does something common in the context. In an urban setting, maybe a taxi-hailing app, subway system map etc.

How do you choose? Look into (1) what permissions does it ask for (2) who is distributing the app and who manages and owns the service. There are a lot of apps out there that are copies of popular apps, made to look like something you want like a game or a subway map and they are actually designed to do other things like send your location to someone else. The developer or company that is distributing the app will be named in the app store. Share what you know about who owns the app/runs the service and research to assess ways in which the values may be similar and different from yours and how that may impact your privacy and safety while using the app. If you are choosing between multiple apps that appear the same, look elsewhere online for more information about the app and who is the developer or company distributing it and double check that you are downloading this one.

Activity: Assessing messaging apps - 30 minutes

Break into small groups. In small groups:

- Identify 2-3 apps that your small group are using for messaging
- Answer the guiding questions

In plenary: Share back, each group share one app until you have shared all of them.

Guiding questions:

- Who, among participants, uses it? Is it easy to use?
- Who owns it? Who runs the service?
- Where are your messages stored?
- Is it encrypted? What other safety and security settings does it have? What other ways do you keep your communication safe when using this app?

- When is it good to use?
- When is it not good to use?

List of messaging apps and considerations

SMS

- Everyone uses SMS
- Mobile company. Particularly risky if there is history of collusion between telco and government, or it´s a government-owned telco or if the company is corrupt.
- Stored by the mobile company -- different retention policies. Messages transmitted to towers between you and the person you are sending the messages through. (to?)
- No encryption.
- Good for communication of topics that are not risky.
- Frequently a cost per message.

Calls

- Everyone uses it
- Mobile company has control over it.
- Stored in mobile company -- metadata, for sure.
- Example of insecurity: Hello, Garcie! Incident in the Philippines where a phone call between the ex-president, Arroyo, and the head of the Commission on Elections, was intercepted, witnessing the president telling the COMELEC head how much lead she wants in the next elections.
- Good for communications that are not risky.
- Frequently a cost per call.

Facebook Messenger

- Anyone with a FB account can use it.
- Comes with its own app
- Encryption promised but not verified
- Facebook owns it
- Instead of using the FB app, use Chat Secure instead. You can use your FB credentials to chat with other FB users. But for encryption to work, the people you are chatting with also need to be using Chat Secure and communicating with you via Chat Secure.

- Frequently free, otherwise requires an internet or paid data connection.

GoogleTalk

- Anyone with a Google account
- Comes with its own app
- Encryption promised, not verified
- Google owns it
- You can use Chat Secure for this as well.

Signal (recommended app)

- Run by tech activists
- End-to-end encryption
- No cloud storage. You store messages on your phone or on your computer, Signal does not store messages after they have been delivered.
- Also has encrypted calls
- Used for sensitive communications

Telegram

- Popular messaging app
- End-to-end encryption only for secret chats

WhatsApp

- Lots of users
- Facebook owns WhatsApp although the WhatsApp developers promise to safeguard users´ privacy in their Privacy Policy
- Only stores undelivered messages. (what only stores undelivered messages, the whatsapp server?)
- End-to-end encryption, but if messages are backed up to your associated email, they are stored unencrypted.
- Good for communicating with a lot of people
- Still some concern about FB ownership

Wire

- End-to-end encryption promised, in the process of verification
- Developed by former Skype developers -- of note because Skype once had backdoors for the Chinese government that they built in collusion with that government
- Has encrypted voice calls

Additional resources

- What is encryption - https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- MyShadow - Alternative Chat apps: https://myshadow.org/alternative-chat-apps
- Why Signal and not Whatsapp
- EFF's Tips, Tools and How-tos for Safer Online Communications - https://ssd.eff.org/en
- It's also a good idea to do a web search about the latest security issues with the apps that you plan on training in. Key words to use are: name of app + security review + year, or name of app + known security issues + year. Depending on what you find, you might want to remove an app with known and un-solved security issues from your training.

image-1605451879726.png
Image not found or type unknown

Using mobiles for documenting violence: Planning and practicing [tactical activity]

This is a tactical activity for activists intending to use their mobile phones to document violence.

