ONLINE EVENTS AND PERSONAL DATA

The **Organiser's Activity Book** is a series of activities to help you explore when, where and how personal information is created and shared, what alternatives there are and how to balance the benefits and risks for you and the people you work with. At the end you have the opportunity to make **Your Data Policy**, a context specific data policy for your events.

In this chapter you will discover:

- □ **How personal data is created and tracked during online events**
- □ **Different risks for personal data created by online meetings**
- □ **When encryption can help (and when it can't)**
- □ **Best practices for online meetings and events**

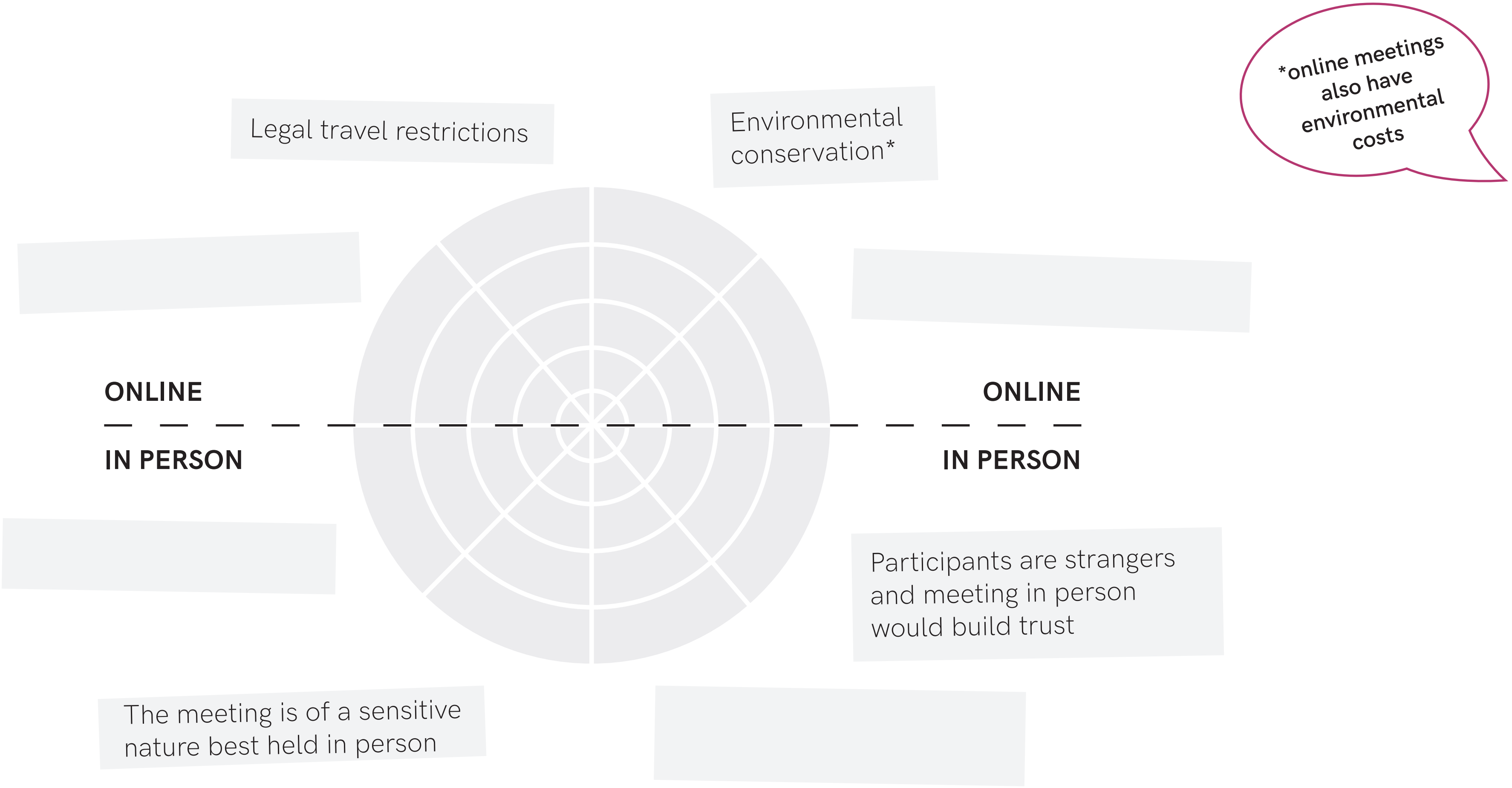
WHY DO WE MEET ONLINE

There are many reasons to hold an event online: a pandemic, concerns for the environment, national travel restrictions, or to keep costs low.

