DATA & ACTIVISM

Activities collection
Events
GET READY...

This book belongs to:

Name*

Draw your selfie here:

This project is a collaboration from Amber Macintyre, Ida Flik, Leil Zahra, the excellent team at Tactical Tech and our partnership organisations.

Each chapter can be downloaded separately, and more information on how to use this activity book can be found at:

https://ourdataourselves.tacticaltech.org/chapters/daa-activities

*Sometimes it’s important to use a fake name, sometimes it’s necessary to use your real name.

This is true for you and for the people you work with: is there risk in them revealing their real name and do they need to? Is it necessary for them to provide a name, and do you need to here? That’s for them and you to work out, but it’s always good to have options and strategies for both.
You can start at the Introduction and work clockwise round the bubble or choose whichever is most relevant for you.
WHAT IS IN THIS BOOK?

How personal data travels between databases, what the data is used for, what privacy policies protect it, and how you are involved with all of these processes can be difficult to understand due to the systems being opaque, technical and complex. Keeping data secure, taking consideration of privacy, and taking effective action can seem intimidating.

These activities present a series of playful activities that provide the questions to help you work out what is right for you, your partnerships and the context you work in.

These activities cover the topics relevant to personal data but there are aspects of events that extend beyond the scope of these activities such as how to create an agenda or run safe sessions.

This book doesn’t give a set of instructions for how and when to act - it is your, and your co-workers’, journey to take.

WHO IS THIS BOOK FOR?

When organising events for others, you have a responsibility to the people you are organising the event for, including their personal data.

These activities are for organisers to:

1) get to grips with the different types of personal data involved in organising events, meetings, and demonstrations
2) understand what questions to ask to make good decisions for how to collect, store and use the data.

This book can help when organising events for activists, human rights defenders and other civil society groups such as:

- annual general meetings
- capacity building
- training
- skill shares
- other meetings
- online calls
- demonstrations
- conferences
AN INTRODUCTION TO PERSONAL DATA AND EVENTS

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:

- Why good personal data practice is important
- How personal data is a risk and a benefit to your event
- Identify who you share data with
- Identify who can help and who hinders good data practice
- Start making your own data policy
WHY IS GOOD DATA PRACTICE IMPORTANT WHEN ORGANISING EVENTS?

There are both foreseeable and unexpected ways we create and share personal data about ourselves or others when organising an event. Draw a line to connect the first half of the story to the second half and find out how these people had their personal information compromised...

Anna was on her way to a workshop when she was stopped at the airport and denied entry to the country, despite not revealing the purposes of her trip on her visa application...

...because an enthusiastic attendee, who was not aware of her not wanting to have public ties with the event, had tweeted about her inspiring talk.

Maria had agreed to speak at a local gathering, but had been careful not to publicly announce her attendance, as she knew certain groups of people would start harassing her due to her participation. Despite this, she started receiving threatening messages some days after...

...because after government security found the workshop agenda online, the government undertook surveillance of unencrypted emails sent by named attendees.

Ali was interrogated by police months after he had participated in an anti-corruption event, despite making sure that he only communicated about his attendance with a secure messenger...

...because the local authorities had found a reimbursement made to his account from a foreign account which was associated with the human rights organisation that hosted the event.

...now head to the rest of the activities in The Organiser’s Activity Book to start to make your data practices better.
YOUR MOTIVATION TO LEARN ABOUT PERSONAL DATA

Are you organising an event or a campaign? Do you manage a database of email addresses? Do you have a specific issue, such as finding the right software to store personal information, or do you have a more general concern about privacy? Write down any questions you have or problems you are concerned about.

Return to this page after completing a few activities from The Organiser’s Activity Book and see whether you can answer the questions or if the way you understand the problem has changed.
YOUR EVENT IN A NUTSHELL

To fill in The Organiser’s Activity Book it may be useful to have an event in mind. Fill in this quick overview of an event either that you organised or attended as a participant or one from the past or one coming up in the future. You can refer to this page when the other activities prompt you to think about a specific event.

