Creating safe online spaces

Facilitate learning and building capacity on creating safe online spaces, specifically for at-risk groups and individuals. We **highly recommend** 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

safe-spaces_compress.png

This module is about facilitating learning and building capacity on creating safe online spaces, specifically for at-risk groups and individuals. Through this module you can explore, through activities and discussions, the factors that affect the ability to create spaces where feminist and sexual rights activists and their communities can feel safe. We explore the meaning of such spaces for feminist and sexual rights activists.

Learning objectives

By the end of this module, the participants will:

- Define what they mean by safe/private online space.
- Come up with some strategies to create safe online spaces for themselves and their networks.
- Develop an understanding of privacy issues, and how privacy affects women and their lives.
- Gain an understanding of the privacy limitations of most social media.

image-1605451259399.png

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

We suggest starting this module with one of the Starter Activities: Unpacking "safe", The bubble, or Develop your internet dream place - in order for the participants to start exploring the concepts. If you want to be more specific, there are starter activities about consent and privacy (Photo social network), cloud storage and data privacy (The Cloud), and consent and device permissions (Visioning + discussion: Settings + permissions). Depending on your group's goals, these will help ground your group in concepts of safety and privacy.

You can use the Develop your internet dream place to **work with a group that needs to redesign an existing internet space or design a new one with values of safety and privacy**.

Then enhance the group´s grasp of the concepts with the Deepening Activities:

- Online safety "rules" is about articulating how the participants want to safeguard their online spaces, but also an opportunity to clarify the basic principles of online safety.
- Privacy, consent and safety is an open lecture-type activity where the concepts can be further deepened and clarified.

The Tactical Activities are practical hands-on sessions.

- Making online spaces safer is an activity to make the dream places real including addressing challenges of current design and policy of online spaces being at odds with the dream space visions. **If you want to get hands-on with online services, this activity provides guidance for analysizing the settings, policies and norms of spaces.** It is not a step-by-step guide to adjusting settings as they change too frequently.

- Alternative tools for networking and communications is relevant for participants who want to start moving away from proprietary, commercial and less secure platforms and tools.

Learning activities

Starter activities

image-1605640724450.png
Image not found or type unknown

- Unpacking "safe" - visioning exercise
- The bubble - visualisation exercise
- Develop your internet dream place
- Photo-social-network
- The cloud
- Visioning + discussion: Settings + permissions

Deepening activities

image-1605640735000.png
Image not found or type unknown

- Input + discussion: Privacy, consent and safety
- Input + activity: Online safety ¨rules¨

Tactical activities

image-1605640743110.png
Image not found or type unknown

- Making online spaces safer
- Alternative tools for networking and communications

Resources | Links | Further reading

Jac's social media and security slide deck

image-1605452256072.png
Image not found or type unknown

Unpacking "safe" - visioning exercise [starter activity]

image-1605640366569.png

Image not found for type unknown

This is a visioning exercise. The main purpose of the exercise is for participants to express their own definitions of a safe space and look for shared understanding of a safe space. A group might use this as a first exercise in designing new online spaces together or in redesigning an existing one with shared values of safety in mind.

This activity would work well as an ice breaker and as a way of grounding our ideas about safe online spaces in our experience of safe physical spaces.

This activity has three stages:

- Individual visualising time which can be done with words or in drawing.
- Small group discussion about "safe".
- Full group reflection to discuss and identify shared and divergent definitions of "safe" within the group.

It is highly suggested that this activity is followed by Input + Discussion: Privacy, Consent and Safety.

Learning objectives this activity responds to

- Define what they mean by safe/private online space.

Who is this activity for?

This activity can be used with participants with different levels of experience with both online spaces and creating safe spaces.

Time required

This activity will require about **40 minutes.**

Resources needed for this activity

- Flip chart paper
- Markers
- Printer-size paper if participants are drawing.

Mechanics

Individual visualisation: 10 minutes

Ask your participants to close their eyes and think about a specific place/time/circumstance in which they felt the safest. Encourage them to be specific in their visualisation – not in terms of the place/time/circumstance, but in thinking about the factors that made them feel safe. This could also be an imaginary place/time/circumstance.

Option: Drawing

This can also be a visualising exercise where you ask participants to draw the place/time/circumstance in which they feel the safest, including the elements and factors that made them feel safe.

Small group discussion: 15 minutes

In small groups of three to five people each, ask participants to share with one another what they have visualised.

Note: For a workshop with six or fewer participants, you can facilitate both discussion steps as a full group. The purpose of using small groups is to ensure that each participant has time to speak about what they have visualised.

Full group: 15 minutes

To process, write "SAFE" in the middle of a sheet of flip chart paper and "mind map" the question: "What was it about the place/time/circumstance that made you feel safe?"

At the end of the exercise, you will have come up with a list of words, phrases and concepts that define "safe".

Notes for the trainer/facilitator

- Look for commonalities in participants' responses but also interrogate differences in their responses.
- Pay attention and highlight factors that can be applied to online spaces, or connect with the basic concepts above.
- Always synthesise key learnings from the activity to reinforce concepts.

Suggested tweak

- Instead of just using a flip chart to mind map the word "SAFE", you can have a co-trainer/facilitator note the words and concepts that the participants are expressing on a notepad or Word document, and as the discussion ends, use a word cloud generator to graphically show the words that define "SAFE".

image-1605451879726.png
Image not found or type unknown

The bubble - visualisation exercise [starter activity]

image-1605640366569.png

Image not found for type unknown

This is a visualising exercise. The purpose of this exercise is to facilitate discussion about privacy and for the trainer and participants to understand varying concerns about privacy in the room.