Weigh up the advantages and disadvantages of hosting an in-person meeting versus an online one: colour in the number of rings which represent how important each issue is to you (five rings for the most important, one ring for the least).

Add any extra reasons you think of into the empty boxes. At the end evaluate if an in-person or online meeting is most appropriate for you.

If you decide to connect online there are many options to make your event more - or less - public. Head back to **'An Introduction to Personal Data and Events'** to think about whether you would choose a live stream or private ticketed event.



Legal travel restrictions

Environmental conservation*

*online meetings also have environmental costs

ONLINE

IN PERSON

ONLINE

IN PERSON

Participants are strangers and meeting in person would build trust

The meeting is of a sensitive nature best held in person

ODD TOOL OUT

There are many aspects within an online meeting in which personal information can be created and collected: Participants talk to each other, share documents, and share screens. For each function, there is a different tool.

Pick the odd tool out in each category and discover the different functions you may need to think about when planning an online conference. If you are not sure and want a hint: ask your co-workers, check out the website and privacy policy of the tools or turn to the next page for a few hints in Tangled Tools.

There are many other tools that you might end up using: polling tools, online surveys, live-streaming websites, and screen recorders. Next time you are in a meeting, consider how many different tools there are, from the hardware such as your laptop or webcam, to the software such as the video or the chat room.

You can self-host cloud tools such as nextcloud or video tools such as big blue button or jitsi on your own server rather than going through a third-party.

1. Browser

Chrome

Edge

WhatsApp

Safari

2. Video tool

Microsoft Teams

Jitsi Meet

Big Blue Button

Riseup Pads

3. Shared documents

Google Docs

Zoom

Cryptpad

Nextcloud

4. Group Text Chats

Signal

Messenger

Telegram

Firefox

For each tool there are different risks involved based on various elements: the data collected, their privacy policies and how you use their platform. Continue to the rest of the chapter to find out more.

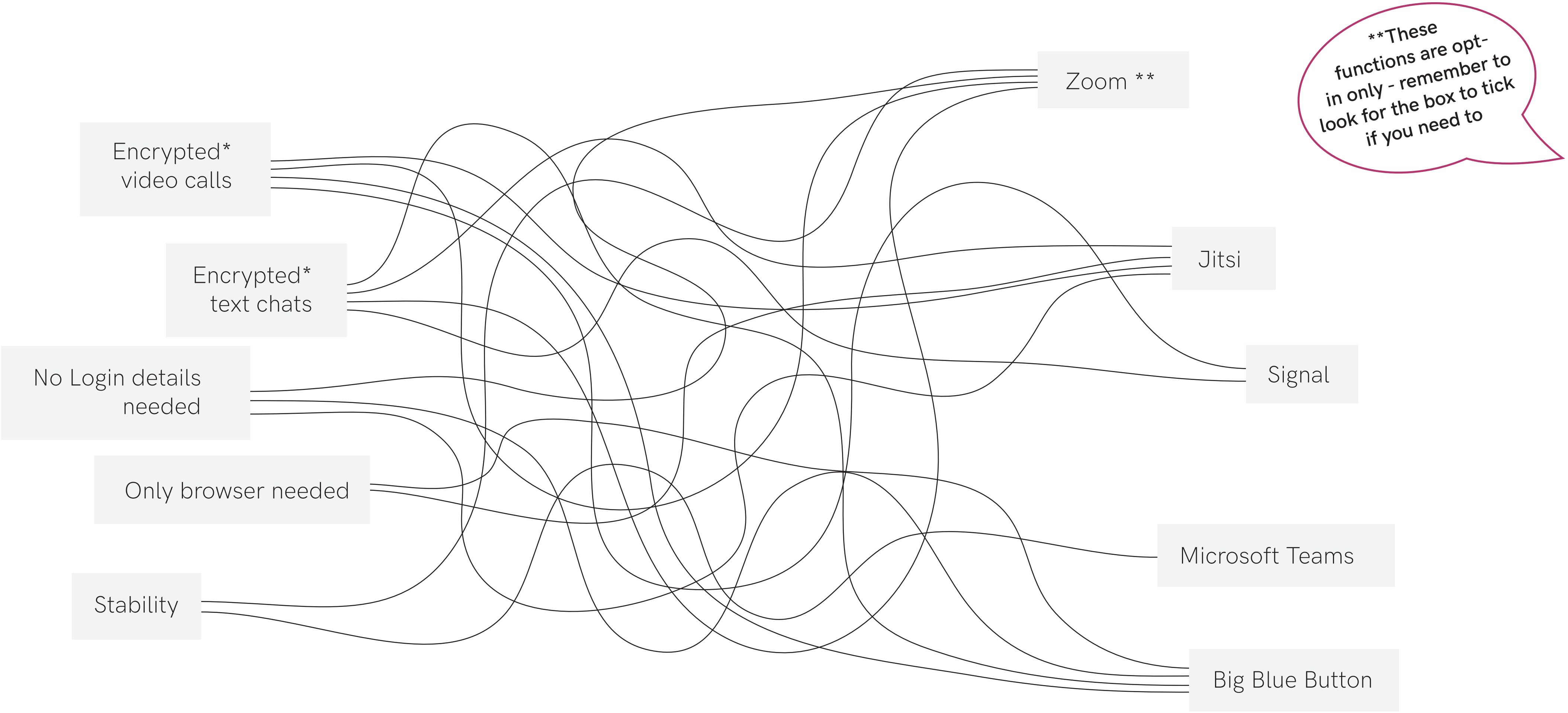
Answers:
1. WhatsApp is for voice calls and texts
2. Riseup Pads are for shared documents
3. Zoom is a video tool
4. Firefox is a browser