**WHY?** What do you want to get out of the event?

**WHAT?** What is it called? Is it a workshop or a training or something else?

**WHO?** Who are you working with? Who else is organising? Who else is attending?

**WHEN?**

**WHERE?**

When this page is filled in it contains a lot of information about the event, connected to you! Think about where you will keep it or when and how you will destroy it.
YOUR DATA CONTACT POINTS

During certain stages of organising an event you will share participant information with others including travel agents, social media companies or funders. You may be sharing this information on purpose, but you may also share it unintentionally.

Use this page to think about who you share data with, who collects data from you, what their intentions are, who has more or fewer technical resources, and who can provide support for finance, morale, infrastructure, or emergencies. Write as many as you can in one box, or fill in on a new piece of paper.

Who do you share the data with? Why?

What software do they use including for email, hosting information, and social media?

Do they have expertise or resources to support their use of technology or do they rely on others?

Who wants to collect data about your event? Why?

Do you have a point person with their organisation?

What connections and contacts do they have?

Once you’ve filled the page in you can begin to evaluate who can access your participant’s data, what risks you might be creating, and what you might be able to do to limit them. Later in this chapter, you can begin to answer these questions in the activity: Who Helps and Who Hinders.
HOW MUCH DATA DO YOU CARRY WITH YOU? LOOK FOR THINGS IN YOUR POCKETS, BAGS, ON YOUR DESK (THAT YOU DON’T NEED) AND GLUE THEM ON THIS PAGE.

How much do you think about your physical data? Reflect on what other people could guess about you from what you found and put on this page. If it says a lot, you might want to find a way to dispose of this page without it linking back to you.

If you were travelling to an event think of what else you might be carrying in your wallet and pockets that contains personal information including travel tickets, event tickets, name tag, and event agenda.
WHO HELPS AND WHO HINDERS?

Now you have evaluated who may have access to the data you own in the previous activity, Your Data Contact Points, it is important to understand what potential risks these contacts pose, and what helps they may be able to provide such as with secure methods for hosting and sharing data. If you aren’t sure about a connection, you can find public information such as their social media accounts, stories about them in the media, and country reports from organisations like Amnesty International. Think of the variety of ways someone can help, or hinder, the protection of your participants’ personal data such as their motivations, their skills, and their resources. See the first example for inspiration.

Write short thank you notes to anyone who has helped you before.

| Help                          | | | |
|-------------------------------| | | |
| - work with others who can provide resources | | | |
| - willing to learn and use privacy tools | | | |

| Hinder                        | | | |
|-------------------------------| | | |
| - based in a country with substantial surveillance | | | |
| - use third party systems (e.g. Google) | | | |
| - no staff dedicated to their tech security | | | |

Once you have filled in this page you can be better informed to choose your tools for collecting, storing and sharing participant data. Go through each and evaluate how they could practically help you, or how they might hinder you and how you can mitigate against that. This can help inform Your Data Policy at the end of this chapter.
YOUR DATA POLICY

Now that you’ve completed An Introduction to Personal Data and Events, 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. This is the introduction, so 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, return to the exercise above, Who Helps and Who Hinders, and ask yourself, are there any risks missing? Can you mitigate for them and if not can you be transparent about these within your own data policy?

Now, head back to the exercise at the start of this chapter, Your Motivations. Do you feel you began to learn what you wanted to? What’s missing? What would you like to learn more about? Then, check out the rest of the chapters, which all help develop and improve other sections of your data policy, at https://ourdataourselves.tacticaltech.org/projects/data-and-activism

The Organiser’s Activity Book
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:

- Public and Private invitations
- Tools for registration and event apps
- Tools for communication with participants
- How to help participants facing higher risks
INVITING YOUR PARTICIPANTS

There are many approaches to inviting participants to attend, or apply to attend, your event. Some of the options are listed in the box to the right showing how they fall on a spectrum from private to public methods. There are risks and benefits across this spectrum. First, fill in the boxes around the edges of the ring below with the benefits of a public event, such as publicity or a diverse audience, and the risks, such as putting participants at risk either due to their background, or to the topic of the event. Then, rank how important these are to you by colouring in the rings - the more rings you colour the more important you feel this benefit or risk will be to take into account when organising the event.