This activity is not meant to deepen awareness of privacy, but rather have the participants reflecting on their individual notions of privacy.

This activity should be paired with either Making Online Spaces Safer or Input + Discussion: Privacy, Consent and Safety.

Learning objectives this activity responds to

- Develop an understanding of privacy issues, and how privacy affects women and their lives.

Who is this activity for?

This activity can be used with participants with different levels of experience with privacy issues online and offline.

Time required

This activity will require about **40 minutes.**

Resources needed for this activity

- Flip chart paper
- Markers
- Small-sized post it notes

Mechanics

This is a visualising exercise. Participants will be given flip chart paper and markers to draw.

Individual visualisation - 30 minutes

If your are comfortable, close your eyes. Imagine a dot of bright light. Is it still, is it moving? How does it move? Now, imagine a circle around this dot. And now imagine both are moving, and the dot remains in the circle the whole time. You are both yourself, the dot, and your boundaries, the circle. How does it feel to be in this? This is a visualization of you inside of boundaries that are safe for you.

First, ask participants to draw an avatar of themselves in a circle in the centre of the paper.

The circle represents their individual bubble of privacy.

There are things inside and outside of the bubble.

On post-it notes, one concept per note, ask them to put the things that they keep most private and people they share the most private things with inside their bubble, and to place things they consider public outside of their bubble.

These things could include:

- people that they share things with
- information about themselves
- feelings that they have
- their activities

A sample of what this could look like:

CircleExample1.png
Image not found or type unknown

After they do the first circle, ask them to draw another circle, and then re-arrange the post-its according the levels of sharing of information that they want to have among different people.

This could look like this:

CircleExample2.png
Image not found or type unknown

The lastly, ask them to draw another circle, closer to their avatar and think about the things that they would never share with anyone, and put those in that circle.

CircleExample3.png
Image box found of type unknown

Full Group Debrief - 25 minutes

To process, ask the participants about the exercise and the reflections/insights that they had as they were drawing.

Ask them how they decided who was inside and outside their bubbles, and about the proximity of those outside the bubble to their bubbles.

Reflect on how their individual bubbles relate to creating safe spaces for themselves – online and offline.

Some guide questions for the debrief:

- How did each participant group the people and things inside and outside their bubbles?
- Was there a need to have more than 3 bubbles? Why?
- What were their insights around the responsibilities that they deal with, the emotions/feelings they have, and the things that they want to express? Was there a difference? Did their drawings show that difference?
- Have any of the participants ever experienced being forced to take a person/an emotion/an issue out of their bubbles? How did that happen? How did they deal with it? Were they able to put those things back in their bubbles?
- Of the things in your images, which things do you communicate about and which people do you communicate with in online spaces? Discuss.

> **Facilitation Note:** Do not comment on the participants' bubbles and where their information/feelings/thoughts in. Do not encourage that kind of behaviour among the rest of the participants as well. Little things like gasping in surprise, raising an eyebrow, or laughing when some is sharing their bubble does not create a safe environment for the participants.

image-1605451259399.png
Image not found or type unknown

Develop your internet dream place [starter activity]

image-1605640366569.png
Image not found for type unknown

In this activity, participants consider elements of an online space where their community can thrive. Depending on the goals of the group and workshop, facilitators can prompt participants to consider possible activities and ways of being in online spaces.

This is a visioning exercise and can lead into a discussion about the online spaces where participants are most often and the possibilities and limitations of using these platforms in alignment with the ideal space they have envisioned.

Learning objective this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.

Who is this activity for?

This activity is for people who participate in online spaces. It may be a good activity for a group to address redesigning a space that is not currently serving the group, or for a group who is establishing new online spaces together.

Time required

Total suggested time for a standard workshop with 12-15 participants: **2.5 hours**

- 30 minutes for discussion on Why are we online? Why is it important to us?
- 45 minutes minutes for the group work
- 30 minutes for the presentations (4-5 groups at 5-6 minutes each)
- 45 minutes for debriefing and plenary discussion.

Resources needed for this activity

- Flip chart paper
- Markers

Mechanics

Discussion: Why are we online? Why is it important to us?

Because we will be looking at the many ways that the internet is not designed for our safety or privacy, ground this conversation in the reasons participants are online. If you are familiar with the group already, you may be able to give examples of the work they are doing online. If you are less familiar with the group, ask the participants for examples of things they are doing online that are significant to them.

Make space for discussion about different facets of people's lives.

Some guide questions for this discussion:

- What spaces do you use online? What for?
- What are the limitations of the spaces that you use? It would be a good idea to tackle this per platform.
- Have there been incidents when you felt unsafe in the spaces that you use? Again, tackle this per platform / tool.
- Are you using different spaces for different aspects of your lives? How? And how do you decide which ones to use for which.

> **Facilitation Note:** It is a good idea to stress the point that the internet dream space is for personal and political / activist work. So, depending on how the participants are responding to the guide questions, challenge them to think about their personal and their activist work and their use of the internet.

Write down the highlights of the discussion.

Small group activity

With the discussion in mind, form small groups (3–5 participants) to develop their internet dream place.

During the small group discussion, ask them to reflect upon and answer the following questions:

- What is it called?
- Why is this space significant?
- Who is it for? Who is it not for? How can you make sure?
- What kinds of things do people do in this space?
- What are the rules in this place?
- Who can join? Who cannot join?
- What will the space look like?
- How will people find each other in this place?
- What topics can people talk about in this place? What can they not talk about?
- Who has responsibility for managing the space?

Have the groups draw out this space as creatively as possible, and get them to prepare a creative presentation for the rest of the group.