TANGLED TOOLS

The following is a series of secure features and a series of tools. Follow the lines to connect the features to the tool. If they don't connect, it means that tool does not offer that function.

Which of them have you heard of? Do you know more tools? Do you know which of the lines they would connect to?

Now you can make a more informed decision, and let your participants know what risks might be involved. For example, they may create a temporary email address if they need a log in detail, or not discuss anything sensitive if it is not end-to-end encrypted.



*Encryption here means end-to-end encryption.
Check out the next page to learn more

ENCRYPTION

Lots of different services use encryption. It enables us to do simple things securely and confidentially online, such as banking or shopping. Encryption is also important for confidential communications. For example, an email, without encryption, is like a postcard - anyone who sees it along the way can read it. Encryption can help protect any personal or sensitive information when you communicate.

Symmetric encryption: information is encrypted and requires a single key or code to be unencrypted.

Asymmetric encryption: both a public key and a private key are required to decrypt the informtion.

Limits of End-to-End encryption

End-to-end encrpytion only protects the content of your information and doesn't protect meta data from where you sent the message, when, how often and to whom.

Some services are opt-in, so make sure end-to-end is enabled. Other services are only opt-in for certain features such as only between two participants, but not for group chats.

End-to-end encrpytion vs transport encrpytion

Some communication services promise users end-to-end encryption, when they only encrypt things between you and their server and then again between them and whomever you are talking to - this is transport encrpytion. Your information is only encrypted when it is in transit to external groups but the service provider can access, process and analyse this data whenever they wish to.

The following tools are used for asymmetric encryption and can keep your online calls safe, but the letters are scrambled using a symmetric code called the caesar cipher. The caesar cipher is a code in which all letters are replaced by a different letter which is a fixed number of places along in the alphabet. Break the code by figuring out how many places along this caesar cipher is set to, and find the names of the tools for encrypted online communications.