Benefits of a public event
- Attract diverse participants
- Topic of the event may attract negative attention

Risks of a public event
- Put participants at risk
- Topic of the event may attract negative attention

Private invitation
- Invitation only
- Word of mouth between in your network
- Open call - Ticketed event with application process
- Ticketed event, first come, first served
- Public announcement - anyone can attend in person or by watching online without ticket or application

Public invitation

If you aren’t sure, for inspiration return to the chapter Introduction to Personal Data and Events, found on https://ourdataourselves.tacticaltech.org/projects/data-and-activism/ to consider what you might need to take into account to make the decision.

Once you’ve filled in your rings, choose from the options in the box above what invitation method you will use.
Make your app-monster come to life with colour or extra eyes, arms and legs.

Organisers can use different websites and apps to register participants for events. However, the company who owns the website or app might not have the same data policy as the event organiser. Use a pen to draw a line to connect the three different monsters’ head, body and feet to discover which software collects what data and with whom they might share it.

Because these tools are easy and accessible, you may still decide to use them, but now you can do so with more awareness of the risks. You may consider asking for less information from participants at the registration stage. If you want to learn more check out the “Research” tab at https://ourdataourselves.tacticaltech.org/projects/data-and-activism

**MONSTER APP MATCH**

**Answers:**

- Monster A: 1, 6, and 8
- Monster B: 2, 4, and 9
- Monster C: 3, 5, and 7

<table>
<thead>
<tr>
<th>Name of website or app</th>
<th>Data collected</th>
<th>Data shared with</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Eventbrite</td>
<td>4. Location, photos/media/files, storage, network connections and full network access</td>
<td>7. U.S. Federal Trade Commission. May be required to disclose personal data in response to lawful requests by public authorities.</td>
</tr>
<tr>
<td>2. Sched.com</td>
<td>5. Identity, calendar, contacts (name, work email, organisation, phone number, zip code) runs at start up</td>
<td>8. Political parties for profiling potential supporters such as Donald Trump’s 2016 presidential campaign team.</td>
</tr>
<tr>
<td>3. CrowdCompass</td>
<td>6. Name, email address, address, IP address, access device or browser, type of event registration, interest in events from website browsing</td>
<td>9. Facebook, Twitter, Umbel, Foursquare, Madrill, Intercom, Google Analytics</td>
</tr>
</tbody>
</table>
In certain countries, merely attending an event, be it a workshop or a conference, can put a human rights defender at risk. In Egypt, for example, the Cairo Institute for Human Rights Studies canceled its annual training program on human rights, which it had held for the past twenty-two years. Explaining the decision in a published statement, the institute wrote, ‘It has become impossible to find a safe space for youth for learning and creativity. Prisons have become the fate of all those who care about public matters.’ Smear campaigns against NGOs in pro-government media outlets have made public outreach more difficult and dangerous: activists report threats of violence from ordinary Egyptian citizens during public activities.” This is just one example of the way, for multiple reasons, states and corporations alike are interested in obtaining your information. From security to marketing, we are reduced to data that is used beyond your control and your knowledge. This makes attending an event yet another threat vector, especially when your data is not secured by those who plan the event or the platforms it is outsourced to.