Shareback

To process the presentations, have the other participants ask clarification questions after the presentations, and list down more strategic/ethical/substantive questions, and hold those off until after all the groups have presented their ideas.

Debrief

To end this learning activity, discuss the following:

- What are critical things to consider when designing safe spaces (go back to the insights from the Shareback).
- Safe for whom? Ourselves, but we are also part of others. So where are the potential moments where we have to care for our own safety as well as others and vice versa (you might want to check out Online Safety Rules for reference).
- What are some limitations to this online space? Can a space be totally “safe”? What may result in a shift in safety?
- In understanding #3, bring home the point that we need to understand who has control over the shaping of a space and how, how the space works, where the space is embedded within other spaces (link also between online and offline), and if safe spaces are important to us, how we can strategise/design them more consciously in our activism?

Notes for the facilitator

1. Ask questions around other considerations in creating safe online spaces:

1. Who are the ones that will threaten the safety of this space? Internally and externally? How can they protect the space?
2. Where are the spaces hosted (i.e. national laws have an impact on whether or not these spaces can even exist, as well as redress if the space is abused)?
3. Are there legal considerations in creating such a space for the target group?
4. What are the responsibilities and liabilities of social media platforms when things go wrong? What are they in reality? And what should they be? You might want to read up on the Manila Principles on Intermediary Liability.
5. What are the international and national human rights standards on privacy? What are the legal privacy considerations?

2. This could directly lead to an input/lecture on the principles of online safety, or a lecture on the privacy issues in social media.

image-1605451879726.png
Image not found or type unknown

Photo-social-network [starter activity]

image-1605640366569.png

Image not found for type unknown

This is a visualization activity. The purpose of this activity is to get participants thinking about online consent and data privacy through the medium of permissions and terms of services on the apps they use.

Learning objectives this activity responds to

- understand a feminist perspective in the digital space about
- meaningful / informed consent
- full control over personal data and information online

Who is this activity for?

This activity can be used with participants with different levels of experience with consent and privacy issues online and offline, preferably with access to a device with which they connect to the internet.

Time required

45 minutes, including set up and debrief.

Resources needed for this activity

- Flipchart with activity scenario written/printed on it
- Post-its
- Markers

Mechanics

This is a visualising exercise. Participants will be given post-its and markers to write.

Individual visualization - 15 minutes

First, read out the scenario from the flipchart as follows:

"Say you were the inventor / owner of a popular new photo-based social network (like Instagram). You make money by offering users the ability to advertise their posts to targeted users based on age, location, interest. To operate, you need access to the users' photo gallery. What permissions would you ask for, and what terms of service would you provide information about?"

You could ask the participants to reflect on the following aspects:

- Ownership and retention of the uploaded photos
- Access the users' photo gallery
- Using user data for advertising

Full Group Debrief - 25 minutes

To process, ask them about the exercise and reflections/insights that they have as they were writing.

Some guide questions for the debrief:

- What permissions would you ask for?
- What are some of the terms of services you would offer?
- Who would own the uploaded photos?
- Where would the uploaded photos be stored?
- How would you ask for consent to access the users' photo gallery?
- How would you use this data for advertising?
- Do you think there is a connection between how such online consent works and offline consent?

You can then reflect upon their responses and discuss them with the group.

image_1605452256072.png
Image not found or type unknown

The cloud [starter activity]

image-1605640366569.png
Image not found or type unknown

This is a visualization activity. The purpose of this activity is to facilitate discussion about cloud storage and data privacy. This activity is not meant to deepen awareness of privacy, but rather have the participants reflecting on their individual notions of privacy on the cloud.

Learning objectives this activity responds to

- to understand a feminist perspective in the digital space about full control over personal data and information online

Who is this activity for?

This activity can be used with participants with different levels of experience with privacy issues relating to the cloud.

Time required

45 minutes

Resources needed for this activity

- Sheets of blank A4 paper for drawing
- Markers

Mechanics

This is a visualization exercise on how the cloud works. Participants will be given paper and markers to draw.

Individual visualization - 15 minutes

Ask the participants to visualize the cloud as a physical space and draw the space on their papers. You could ask them to reflect on the following:

- How does the space look?
- Who is controlling this space?
- Can you see what is happening inside the space?
- Can you and your community audit/test the space?

Full Group Debrief - 25 minutes

To process, ask them about the exercise and reflections/insights that they had as they were drawing.

Some guide questions for the debrief are:

- How did each participant visualize the bubble to look like?
- Who was controlling the entrance to your space?
- Based on how much of the space was accessible to you, is your cloud proprietary or open-source?
- What would be the difference between proprietary and open-source cloud storage?
- Which kind of cloud storage would you prefer and why?

You can then reflect upon their responses and discuss them with the group.

image-1605451259399.png
Image not found or type unknown

Visioning + discussion: Settings + permissions [starter activity]

image-1605640366569.png
Image not found or type unknown

This is a visualising and discussion exercise. The purpose of this exercise is to facilitate discussion about online consent, device settings, and permissions. It can also help participants to understand varying concerns about consent on their personal devices.

Learning objectives this activity responds to

- Understand a feminist perspective in the digital space about
  - meaningful / informed consent
  - full control over personal data and information online
- to learn practices of control over one’s digital persona

Who is this activity for?

This activity can be used with participants with different levels of experience with consent and privacy issues online and offline, preferably with access to a device with which they connect to the internet.

Time required

This activity will require about 1.5 hours

Resources needed for this activity

- Post-its for writing
- Sheets of blank A4 paper for drawing
- Markers for writing and drawing

Mechanics

This is a visualizing and discussion exercise. Participants will be given post-its and markers to write and draw.