About this learning activity

tactical_activ_circular_200px-withte

Image not found or type unknown

This is a **tactical activity** for activists intending to use their mobile phones to document violence. Participants will practice doing a safety assessment and making a documentation plan. Participants will then work hands-on with their mobile phones to practice documenting using their apps and tools of choice.

> ***Care note:*** *Facilitators, this is a long activity and may take most of a day. Be sure to take breaks as you go through this. Acknowledge that the act of documenting is stressful and encourage your participants to share exercises that they find helpful when they are documenting for example breathing and motion exercises.*

This activity has 2 parts:

Part 1: Assess and plan

Participants will first plan their work, assessing safety issues and the wellbeing of those involved and will make safety plans and decisions about managing mobile phones and media based on this assessment.

Part 2: Setup and practice

Following this, participants will practice tactics for documenting violence using mobile phones.

We recommend also using the Deepening discussion about mobiles for documenting violence and tactical Back it up, lock it, delete it.

Learning objectives this activity responds to

- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements

Who is this activity for?

Groups who are currently or considering using mobiles to document violence.

Time required

This activity will require about **1 hour 45 min**.

Resources needed for this activity

- Printed or linked case studies

Mechanics

Introduction - 5 minutes

Share some recent examples of movements using mobiles to document violence and ask participants to share examples of how they are using mobiles to document violence or to share documentation. Examples may include: documenting state violence, forwarding videos of violent acts, the implications of having possession of this kind of media.

Part 1: Assess and plan – 30 minutes

Facilitate participants to make small groups based on common situations in which they are documenting violence.

> ***Care note:*** *Facilitators, encourage participants to assess and plan for their own care needs. Documenting acts of violence can be activating and stressful for the documenters. Encourage participants to share how they are self-resourcing, how they are working with other activists to address the impacts of documenting.*

see also Back it up, lock it, delete it

Purpose and planning: Discuss the purpose of the documentation

- What are you documenting and why?
- What is the situation?
- What is the purpose of your documentation? If it is to be used as evidence, plan for evidentiary requirements. For more information, see WITNESS' Video as Evidence resources: https://vae.witness.org/video-as-evidence-field-guide/

Assessing risks and taking care: Discuss known and likely safety issues for the people documenting and being documented

- What are likely safety issues you will experience during this work? Are you likely to encounter police or antagonists?
- What about your context might change in ways that will impact your safety and how will you plan for this? Discuss some likely scenarios. Examples might include police and other

antagonists becoming more aggressive or violent. Responses might include continuing to document, increasing frequency of safety check-ins among your team, stopping the process of documenting.

- Who will be participating in the documentation (filming, support, communications, etc) and what support do they have and need?
- What do you know about safety issues – does anyone in our group feel more or less safe participating based on the content or the context of this documentation? What roles are they comfortable taking?
- What strategies will you and your allies have in place to keep yourselves safe during the documentation?
- What role does consent play in this documentation? Will you seek the consent of those you document and how will they consent to being filmed or documented? Will you seek the consent of those you document regarding sharing of that footage and documentation later?
- What are safety issues related to you possessing this footage? What are safety issues for people who appear in the footage? How will you take care of the footage once it is shot and is stored on your device, on secondary storage? Consider where you will store it, who has access, if storage is encrypted, when you will delete.
- How might you be impacted by documenting violence? What resources do you need as an individual to be well and grounded while doing this work? What resources could others provide? How will you and your team support each other in your individual resourcing needs and what can you do together to support each other?

Know your rights

- Where you are, what are your rights around documentation?
- How do these relate to the context of your documentation? Example questions you might ask - is it legal to film police, is public assembly legal?
- Are police allowed to search your devices?
- Do police search your devices or force people to delete media?

Preparing your device

- Are you using your personal mobile?
- What files will you delete from your phone? Why?

- What applications will you install or uninstall? Why?
- Location services: Is it safer for you to have location and tracking on or off? Do you have colleagues who should be able to follow your location?
- Do you want to activate remote wipe / deletion in case you lose access to your device?

Discussion: Why or why not, do you use your personal mobile for documenting violence?

Input

Use information from What is a phone? to explain how mobile phones are linked to the people using them, how identification works with real-time surveillance, how metadata about phone usage and media EXIF data can be used to identify you.