In September 2011, two iPads were stolen from an Eventbrite employee which contained data collected at one of their customer’s events. Eventbrite describes itself as the “world’s largest event technology platform,” building “technology to allow anyone to create, share, find and attend new things to do that fuel their passions and enrich their lives.” Kevin Hartz, Eventbrite’s co-founder and CEO at the time, wrote in a blog post on the company’s website that the “potentially compromised data included full credit card information for 28 people who bought tickets for the event; names and email addresses for some customers who bought tickets online for the event; and the names, email addresses and last four digits of credit cards for some fans who bought tickets at the event. The full credit card information was erroneously stored due to a glitch in the iPad app that has since been fixed.” Though the company notified the attendees whose email addresses were potentially exposed, and immediately alerted authorities and initiated a remote password-lock and a wipe of the data on both devices, Hartz went on to say that he knows that having one’s personal data compromised is a violation of the trust put in Eventbrite, and expressed his apologies to the people affected.
DOODLE WHILE YOU THINK ABOUT THE STORIES, WRITE DOWN ANYTHING THAT COMES TO MIND, OR TAKE A BREAK AND BREATHE. YOU’RE A STAR!
CONNECTING WITH YOUR PARTICIPANTS

There are different platforms you can use to collect initial information from your participants such as their name, contact details or reasons for interest in the event. However, the company who owns the platform can also collect, store, and analyse not only the data you collect on your participants but also extra data that the platform requests. In the bubbles, highlight the information that you use the platform for and note to yourself how much more the software can see.

Some of these tools are the most accessible to you and your participants, but it is important to check out the relevant risks and how you will mitigate for them. Think about whether any of the information could put any of your participants at risk if it were compromised.
PUT YOURSELF IN THEIR SHOES

When organising an event, you might need to mitigate for risks and put in place logistics that can support a diverse group of participants. Fill in the empty circles with information about your participants that may require you, as an organiser, to consider risks or provide specific resources. Around each of the circles, add how you might mitigate these risks or deliver the requirements.

Now you’ve filled in this page, consider whether you could keep this information anonymous by planning for these eventualities without asking the participants for the information. For example, ask if they have specific requirements, rather than for their personal information. Once you collect this data, decide how you will store it safely and when you will delete it. Remember, whilst this data is helpful to an organiser to improve the participants’ experience, in the wrong hands it could be used to make things more difficult for the participants.
Now that you’ve completed Event Registration and Participant 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 Put Yourself In Their Shoes, is there data you might need but would be too risky to collect? How will you collect and store that data? Can you be transparent about this within your data policy?

Now head back to the list on the first page of what you will discover in this chapter. Do you feel you began to learn what you wanted to? What’s missing? What would you like to learn more about? Heading to the rest of the chapters, which all have their own data policy section, at https://ourdataourselves.tacticaltech.org/projects/data-and-activism
TRAVEL AND OUR DATA BAGGAGE

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:

- Personal information collected by different transport options
- Data collected when booking flights
- Data collection for visa application
- Ensuring data protection from a travel agency
- What personal information maybe involved in different options for accommodation
There are many different reasons that we travel, or ask others to, when involved in social action. These include attending meetings face to face with stakeholders, bringing people to a public demonstration or delivering capacity building workshops. You may only travel in your local area, or you may often travel across the world. Whether far or near, there are many aspects of travelling that involve the creation and collation of personal data.

There are also many reasons not to travel such as to protect the environment, during a global health crisis or because we take care of children or other dependents. If you choose not to travel, or your participants do, you can look at our chapter on online meeting tools (upcoming). Even in these cases you may travel locally, or be involved in organising someone’s travel to visit you, so this chapter could still be of use. This chapter presents some of the factors to consider regarding personal data when travelling. Throughout the exercises remember that travel environment changes. There may be new border checks, local transport timetables, and accommodation regulations.

It may be good to start with a few ideas in your mind of why you travel. Choose either places you have travelled to for social and political action or places where your organisations has held events. Write down destinations and reason for travel for different points on the map below. Add features such as hills, trees and buildings to include more destinations. If you want, add the modes of transport to each location.

Remember this page contains sensitive information once filled in, which may affect how you store it or throw it away.
LOCATION, LOCATION, LOCATION

Whether a workshop, training or conference is held locally or far from home, there may still be travel between several locations that needs to be considered.

Travel around the map on the side and trace the potential journey of a participant. As you reach each location, think of the types of personal data that could be collected there. There are a few prompts below to start you off.