Individual Visualization - 30 minutes

First, ask participants which device they use to access the internet (mobiles, tablets, personal computers, desktop at work/home/other public spaces etc.). Then tell your participants to think of and write down on post-its the first three activities they consented on their mobile, regardless for which apps.

Following this, on sheets of blank paper, ask them to draw their mobile. Then ask them to identify which operative system their device uses. Finally, ask them to write down (in the drawing of the mobile outline) 5 apps they use the most, verify permissions granted to those apps, and write them down next to each of the applications.

Full Group Discussion - 1 hour

Once all participants have visualized these details, ask them to share with one another what they have visualized. Some apps (such as WhatsApp, Facebook, Twitter, Google Maps etc.) are commonly used by many people, so you may find commonalities in the responses. Look for commonalities in participant's responses but also interrogate differences in their responses.

> **Note:** If there are more than 6 participants, you can optionally make smaller groups of 6 each to ensure that each participant has time to speak about what they have visualized.

You can then facilitate the discussion with some questions such as:

- What device did you draw?
- Does your device connect to the internet?
- If your device is a phone, is it a feature phone or a smartphone?
- What Operating System does your device use? (example: Android, iOS, Windows etc.)
- Is your Operating System open source or closed source?
- What is your device’s manufacturer?

Before going into questions on settings and permissions, you can explain:

> "*Since smartphones offer even more functionality and options than feature phones, the amount of information that can be observed and logged is far greater. In addition, smartphone users are sharing that very detailed identifying information about themselves and their usage to far more companies than just their mobile network operator - every app you choose to install can also send selected data about your usage, call times, contacts, and data use to whomever makes that app.*
>
> *What an app can see and log is often set by the app designer, but there are very few laws and regulations constraining what they can design their app for. Similarly, the operating system and manufacturer of a smartphone has implications on where your data goes and who can see it aside from your mobile network operator.*" Source

Once this basic understanding has been established, you can lead to more detailed discussion on device settings and permissions. Some guide questions for the discussion:

- What are some features of your phone that your chosen apps can access? (example: camera, microphone, location etc.)
- Why do you think these apps require this information?
- Did you consent to this information being shared?
- Do you think there is a link between offline consent and such online consent?
- Where do you think this information goes?
- Do you think this information is protected?

You can refer to the following for some basic information to guide the discussion:

> "*Android devices share a massive amount of user data with Google, since their operating system is deeply entwined with a user's Google account. If you use Google services and apps as well as an Android-powered smartphone, Google knows an overwhelming amount of information about you – possibly more than you'd realize about yourself, since they log and analyze that data.*
>
> *Similarly, iPhones (using iOS as their operating system) provide a similar amount of information about users to Apple, which can be combined with a user's data if they use other Apple products and services. In addition, iPhone and Apple are highly proprietary and their software and hardware are closed source. This includes the iPhone itself, as well as the Apple apps that run on it; in comparison, Android is open source, which allows everyone to review their code and know what the Android does.*

Smartphones are able to use GPS (Global Positioning System) satellites in addition to the approximate location triangulation of mobile network towers can provide. This gives far more detailed location data to operators and to any apps who have access to that information. This more precise location can be attached, along with the date and other information, to any pieces of data that the phone collects to post online or store on its memory." Source

image-1605451879726.png
Image not found or type unknown

Input + discussion: Privacy, consent and safety [deepening activity]

This learning activity is about the trainer/facilitator giving input and facilitating a discussion on the issues relating to privacy, consent and safety.

About this learning activity

image-1605640472202.png
Image not found or type unknown

This learning activity is about the trainer/facilitator giving input and facilitating a discussion on the issues relating to privacy, consent and safety.

We suggest that you use this learning activity to cap the other learning activities such as: Unpacking "Safe" or The Bubble.

Learning objective this activity responds to

- Develop an understanding of privacy issues, and how privacy affects women and their lives.

Who is this activity for?

This activity can be used with participants with different levels of experience with both online space and creating safe spaces. Of course, if the participants have only a very basic understanding of feminist concepts such as agency and consent, then the trainer/facilitator will need to clarify those terms at the beginning of the input and discussion.

Time required

Minimum of 40 minutes.

Resources needed for this activity

- Flip chart paper or white board
- Markers

The trainer/facilitator can also opt to use a presentation for this activity.

Mechanics

If Unpacking "safe" or The bubble have already been done, use the insights from those activities to launch into defining privacy. Specifically:

- Draw from the the definitions of safety/safe that came from the activities that can be connected to privacy and consent issues.
- Key concepts raised during the prior learning activity that either need to be stressed/reiterated or further clarified (this is an opportunity to clarify notions/ideas that are against feminist values on privacy, consent and safety).
- Experiences shared in the prior activity that highlight the connections between privacy, consent and safety.

image-1605452256072.png
Image not found or type unknown

Unpacking consent and privacy

image-1605640472202.png
Image not found or type unknown

Key points to be raised in this input and discussion.

Unpacking "consent"

We tend to think of consent as a one-off thing. Like signing a piece of paper once and then it is set. However, from experience we know that consent is simple yet complex at the same time. Simple in its principle yet complex in its implications. Here are some things to discuss:

- Duration of consent.
- Ability to withdraw consent, what it means for a user to withdraw consent and their use of the platform or tool
- The data / information about the user that they cede when they consent to services
- How is that data used
- Conditions of consent – being able to consent only under certain circumstances and not others.

Watch the video Tea and Consent.