VLJQDO = ____________

a voice and text end to end encrpytion tool

PDLOYHORSH = ____________

a tool for applying encryption to emails

YHUDFUBSW = ____________

a tool for encrpyting files

ZLUH = ____________

allows for end to end encrpyted group voice calls

Answers:

This uses a caesar cipher moving all letters three times forward in the alphabet:

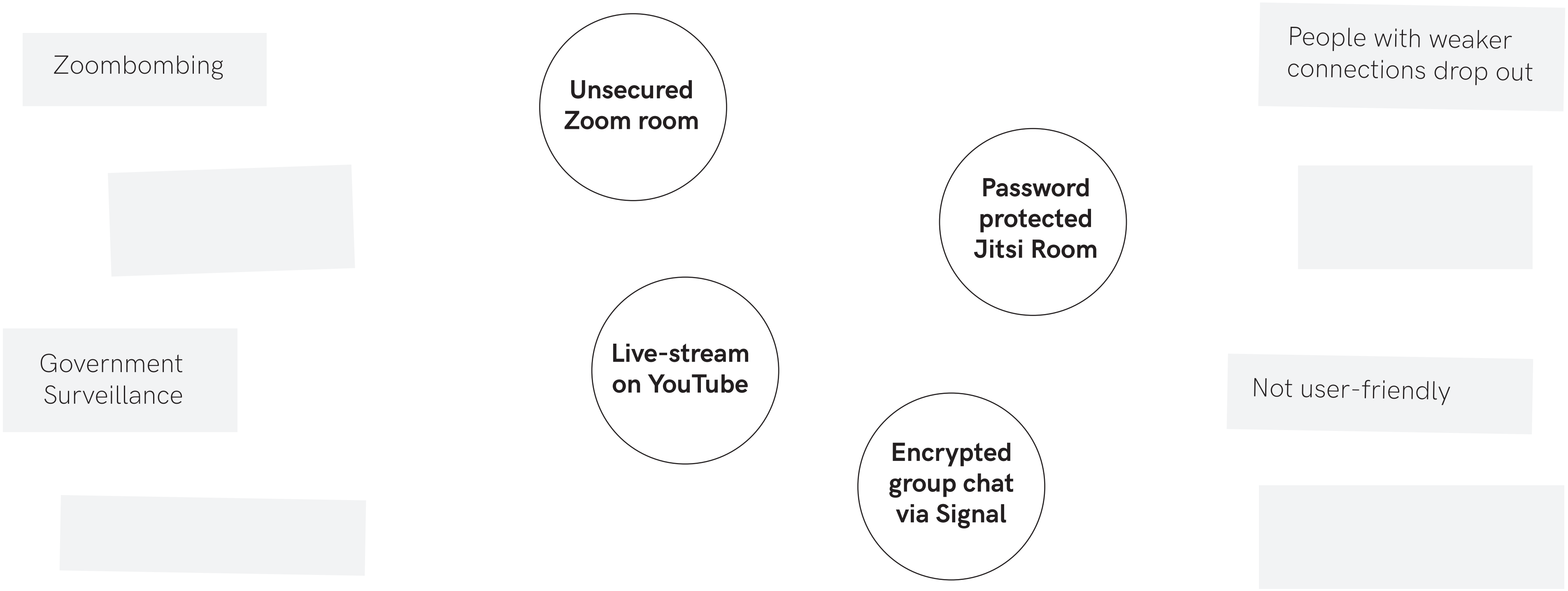
1. Signal, 2. mailvelope, 3. wire, 4. veracrypt

DIFFERENT TOOLS, DIFFERENT RISKS

There are various risks and disadvantages to take into account when you hold meetings and events online: uninvited people turn up unannounced (zoombombing), personal data can be collected by commercial data brokers, or people drop out and disrupt the meeting.

Draw a line between the meeting channel in the middle with the risks of that channel on the outside. Fill in the empty boxes with any further risks you can think of.

After you've identified the risks, you can also consider what you are looking for in a tool. You might choose between whether a tool is open source or supports multiple languages, whether it is hosted by your organisation but supports only small groups or is third-party but mature and stable. Remember some people have different devices, different connection speeds, and different risks.