The personal data collected at each of these locations may be a greater or lesser risk for your participants. If you want a reminder of how to evaluate the different risks for your context head to the first chapter in this series: An Introduction to Personal Data and Events.

Consider how you might mitigate risks such as by using the office of a trusted partner or providing your own transport. Whatever you decide to do, consider how you can inform your participants about what personal data may be collected on them, so they can evaluate the risks for themselves too.
Once you’ve filled this table in with all the options, you might choose a venue or location based on how easily and safely it can be reached. And when you fill out Your Data Policy at the end of this chapter, remember to add what elements of personal data could be collected depending on how the participants travel.

**Tracking Transportation**

Participants will have to travel to events, demonstrations or trainings and the mode of transport they choose can leave a trace of where they came from and where they were travelling to. In the table below, colour in the boxes where the answer is ‘yes’ to the questions at the top of each row. If you don’t know the answer check out the transport provider websites or ask others who have experience in this area. Add additional risks and transport options relevant to the area of your event...

<table>
<thead>
<tr>
<th>Means of transportation</th>
<th>Do you have to provide the participants’ real name to make the booking?</th>
<th>Is it necessary to pay with a debit/credit card or bank account, and therefore to leave financial traces?</th>
<th>Are identity checks by police or other authorities likely on this route?</th>
<th>Are there CCTV cameras along this route?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bus</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Train</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rented Car</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We sometimes have to fly to attend events, participate in meetings or carry out other elements of organising. When we book a ticket, we are assigned a PNR (Passenger Name Record). Do you know what data is stored in these records? Try to find them in this word search. Answers can be forwards, backwards, up, down, and diagonal.

| A | P | N | X | T | I | C | J | T | A | F | R | I | X | P | S | M | R | F |
| B | S | K | N | L | C | A | N | H | N | T | I | Y | N | G | E | R |
| T | R | A | V | E | L | I | T | I | N | E | R | A | Y | S | T | O | R | E |
| L | M | V | G | W | K | J | D | A | K | M | M | Q | E | G | S | A | S | M | Q |
| E | P | S | C | Y | G | X | Y | C | Z | V | Y | M | E | P | D | H | U | U |
| G | Z | K | E | A | L | G | Z | H | O | B | C | A | N | O | L | O | N | E |
| R | I | H | B | A | G | G | A | E | H | D | R | P | R | R | B | E | W | E | N |
| W | C | K | D | F | I | D | B | B | L | I | F | E | K | R | T | V | N | N | T |
| B | O | O | K | I | N | G | D | A | T | E | S | S | S | M | Z | A | O | F |
| N | U | M | B | E | R | O | F | P | A | S | S | E | N | G | E | R | S | H | L |
| E | D | O | C | R | O | T | A | G | O | L | V | F | N | L | V | T | H | P | Y |
| S | S | E | R | D | D | A | L | I | A | M | E | D | X | C | U | T | O | E | E |
| W | Y | H | N | D | R | S | M | Q | G | V | X | R | R | F | C | F | W | L | R |
| N | O | I | T | A | M | R | O | F | N | I | T | E | K | K | C | T | T | A | R | S |
| T | R | A | V | E | L | A | G | E | N | T | Y | L | U | I | S | E | T | J |

Carry on to the next page to find out more...
PNR SCAVENGER HUNT

Now you know what data can be created and what personal data you are asking participants to give away if they need to fly to your event. Keep in mind these categories might be added to or taken away from depending on global context, crisis and country-specific requests.

Even if we cannot ‘see’ information in the barcodes or sequences of letters and numbers on our plane tickets, other people may be able to derive meaning from them, including the PNR information recorded above. Security researchers were able to go to Instagram, and use people’s photos of their boarding passes to access the traveller’s booking and PNR (for more information follow the link below). This could happen to any of your participants if they publicly share their boarding pass. Check out how the researchers did on the right hand side of this page.