Show this graphic:

Everydayfeminism-consent.png
Image not found or type unknown
The facilitator can focus a few scenarios to highlight the points:

- Agreeing to the Terms of Service in proprietary, commercial platforms in order to be able to use that platform.
- Emergency scenarios where we consent to allow others to control our spaces / devices in order to safeguard it. How to we ensure that this conditional consent is temporary? Perhaps use the example of Facebook Trusted Friends as a way to highlight this point.
- Events that ask participants to sign-in at the door – what does that mean as far as consent goes?
- Sharing a password to a loved one as an act of intimacy and trust. What are the implications of this?
- Ask the participants for examples of situations where they had given their consent to different platforms or services.

Unpacking "privacy"

Key points for this input can include:

The different dimensions of privacy:

Territorial/spatial

- Why do we lock our doors? Which doors do we lock?
- How do we protect our spaces and why?
- Why do we close the door when we pee? When everyone does it?

Relational

- Do we protect the privacy of the people that we know? Who of them?
- Do we violate the privacy of our relatives, friends, colleagues when we talk about them?

Embodied

- Which parts of your body do you choose to disclose? When you pick what clothes to wear, and depending on who will see you (gaze as violation of privacy)?
- Embodiment online. Self-representation online. From simple things like user pics, to carefully crafted identities, to other kinds of information that reveals things about our bodies (health/medical/sexuality/gender). And how this also translates body as data.

Data privacy

- What data do we willingly cede about ourselves and others?
- Are we able to give consent to the collection, storage and aggregation of our data?
- How about the data about us that is collected, stored and aggregated without our consent?

Defining privacy

- Defining privacy as a fundamental human right, and why it is important for women.
- How privacy has been defined in policy (could be national, regional and international policy), and what that means for individuals, WHRDs and women.
- How privacy plays out on the internet: how social media has seemed to redefine privacy both in individual practice and the platform's use of users' data.
- How the internet – and how its being used and developed now – is challenging how we practise privacy.
- The relationship between privacy and consent.

Discussion questions

- When do we "forfeit" our right to privacy? For example: Does anonymity facilitate online harassment and GBV?
- How critical is the relationship between anonymity and privacy and safety?
- In the age of selfies and when people willingly cede information about themselves and others, is privacy dead?
- Technically, how would privacy-by-default work on the internet? What kind of changes would platforms like Facebook need to make to have privacy-by-default? (We could develop an activity around this in the future.)

Facilitator preparation notes

While this learning activity has the trainer/facilitator doing most of the speaking, it is also important to reiterate the safe, open and interactive space that all FTX workshops try to create. This can be

done by framing this activity with guidelines that allow participants to raise their hands to ask questions or to argue or to stress or clarify a point being made in the presentation. The other way to encourage interactivity during presentation-style learning activities is to "popcorn" topics – ask a question to the group to start a topic, and then use their answers to launch a presentation/input.

In order to prepare for this learning activity, the trainer/facilitator will need to brush up on the following:

- The state of play on privacy issues – policies, trends, recent cases.
- Context-based understanding of privacy: current laws in the location of the workshop or the participants, recent cases relevant to the participants.
- Feminist Principles of the Internet

Additional resources

- Feminist Principles of the Internet
- "Neutral" definition of Consent (Merriam-Webster)
- "Neutral" definition of Consent (Wikipedia)
- "Neutral" definition of privacy (Merriam-Webster)
- "Neutral" definition of privacy (Wikipedia)
- Privacy and EDRI
- Three key issues for a feminist internet: Access, agency and movements
- A feminist internet and its reflection on privacy, security, policy and violence against Women
- GISWatch 2015: Sexual rights and the internet & Full report
- GISWatch 2013: Women’s rights, gender and ICTs & Report
- How much control do we have over our data?
- Establishing a baseline of privacy and security knowledge
- What privacy & anonymity have to do with tech-related VAW
- Invasion of Privacy & The Murder of Qandeel Baloch - By Digital Rights Foundation
- Peeping Tom Porn and Privacy - By Rohini Lakshané
- Mapping and privacy: Interview with Privacy International's Gus Hosein
- The ability to say NO on the Internet

image-1605451879726.png
Image not found or type unknown

Input + activity: Online safety "rules" [deepening activity]

image-1605640472202.png
Image not found or type unknown

This learning activity is about sharing basic principles of online safety, and having the participants articulate personal or organisational policies to safeguard their online safety.

This activity can be done after Input + discussion: Privacy, consent and safety or Develop your internet dream place, and be the basis for Making online spaces safer.

There are three main parts to this learning activity:

- Input on the basic principles of online safety
- Reflection on communication practices
- Articulating "online safety rules".

Learning objective this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.

Who is this activity for?

Participants with differing levels of experience. However, note that participants with more experience with digital security might find this too basic.

Time required

105 minutes total (1 hour, 45 minutes):

- Input on Basic Principles of Online Safety (15 minutes)
- Activity on Communication Practices (30 minutes)
- Input on Areas of Consideration for Online Safety (20 minutes)
- Activity on Articulating "Online Safety Rules" (30 minutes)
- Debrief/Synthesis (10 minutes)

Resources needed for this activity

- Flip chart paper or white board
- Markers
- Printer paper

Mechanics

Start with listing down the **Basic Principles of Online Safety** (see Additional Resources)

> **Note:** It would be good to refer to examples that were shared in previous learning activities as you expound the principles.

Then move on to having the participants reflect on their communication practices by having them individually fill in this form (filled out a sample). To frame this, and to not conflate this activity, ask the participants to think about the last 24 hours and who they communicated with and what they communicated about.