Zoombombing

Unsecured Zoom room

People with weaker connections drop out

Password protected Jitsi Room

Government Surveillance

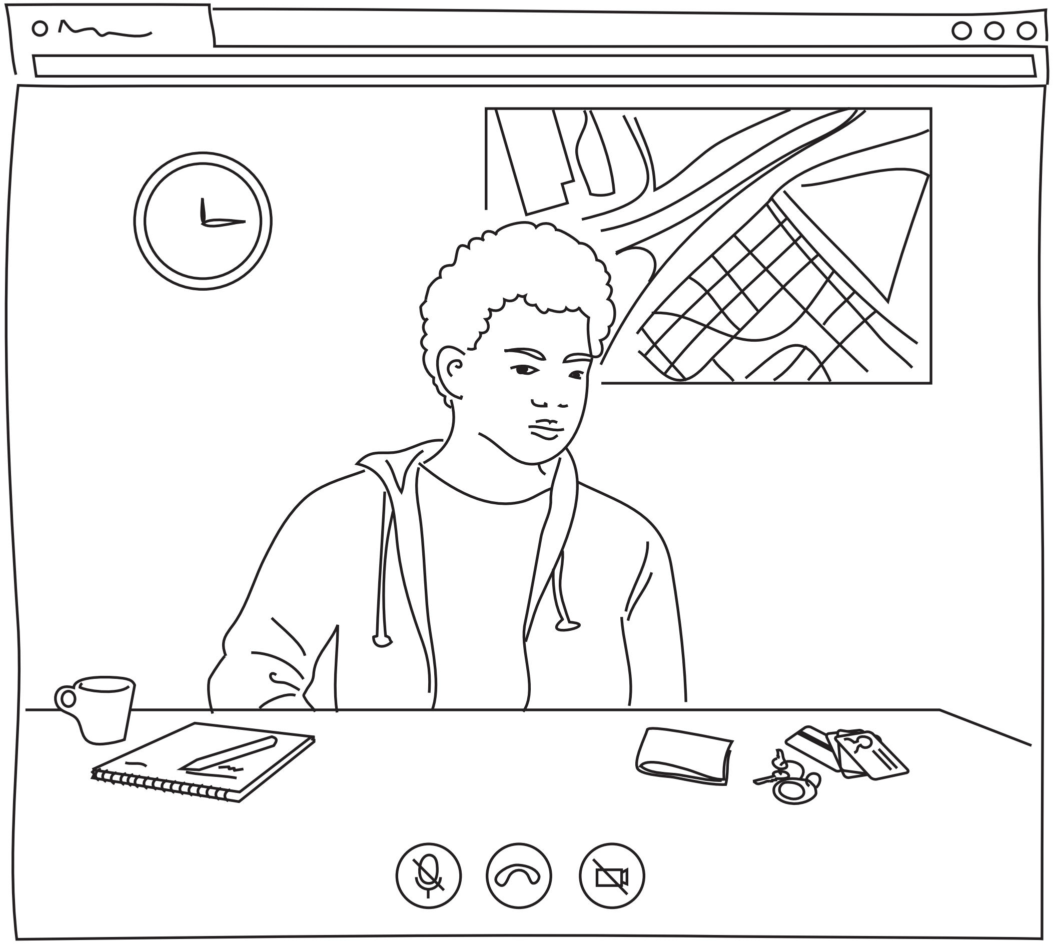
Live-stream on YouTube

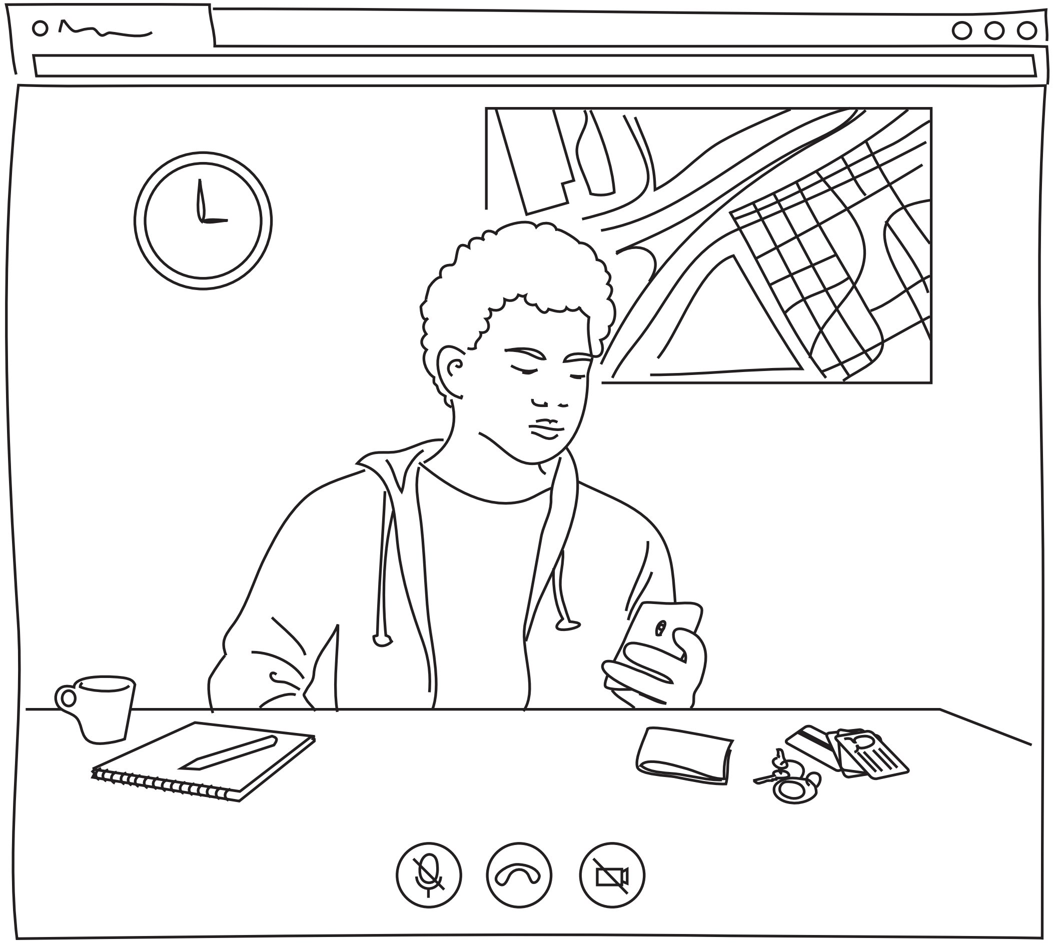
Not user-friendly

Encrypted group chat via Signal

SPOT THE DATA

When we engage with online tools, there are various types of personal data that can be collected. Spot the difference between these two pictures to identify what type of personal data might be collected about you.





Once you are done, think about who you would not want to share this information with and how you might protect each of these through different methods for each.

Answers:

1. Eyes: Biometrics, which also includes facial, fingerprints or voice
2. Clock: The time, date, and length of call
3. Map poster: Location
4. ID card: ID or email/concact address
5. Phone: Information about the device and browser
6. Notepad: Any texts sent in the chat

WHAT YOU SAY ABOUT YOURSELF

There are a variety of different methods you can use on top of encryption to protect your identity. Use different names, ensure that recordings and screenshots aren't taken and finally, make sure your background doesn't give away your location or other personal information.

Draw your selfie and draw in the background what people normally see when you are on online calls. Think about what could gave away personal information in your room and what people could learn about you from its contents. Can you change your background to give less away?

Look at your laptop screen - what do you have in the browser and what applications do you have open? Think about what people could learn about you from its contents. Remember to shut extra programs and tabs down before starting a call.