If you want to, find a friend or colleague and play with one of your own boarding passes. If you see someone you know post their boarding pass online, let them know the risks.

Other personal information is on our tickets too, and any PNR could contain further information in the field for extra notes depending on the country’s requirements, such as our health status during a global pandemic. Consider this in Your Data Policy at the end of the chapter so you can alert your participants or mitigate any risks that might be generated by this data being collected.

The security researcher’s method:

STEP 1
Many airlines only require a traveller’s last name and booking reference number to log into their customer portal. Look for a widely used airline company who uses the same mechanism (tip: such as Lufthansa or easyjet)

STEP 2
Search for photos of boarding passes online (e.g. image search, instagram #boardingpass, ...) and look for one from the airline you chose in step 1.

STEP 3
Take a screenshot of the barcode on the boarding pass.

STEP 4
Read the PNR code with a barcode scanner, which you can find in your phone’s app store. Look for the person’s last name and booking reference.

STEP 5
Use this information to try and log in on the airlines website.

Find a friend or colleague and play. Can you find anyone’s information following the same steps the researchers did?

Read more of this story in Tactical Tech’s research on our travel data, available at https://ourdataourselves.tacticaltech.org/projects/data-and-activism/
If participants have to travel to another country to attend an event they may need to get a visa. Different countries ask for different types of personal data in the visa application process. Check out the starred boxes on the right to see which letter corresponds with which collected data. Draw a line from each letter to the country you think requires that personal information in the visa application process.

*The Schengen Area Countries are 26 neighbouring European countries which opened their internal borders to each other.
INTERVIEW YOUR TRAVEL AGENT

Travel agents have the resources and expertise to help manage various aspects of logistics for large groups, from transport to accommodation. However, by involving them, you add an extra party who will have access to your participants’ data. Call your travel agent, find out what information they collect and for what purposes.

START HERE

To whom am I speaking?
What is your job title?

Great, can you help me with questions about your data policies?

Yes
No

How important do you personally find privacy and security on a scale of 1 - 10?

1 - 4
5 - 10

Thank you, my first question is, if I booked flights for participants of an event with your agency, what information would you ask from me?

Thank you, and who do you share this information with?

Can I contact your organisation with some materials on this topic?

Would you like to explore more of these issues?

Okay, and what do you need each of these pieces of information for?

Is there anyone else? What software and services are you using?

Thank you for your time, I can share materials from Tactical Tech if you want to know more about the topic.

Thank you, my first question is, if I booked flights for participants of an event with your agency, what information would you ask from me?

Once you’re done, you can choose which travel agent to work with, or how much you are willing to share with them. Record this information in Your Data Policy at the end of the chapter.
Various risks and benefits need to be weighed up when you book accommodation. Consider the following questions, and write their answer in each corresponding box. Add other types of accommodation and questions you might have using the empty spaces. Weigh up how important each of the questions is to you. If you want, add their level of importance for your event from high, medium, or low in each box.

Consider which circumstances might change regulations and how such as during a pandemic, after a natural disaster, or if the country has a sudden and controversial change in political leadership.

From this you can choose which accommodation is best for you and your participants. It may be that you choose different options for different participants. This may also help you think about who else might have information about your participants. In Your Data Policy at the end of the chapter, make sure you include any person or company you think of, including accommodation owners.

<table>
<thead>
<tr>
<th></th>
<th>Is the area safe for your participants?</th>
<th>Can you book under the organiser’s name rather than the participant’s?</th>
<th>Do they require participant’s name, passport number and country of origin?</th>
<th>Is it close to the venue?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AirBnB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local contact’s home</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Would booking accommodation under your name reduce the need for participants to share their personal details?
REFLECTIONS

Take a minute to reflect on how you are feeling. Have you learnt new information through The Organiser’s Activity Book? Think about the last time you travelled to an event - is there anything you will change now? How do the activities make you reflect on how you handle other people’s information? Is there anything you are more nervous about? Do you have practical steps you want to take to change your data practices?