Who do you communicate with	**What topics you communicate about**	**Is the communication private?**	**Communication channels**
Mother	My current trip	Yes	Facebook messenger
Kartika	Details of current work	Yes	Email, Telegram, Facebook messenger
Lisa	Event with them next month	Yes	Email
Marina	Dinner with him next week	Yes	SMS
	About how Trump sucks	No	Facebook group
	Feminist principles of technology	No	Personal blog

> **Intersectionality Note:** The names on the table are suggested names. You can change those names to fit in more common names in your country or context.

The starting point can be the people they communicated with, or the topics they communicated about in the last 24 hours.

After getting the participants to fill in their individual forms, have them reflect on the following questions:

- Of the communications that they had done in the last 24 hours, which of these do they think they should be securing the most?
- Of the communications that they have done in the last 24 hours, which one causes the most stress? Why?

Then move on to presenting the Areas to consider in online safety (see Additional Resources).

After, ask the participants to reflect on the areas to consider and write down their personal "online safety rules" based on this template:

- Which topics that you communicate about are private, and which are public?
- Who do you communicate with, and what about?
- Who are you permitting to have access to your communication channels?
- Which communication channel or device are you limiting access of others to?

> **Note:** These rules are draft rules and are personal to each participant. It is important to frame this activity this way, and keep on reiterating the Basic Principles of Online Safety.

After the participants have written down their "online safety rules", debrief on the activity:

- Insights on your communication practices?
- Any concerns that were raised because of this activity?
- What else needs to be clarified?

It is suggested that you then move on to Making online spaces safer.

Facilitator preparation notes

You might want to read this piece from Level Up: Roles and responsibilities of a digital security trainer to mentally prepare for this activity.

Additional resources

Basic principles of online safety

- The idea of perfect online safety is false. The security and safety scenario is contextual – it changes over time. What is safe today may not be safe tomorrow.
- Online safety must always be end-to-end. You are only as secure as the least secure person you communicate with, or the least secure platform you use.
- Online safety will always entail a combination of strategies, behaviour and tools. Merely installing security apps does not equal being safe online, especially if you have un-secure communication practice and behaviour.

> **Facilitation Note:** These may seem sanctimonious and might cause participants to feel paranoid about their safety. One way to go about this, as a feminist trainer, is to give examples that are personal to you and your experience. This way, the participants will not see you as someone who will judge them for their communication and digital security choices.

Areas to consider in online safety

These are areas the participants should be considering when they think about their online safety.

Who you communicate with and what you communicate with them about

- What topics do you talk about with the different people you communicate with?
- Are any of the topics you communicate about sensitive? How so? What are they?
- Are any of the people you communicate with at risk? Have they experienced surveillance? Is the work that they are doing a threat to someone with power?
- Are you at risk? Have you experienced surveillance?

What you use to communicate

- What platforms do you use? Do you know where they are hosted?
- What devices do you have?
- Do you use different devices for different people? Do you differentiate devices based on the public or private nature of your communications?
- Who has access to these communication channels? Are they shared?

Your specific context, capacity and risk

- Are there laws in your country that threaten your online safety as an individual? What are they, and how do they do this?
- Have there been examples of cases where individuals in your context (define that as you will) have had their online safety compromised? How?
- Have you ever experienced surveillance? From whom?
- Search yourself. Is there any information there that you don't want out in the public? Why?
- How do you safeguard your communication channels? Do you have passwords for each device and communication channel?

image-1605451259399.png
Image not found or type unknown

Making online spaces safer [tactical activity]

The goal of this activity is to go through the privacy options for accounts and groups of the agreed-upon (i.e. commonly used in the group) social media sites.

If you want to get hands-on with online services, this activity provides guidance for analyzing the settings, policies, and norms of online spaces.

About this learning activity

tactical_activ_circular_200px-withte

Image not found or type unknown

The goal of this activity is to go through the privacy options for accounts and groups of the agreed-upon (i.e. commonly used in the group) social media sites. For groups who have gone through the exercise Develop Your Internet Dream Place, this is an activity to make the dream places real, including addressing challenges of current design and policy of online spaces being at odds with the dream space visions. For groups who already have online spaces and want to alter them to make them feel more safe, you can also use this activity.

If you want to get hands-on with online services, this activity provides guidance for analysing the settings, policies and norms of online spaces. It is not a step-by-step guide to adjusting settings, as they change too frequently.

Learning objectives this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.
- Gain an understanding of the privacy limitations of most social media.

Who is this activity for?

This activity can be used with participants with different levels of experience with both online spaces and creating safe spaces. Participants will be asked to explore and set privacy settings in the tools they are using.

Time required

This activity will require about **3 hours.**

Resources needed for this activity

- A soft-copy of the planning tables.
- Computers for people to work on their plans on

image_1605452256072.png
Image not found or type unknown

Mechanics

tactical_activ_circular_200px-withte
Image not found or type unknown

1. Map your space

Developing new spaces: If you have done Develop Your Internet Dream Place, you can use the work from that exercise as your map.

Redesigning existing spaces: If your group would rather redesign an existing online space, identify a space that the group already participates in or ask the participants to form groups based on spaces they participate in and facilitate the group(s) to answer the questions from Develop Your Internet Dream Place, about these existing spaces:

- What is it called?
- Why is this space significant?
- Who is it for? Who is it not for? How can you make sure?
- What kinds of things do people do in this space?
- What are the rules in this place?
- Who can join? Who cannot join?
- What will the space look like?

- How will people find each other in that place?
- What topics can people talk about in this place? What can they not talk about?
- Who has responsibility for managing the space?

Have the groups draw out this space as creatively as possible, and get them to prepare a creative presentation for the rest of the group.