After

- Make a plan to come together to debrief. How did things go? What unexpected things occurred and how did your group respond? What still needs response? How are people feeling and who will participate in the next steps?
- Sharing – review your agreements about consent and sharing. Be sure to share these agreements with anyone else you will be working with to share the footage.

Discussion

What else do you want to do after documenting?

image-1605452256072.png
Image not found or type unknown

Part 2: Setup and practice - 60 minutes

Depending on the time available, you can do these activities together or break into smaller groups and participants join whichever groups suit their needs the most.

Recording tips and tricks

How to use photo, video, and/or audio recording to document violence

- Find the built-in tools on your phone for recording: photos, video, audio
- Practice using these tools, consider the tips on WITNESS's Filming with a mobile phone tip sheet (linked in resources below)
- Plan your shots, be selective
  - Capture Detail and Perspective: physically move closer to record more details and move back to show a wider perspective of events
  - Keep your shots steady: choose your shot and hold steady for at least 10 seconds, avoid zooming, use both hands and keep your elbows against your body for extra stability
  - Hold your phone horizontally to capture a wider angle
  - Get in close for good sound: be aware of loud noises that could drown out interviews
  - Be aware of lighting: record in a well-lit location and keep the sun and bright lights to your back

- If you have a lot of time, work in teams to plan documenting using these tools. Practice creating a piece of media.
- If you will be sharing on YouTube, consider using the subtitle feature: https://support.google.com/youtube/answer/2734796?hl=en
- Context and messaging. Plan your messaging. Where will you post this and what text will you post to accompany it? How will you link this to your larger objectives?

Recording phone calls

Input: This has proven useful for sex workers who were being threatened by authorities.

Using an app

You can install and use an app that allows you to record. This will require data for downloading, data for conducting the call as the app will use data and not the phone line and will take some planning ahead.

- Assess which app you would like to use and install it
  - Google Voice allows you to record incoming calls, not outgoing calls
  - Your mobile phone may have a built-in recording app

- Test with a partner
- Practice locating the media and saving it off your phone to a safe location where you can access it when you need it.

Using a recorder

If you are unable to or choose not to use an app for any reason, you could work with another person, using your phone on speakerphone and using a recording device or their phone to record from the call using their phone as a voice recorder. Some phones have a built in voice recording feature.

- Assess which tool or app you would like to use and install it
- Test with a partner. For best sound, get close and record in a location away from other loud sounds.
- Practice locating the media and saving it off your phone to a safe location where you can access it when you need it.

Screenshots

You can take screenshots of your phone to document textual harassment and violence.

- Choose an app to screenshot and practice:
  - On Android: a phone using Android version Ice Cream Sandwich, you can press the Volume Down and Power button at the same time, hold for a second, and your phone will take a screenshot that is saved to your gallery.
  - iPhone X, XS, XR: Press and hold the Side button on the right and click the Volume Up button at the same time and your phone will take a screenshot that is saved into your Albums in an album called Screenshots.
  - iPhone 8 and earlier: Press and hold the Power Button on the right side and click the Home Button at the same time. This will be saved into your Photos. Look for an album called Screenshots.
- Practice locating the media and saving it off your phone to a safe location where you can access it when you need it.

Notice, you will not be able to screenshot all apps. Some apps, like Signal, have a security setting that allows a user to prevent others from screenshotting specific conversations.

Documenting the events for internal records

As an incident is occurring, whether it is brief, long, one time or repeated, it is important to document information about the event. Whereas many of the other tactics are around documentation for public and social sharing, this may be mostly useful as an internal practice. Where is the event occurring, when, who is involved, what is happening. Keeping track of this information can be useful in reconstructing events, assessing and planning responses.

Live Streaming

Adapted from the WITNESS resource: Livestreaming Protests, written for activists in the USA

You are livestreaming at an event like a protest, rally, etc. Definitely use the Planning activities and Prepare activities. This may be a great way to show events that are unfolding and to engage people who are watching in supporting. There are also some elevated risks as there may be police presence and there may be police watching now or later to target activists.