YOUR DATA POLICY

Now that you've completed Online Conference Tools and Personal Data **you can begin to create your own data policy. You can keep** Your Data Policy **on hand for your own reference and to share with attendees and partners so they can make their own risk assessments. To start making your data policy, answer the questions in the boxes. Don't worry about covering everything straight away, just add anything you can think of from big to small.**

1: Write a list of all the data you might collect such as: participant names, participant travel data, participant dietary requirements, the speakers' details, financial details.

2: Write a list of everyone you share need to share it with such as: partners, cloud providers, funders, other participants

You might want to create a new box for each individual bit of data from question 1. From here, ask yourself what risks are involved with everyone who you choose to share it with. This can dictate what software you choose to use, what you decide is not worth the risk, as well as what data you might decide not to gather. Note the risks involved with any you choose to work with.

3: For the data you decide to keep, when will you delete the data? If it is shared with someone else, when will they delete the data?

Once you're done, look back at the last exercise, identify any gaps in your knowledge that you want to address. Then head to the rest of the chapters, which all have their own data policy section, at **https://ourdataourselves.tacticaltech.org/projects/data-and-activism.**

1 What personal data do you need?

2 Who will you share the personal data with?
Who else can access the data?

3 When will the personal data be deleted?
When will those listed in 2 delete the data?