2. Choosing spaces: Spaces that work and assessing safety

If you have done Input + activity: Online safety "rules", you may have already had a conversation about choosing spaces and assessing risks of online communications.

Choosing spaces for functionality

How do you choose platforms and assess risks to yourselves on those platforms? Choose spaces that help us reach our communication goals and try to participate in these spaces in ways that do not expose us to risks we do not wish to take.

Look at the map you have made. Can you identify a platform already that will allow you to create the space you have mapped? Which of the components of your space will be easy to create? Which will be difficult? Are there alternative spaces where pieces will be easier or harder?

Choosing spaces strategically

Does the space you chose match your strategy? Is this a good space for: organising, mobilising, for announcements/influencing discourse?

Facilitator: Introduce how these different activities bring with them different levels of risk.

Suggested questions to ask

- What are some risks with different types of communication?
- Who are you communicating with in these activities?
- Who are you not communicating with?
- What are the consequences if someone you do not intend your message for accesses it?
- How public can the audience be?
- What risks might people face if they are known as message creators or recipients in this communication?

This discussion leads into the next discussion section looking at risks people are most concerned with.

Note to facilitator: This section may be very quick, with everyone agreeing that they need to be on a single platform right now, for instance, Facebook. You may, however, get to talk about a variety of tools and platforms.

Discussion OR Input: Assessing dimensions of safety and the internet: What are the current issues?

Ask the group: What safety risks are you concerned about in online spaces? Facilitate this discussion to include concerns about actions that individuals can take in these spaces as well as actions taken by the software companies who own the spaces.

If you have already done Input + activity: Online safety "rules", you may reference that discussion and abbreviate this section.

Otherwise, facilitate discussion about safety risks in online spaces. Draw from the experiences of the participants but also prepare some examples of stories where privacy was breached through online spaces and that impact that had on individuals.

Discussion: Ask participants what safety concerns they have in online spaces. Are there any specific incidents or risks people are concerned about and want to address in their Dream Space or redesigned space?

Input: We suggest familiarising yourself with 2-3 case studies and sharing them here. To share these with the least amount of time, present them as a lecture. If you have more time, or want to facilitate deeper conversation and engagement with the issues, find some media like articles, short videos, interviews, regarding a case and share them with the group. Ask group members to discuss them together in pairs or small groups.

- Real name policies and their implications for organising and expression online.
- The myth that to be online is to be anonymous and therefore safe – laws and policies that don't allow for this.
- Women's experience of the internet – harassment, attacks, etc.
- The value of the internet; why do people stay in online space; how is it of value to us and our community?
- Diversity of access and comfort level of online spaces that we choose. Is it a barrier for people in our networks to participate because you´ve chosen a specifc platform?
- Are there cost implications for the space that you are choosing to use for the people in your network community?

Facilitator: ask participants to consider why the platforms we are on are not safer by design.

3. Make a plan: Address the risks of the spaces that you are using

Using the Dream Spaces or Redesigned Spaces as examples, have the participants make plans for implementing this space online.

This would be most useful if they have active spaces they want to secure and safeguard.

Issues to consider here:

- Privacy settings on social media – is it enough? What are the limitation of available settings?
- Considering moving to non-commercial spaces – what are the barriers?
- Safer options for online communications – tools that offer encryption by default.

Consideration	Platform or Space	How will you address this
Who can see what	Twitter (this is an example)	Review my privacy settings; consider content that I post, respond to, like, and the default privacy settings on different types of content; reduce the number people I'm linked to; prohibit tagging
Do you know everyone you're linked to		review my connections; remove connections to people I do not know;
Do you want to use your real name; anonymity and how hard it is		use a pseudonym; prevent others from naming you with your real name
Do you want to share your location		No, I do not want to automatically share my location; turn off location services; limit photo posts showing my location

Authorisation

Consideration	Platform or Space	How will you address this
Ensuring that I am logging out	f-book	do not save password in browser; review setting on f-book for automatic logout
2-factor on accounts and devices		set up 2-factor to be more certain that only I am logging in
Shared accounts		review who has access to shared accounts; review password policies on these accounts

Devices

Consideration	Platform or Space	How will you address this
Device-level safety	Twitter or any app	do not automatically log in to any apps or through browsers
Do I want notifications to show on my devices		turn off audio and visual notifications

Group Administration

If you are working with a group to implement a space online, use the following table of questions and work through the answers, finding the appropriate settings on the platform you are using to implement the group's preferences.

Example design/implementation table:

Link to Group or Personal Page	https://www.facebook.com/APCNews	**What are you doing to implement this?**
Who can see this space?	anyone on the internet	our group is public on Facebook and searchable on the web
Who is this space for?	APC members, community and potential APC members	we invite APC staff and network members to join, mention them in posts, invite them to events posted through this page
Who is it not for?	APC members, community and potential APC members	closed/public - we limit who can post, but make the page findable on facebook and through web searches
What kinds of things do people do in this space?	notifications about APC work and links to APC network content published elsewhere	
Who can create content in this space? What kind of content?	staff and members	-
How do you want to communicate the rules of the space?	on our group's about page	we will write our rules based on this chart of questions and answers and post it on our about page

Well-being Note: Bringing up risk and technology concepts might cause participants stress. Be aware of this. Pause for a breathing exercise. Or allow participants to take a walk around the venue to decompress when they need to.

Additional resources

- If you want to spend more time discussing tools and choices, there are a lot of great resources here: https://myshadow.org/.
- How to Increase Your Privacy on Twitter
- Security in a Box: Social networking
- Protect the privacy of your online communication
- Create and maintain strong passwords

image-1605451259399.png
Image not found or type unknown

Alternative tools for networking and communications [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

This learning activity is mostly guided hands-on for individuals and groups to start using alternative tools to "free" proprietary services.