- **Location:** Document your location intentionally. Film street signs, buildings, and landmarks to document your location. Also, consider how revealing your location in real-time relates to your own safety and the safety of those you are filming.
- **Identification of participants:** Will you be able to get the consent of those you are filming? How do you want and need to protect their identities? Consider not filming faces.
- **Identification of tactics:** This works both ways. You might unintentionally film the tactics of the activists in a way that negatively impacts them. At the same time, you may be able to document the tactics of police to better assess their formations and likely actions in the future.
- **Who to stream to:** What are your goals of livestreaming? Do you want to stream to a small trusted group first who can support you by recasting your media?
- **Work with a team:** Work together with others who can support you by engaging viewers in comments and discussion, can repost the media to multiple channels.
- **Have an ask:** Engage your viewers to act.
- **Your device:** Do you want to user your personal device? Whichever device you use, encrypt and password protect your device. Do not use your fingerprint.

Shareback - 10 minutes

- Ground the shareback in a conversation about why we document violence. Acknowledge that this work is stressful.
- Share any media that breakout groups created.
- Share any learnings, new tools and tips shared by participants.

Additional resources

- Video For Change Network: https://video4change.org/
- WITNESS - Filming in Teams: Protests, Demonstrations, Rallies - https://library.witness.org/product/filming-in-teams-protests-demonstrations-rallies/
- WITNESS - Filming with a Mobile Phone - https://library.witness.org/product/filming-with-a-mobile-phone/
- WITNESS - How-to Guide for Interviewing Survivors of Sexual and Gender-based Violence - https://blog.witness.org/2013/08/new-how-to-guide-for-interviewing-survivors-of-sexual-and-gender-based-violence/
- WITNESS - How to Livestream Protests (US) - https://library.witness.org/product/livestreaming-protests-usa/ and video https://www.youtube.com/watch?v=Tm4hgbVuPlk
- https://library.witness.org/product/video-metadata/
- UWAZI, https://www.uwazi.io/ - Uwazi is a free, open-source solution for organising, analysing and publishing your documents.

image-1605452256072.png
Image not found or type unknown

Reboot your online dating safety [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

This is a **tactical activity** in which participants share safety tips and tricks for online dating. Participants will work in small groups or pairs to update their own online dating profiles and practices. Participants will share their different needs and preferences around dating apps, privacy and security. Participants will share and practice different tactics for increasing the privacy of their dating app use.

> ***Intersectionality note:*** *Facilitators, make space for people to share how their online dating considerations and practices relate to their gender and sexuality. Among your participants, how do gender and sexuality related to the apps people are using to date? How do they relate to concerns about privacy and safety?*

This activity has 2 parts:

- Sharing online dating and safety tips and tricks
- Hand-on: Reboot your online dating safety

Learning objectives this activity responds to

- an understanding of how mobile access and communications are gendered and intimate;
- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

People who are using dating apps and want to use them more safely.

Time required

This activity will require about **2-2.5 hours**.

> **Facilitator note:** The exercises take about 2.5 hours and we recommend taking a few breaks as you work.

Resources needed for this activity

- Internet access
- Mobile phones to update dating profiles
- Flipchart or whiteboard

Mechanics

Sharing online dating and safety tips and tricks

Ice breaker - 5 minutes

- Who is using a dating app, which ones? How did you choose it and why?
- How do you already think about your safety and privacy and take care of it?

Safer dating – 30 minutes

Before getting into the apps and hands-on with devices, facilitate sharing of dating safety tips between participants.

Ask:

- What is safe behavior to you while using online dating apps?
- What do you consider when deciding to meet matches face-to-face?
- What are the strategies you have in ¨knowing¨ that it is safe to meet someone?
- Do you have back-up plans for when things go wrong? Check-in time for a friend? Or letting a friend know where you are going, who you are meeting, etc?

Write this on a flipchart or somewhere visible for participants.

Share the following additional safety tips and ask participants to share and add:

Dating app (safety tips)

- Make sure your photo will not give more information, especially your location, the school you are studying in
- Use a secured and separate email address
- Don’t use a user name similar with your other social media account name
- Use a photo which is different from your social media account profile pictures.
- Don’t use personal information
- Be careful and deliberate when writing your profile on the dating app
- Offline follow up: Meet the person in a public place when meeting in person for the first time. If possible, inform a friend/family member about your meeting location and timing.
- Set a password on your applications when possible
- Password protect and encrypt your device

New models for dating

Are there any features you especially like about existing dating apps that you can look for in newer apps?

What possibilities and features do newer apps offer? (i.e., red-flagging users with bad reputation, documenting scammers, sharing tips about selecting matches).

In what ways are you already connecting with your trusted friends and community members around online dating?

Hands-on: Reboot your online dating safety - 60-90 minutes

Start with lightly Doxxing Yourself – see what information is available about your name in your dating apps. Using the information on your dating app profile, look for yourself on other platforms. Try searching for your username or information you share in your profile. Reflect on what information about you that is available outside the dating you don´t want to the dating app folks to know. Based on that, re-do your profile.

In pairs, go through the Safety Tips and update your profile. Share with each other and support your partner to point out if there is identifying information or if they can change more elements to be less identifiable and meet their own safety goals.

Reboot your pix

Check and replace any images including your profile and other account photos if they do not meet the safety tips you want to follow. Consider removing identifying metadata and removing identifying information about other people in the images.

Reboot your text

Check and rewrite your text if you are revealing more information that you would like to, considering your safety. Work with a partner to rewrite this if you want!

Set up a secure separate email address.

Shareback - 10 minutes

How was that? What was surprising? What was easy? What was hard? What are you doing to do next?

Facilitators: Are participants interested in sexting? Check out the safer sexting module.

Additional resources

Privacidad y seguridad en contextos conservadores: las apps de citas para mujeres de la diversidad sexual. Steffania Paola: https://www.genderit.org/es/articles/edicion-especial-privacidad-y-seguridad-en-contextos-conservadores-las-apps-de-citas-para

Self-Doxxing: https://gendersec.tacticaltech.org/wiki/index.php/Step_1#Self-Doxing

Dating App Safety Resources

- Grindr - https://help.grindr.com/hc/en-us/articles/217955357-Safety-Tips
- Planet Romeo - https://www.planetromeo.com/en/care/online-dating/
- Tinder - https://www.gotinder.com/safety
- OKCupid - https://www.okcupid.com/legal/safety-tips
- Hornet - https://hornet.com/community/knowledge-base/tips-on-how-to-stay-safe/
- Scruff - http://www.scruff.com/gaytravel/advisories/

image-1605451879726.png
Image not found or type unknown

Safer sexting [tactical activity]

tactical_activ_circular_200px-withte
Image not found or type unknown

This is a **tactical activity** in which participants share and practice safer sexting tactics.

Learning objectives this activity responds to

- an understanding of how mobile access and communications are gendered and intimate;
- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

People who are sexting or interested in sexting and who want to discuss and practice safer sexting.

Time required

This activity will require about **2 hours**.

Resources needed for this activity

- Mobile data service
- Mobile phones

Mechanics

In pairs, discuss - 10 minutes

- Have you ever sexted? When was the first time you sexted? What were you using – landlines, notes, letters, postcards, online chat.
- How do you use your phone to sext? Apps, texting, voice, photo, video, etc, what do you like, what are pros and cons of these for you?
- What safety and privacy issues do you consider when you are sexting and what do you to to take care of your safety and privacy?

Full group shareback and strategy share - 35 minutes

Facilitate participants sharing of what is fun and pleasurable about sexting with phones.

> ***Intersectionality flag:*** *Is there social stigma around sexting and how do participants of different genders, sexualities, races, classes, ages, experience this stigma differently? How do participants address social disapproval?*

Discussion questions you might ask:

- What kinds of media do you like to use and which apps they like to use most. What do you like the most about this? What else do you wish you could do with the app, with media?
- What is the most fun you've had sexting and why?

Strategy share

Facilitator, prepare large pieces of paper with the following titles:

- Cumming to agreements
- The love we make, the data we share
- Apps and basic safety/device considerations:

- Wildcard

Facilitate a conversation with the guiding questions below. Make notes on the large paper with strategies shared by participants.

Cumming to agreements

- Make agreements with your sexting partners – what agreements do you want to make about saving, digital or in-person sharing?
- Have you ever negotiated sexting agreements with your partners, how do you do it?
- Breakups happen, how do you negotiate with your partners after a breakup about sexting? Do you keep yours, do they?