This activity is most effective when the participants are part of the network so they are able to start developing new ways of communicating among each other.

This activity will focus on three communication tools that are commonly used: Email, chat apps, and alternatives to Google docs.

Learning objectives this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.

Who is this activity for?

This can be run with participants with varying skill levels in using online tools.

Time required

To complete this, you will probably need at least 5 hours.

Resources needed for this activity

- Internet connection
- Laptops
- Mobile phones
- Projector

Mechanics

The point of this activity is to encourage your participants to be less reliant on commercial services that breach users privacy and security.

Protonmail hands-on

Why Protonmail?

- Non-commercial
- Hosted in Switzerland with strong data protection
- Has strong privacy policies about user data
- Offers end-to-end encryption by default (depending on the experience of the group, you might need to do explain this). By default, they employ encryption at-rest. Emails are stored encrypted on their servers – which means the people who own Protonmail will not be able to read your emails (different from the Google model where they focus on encryption in-transit only – messages are encrypted while it is being sent, but once it gets to their servers, they have the means to ¨un-lock¨ your emails). This might need some differentiation between HTTPS and GPG to explain.
- Will allow users to send password-protected emails between different email services (i.e., a Proton user can send password-protect emails to a Gmail user, and the using that same message send a password-protect email back)
- You can opt to have self-destructing messages – for your most sensitive communications.
- Has GPG built in, so if you are looking to extend the training to GPG encryption, this is a good tool to start with

Protonmail limitations

- For free accounts, only 500 MB of space. For 5GB space and more, users need to pay. https://protonmail.com/pricing

To sign up for a Protonmail account: https://protonmail.com/

Notes: If you all using the same internet connection (as we do in training workshops), Protonmail might not allow multiple sign-ups on the same IP address. This might cause delay in the activity. Having multiple access points (with different IP addresses) will mitigate this issue.

> **Jargon Watch:** This has a lot of jargon. Please make sure that you have established a way for the participants to pause and clarify concepts they don´t understand as you do your training. It could be as simple as reminding them that they can raise their hands any time when they don´t understand something, and you asking them directly if they don´t understand a technical term.

Signal hands-on

Why Signal?

- Independently-owned and run by tech activists
- Offers end-to-end encryption
- The encryption protocol that WhatsApp uses is based on the Signal back-end. The difference is that Facebook does not own Signal – so communications and users are more secure.
- Messages in Signal are stored only on their servers until it received by a device (mobile or computer). Once it received, the message is only stored in the device that sent the message and the device that received it.

Signal limitations

- Can be slow
- The interface is basic
- Requires a mobile number to use – so for contexts where there is registration of mobile phone numbers, this can be an issue.
- There is no message syncing on Signal. So even if you can use Signal on your mobile phone and your laptop with the same account, the messages will only be stored in the device that receives the message first. This is part of what makes Signal secure.

Signal can be downloaded on the Google Play Store and on App Store.

Tasks for the Signal hands-on

- Download the app
- Set up an account. This requires the mobile number being used to be accessible to the user during set up.
- Sync contacts.

- You can opt to use Signal to manage even your SMS messages – it means it will store those messages on your phone encrypted. It will NOT encrypt your SMS messages as they are sent.
- Password protecting your Signal app. Privacy >> Screen lock
- Block screenshots in the app. Privacy >> Screen security
- Verify identities. Have everyone share with each other their Signal numbers. Once they have added people others to their Address Book, click on a contact then scroll down to look for View Safety Number, then click on Verify. This will have two users to scan each others QR codes to verify identity.
  - What this means is that if ever that contact changes phones you will have to re-verify their identity on Signal. This is an extra layer of security to ensure that you are know who you are talking to, and if that person is no longer verified, you should probably take steps to be more careful with your messaging with that person.
- If needed, create a group chat on Signal.

Riseup Pad / Ethercalc hands-on

Why?

- You don´t need to sign-up for an account to use these services
- Simple, light-weight interface for communities with slow connections
- Offers anonymity
- You can control how long the pads / calcs can be retained

Limitations

- Simple formatting
- Pads can´t have tables
- Ethercalc editing is not like Excel

Set up a pad: https://pad.riseup.net/

Set up a spreadsheet: https://ethercalc.org

Safety considerations in using pads

- Check to make sure that your pads are updated as some of them expire and are deleted automatically, if not updated for a long time.
- You can password protect a pad to limit access to it
- Be sure to send pad links (and passwords, if you´re using that option) using secure communications channels

Jit.si hands-on

Why Jitsi?

- Allows you to make temporary chat rooms that don´t need log-ins
- Much harder to find a live jitsi chat room (as it is temporary)
- No applications needed (for computers) – just a web browser
- Promised end-to-end encryption

Limitations

- For more than 10 people in the room the connection becomes unreliable

Tasks for Jitsi hands-on

- Set up a chat room at https://meet.jit.si/.
- Share the link with the participants.
- For those who want to use the mobile app, download the app and enter the room name.
- Test voice, video and other functionalities in the app

Trainers notes: Before you begin, practice setting up the services/tools just in case how to do tasks have changed.

Additional resources

Alternative To is a website crowd-sources lists and ratings for alternative tools (platforms, software, apps). They have notes / tags that mention security functionalities of the listed tools. This is a good resource to find alternatives to popular tools.

After finding an alternative tool, confirm its security and privacy features by doing a search with the following terms:

- Name of software + security issues
- Name of software + privacy policy
- Name of software + security review

image-1605452256072.png
Image not found or type unknown