The love we make, the data we share

– information that goes with our photos and the stories it tells:

- Think if you want to share intimate images with your face visible
- Try to cover identifying features of your body, like tattoos, birthmarks etc.
- Use Exif editors to clear a photo's metadata, geotag etc.
- Use apps to blur out face, tattoos etc. (like Pixlr)

Apps and basic safety/device considerations

- Choose an app that offers privacy and security features like encryption, message deletion, and screen-shot blocking
- Use a secure messenger to sext so that you have control on the images and messages sent, and you can delete them if you want.
- *Jargon note: Self destruct* - We use snapchat and other "self-destruct" promised apps, but often these are not entirely destructed and people are able to access the images for later distribution.
- Set a password and encrypt your device
- Set a password on your applications
- Consider using a secure email address and alternative phone number for your app account (app safety, so not just selection of apps or things to do with your sexting apps maybe as a sub section?)

- Know how to delete and save
- Consider if your app is syncing and whether and how you want to sync and store sexts

Hands-on: Safer apps and image editing

Discussion about choosing sexting apps

What apps are participants using for sexting and why? What safety concerns do you have choosing an app and what safety features do you like about your app? What are you concerned about?

Use apps that are:

- Encrypted
- Password protectable
- Prevent saving and screenshots
- Where messages can be deleted

Assessing SMS and MMS. SMS and MMS do not offer any of these features. See Activity: What is a phone? How does mobile communication work? For more information SMS and MMS and surveillance.

Hands-on activities

Facilitator, this activity is an opportunity for participants to practice safety strategies recommended by contributing trainers to the FTX Safety Reboot. Select whatever activities are most appropriate for your context. Some others to consider:

- Encrypting and password protecting a device
- Removing identifying information from photos and mobiles
- Set up a secure separate email address and phone number

Share this list of tasks with participants and instruct them to practice these tips in small groups, using each other and the internet to answer questions.

Hands-on with images

- Practice taking photos without your face visible

- Try to cover identifying features of your body, like tattoos, birthmarks etc.
- Use Exif editors to clear a photo’s metadata, geotag etc.
- Use apps to blur out face, tattoos etc.

Hands-on with devices and apps

- Choose and install a secure app
- Set a password on your applications
- Know how to delete and save chats
- Know how to delete images from your device

Shareback - 10 minutes

How was that for you?

- What did you do?
- Prompt participants to share media if they are willing.
- What was hard, what was easy? What were you surprised about?
- Where did you look for information when you had questions?

Additional resources

Luchadoras' Sexting Workshop – moments of sexting like lead up, during, after. Storage and sharing, Shifting consent and consent in all these moment.

> **Trainers Notes** As deleting images from apps and devices is a bit more complicated, here are some specific instructions to support participants to “Know how to delete images from your device” (last updated May 2019): Knowing how to delete images from your device requires understanding how to do this in your app memory and also knowing the location of where your images are stored in your mobile phone. On IoS devices this more opaque as you don't have access to files aside from the apps where the files are created. This also depends on whether or not you are using the chat apps to take photos, or you are preparing photos in advance (using the mobile phone's camera app).

For Telegram users, click on the header of a conversation, then look for Photos and Videos, you can delete images from there. This will delete the images from the Telegram app but if you had saved those images on another folder in your device, you will have to use a File Manager to do delete those. You can also look at and explore shared files with a specific user or a group.

On Signal, click on the header of a conversation. You will see thumbnails of Shared media. You can delete from there. Again, this will only delete the images / shared media on Signal, and if you had saved it elsewhere on your device, there will be a copy there. This also applies to who are sexting with.

For Android users, using a File Manager Removing media and images on Telegram: go to Internal Storage, and look for the Telegram folder >> Telegram Images / Telegram Video / Telegram Documents / Telegram Audio. Then delete the files in those folders. For Signal, if you save an image / media to away from Signal you can choose where to save it. Other places where your pictures / media could be: Internal Storage >> Pictures. You will generally get a directories (folders) that store your photos. By default, saved images from Signal get saved here.

image-1605451879726.png
Image not found or type unknown