If you checked out the chapter An Introduction to Personal Data and Events, at https://ourdataourselves.tacticaltech.org/projects/data-and-activism/ look at your answer to the exercise called Your Motivation to Learn About Personal Data and see if your ideas have changed.

Use this space if you prefer to draw, colour, or doodle instead!
Now that you’ve completed Travel and Our Data Baggage, 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 through the exercises. Is there anything you’ve missed? How will you be transparent about the risks that remain for your participants within your data policy?

Now head back to the list on the first page of what you will discover in this chapter. Do you feel you began to learn what you wanted to? What’s missing? What would you like to learn more about? Heading to the other chapters, which all have their own data policy section, at https://ourdataourselves.tacticaltech.org/projects/data-and-activism
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 information can be pieced together from social media to tell a story about your event
- The risks of the social media archive
- How to create a social media policy for an event
- How to limit the risks associated with taking photos at your event
What we post on social media can reveal more than we think, especially when it can be connected to other information. Think like an investigator: you know three people, who all work in different organisations, attended an event each - but you don’t know which. Use the posts on the right to match the name of each participant with their organisation, and to which event they attended. Use the following table to help you solve the puzzle by crossing boxes with the information you can take from the posts to the side. Then use the information you have to fill in the blanks.

<table>
<thead>
<tr>
<th>Event</th>
<th>Affiliated Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local event</td>
<td></td>
</tr>
<tr>
<td>International event</td>
<td></td>
</tr>
<tr>
<td>Regional skillshare</td>
<td></td>
</tr>
<tr>
<td>Tactical Tech</td>
<td></td>
</tr>
<tr>
<td>Freelancer</td>
<td></td>
</tr>
<tr>
<td>Large NGO</td>
<td></td>
</tr>
</tbody>
</table>

Once you’re done think about how you post about speakers, participants, and topics at events you organise and attend. Do you tag others? How much about them do you give away?
WHAT SOCIAL MEDIA CAN REVEAL

Social media can be a great way to promote an event, for participants to connect with each other, and to add an extra layer of conversation. Social media platforms can collect data for their own purposes from posts and platforms, and save this data for a long time. If the conversation is happening in public spaces such as Twitter, or public Facebook pages, other people can also track this conversation.

Look up the hashtag(s) of a previous event you organized or demonstration you attended (if you haven’t organized any event, yet, use an event you attended or a large scale one you have been interested in attending in the past). Think like an investigator - write down everything you can learn on this page. Write tweets you see here, connecting hashtags, names or organisations that stand out, and anything about the topics and views discussed. You can draw a network of all connections you discover, make a collage of different headlines, or write a mini investigation report. - whatever you feel like.

Once you’re done review everything you learnt about the participants, the topics discussed, speakers, or anything else. Was it what you expected to see? Did you learn anything unexpected?

When creating Your Data Policy at the end of this chapter, how can you protect participants - would you encourage them to share less? Can you use other software to achieve the same results of connecting participants? Can you keep identifying information out of public promotion posts? Remember there are different risks and benefits from everyone, which you will need to evaluate for yourself.
TIME TRAVEL

Take a look at the activity What Social Media Can Reveal, one of your own recent tweets, or a tweet of an organisation you know. Travel to the future for a moment, and imagine what might have changed - have your adversaries gained new power, are new technologies making it possible to identify people from existing documentation more easily? Write down what could happen and what you could do preventatively to minimise harm in the future.

IN 5 YEARS...

Who will have control over the information saved on social media platforms: companies, citizens, government or another entity?

What technology will still be used and what will be new?

Who will be elected at the time? What will be the politics?

IN 10 YEARS...

IN 100 YEARS...
CREATE YOUR EVENT SOCIAL MEDIA POLICY

The use of social media can have different benefits and risks for different people. As an organiser you cannot always know what everyone’s risks are, and sometimes it is best just to ask! Creating a collaborative social media policy which you agree by consensus for your event at the start can not only make sure everyone can express their different benefits and risks, but also make sure everyone knows the policy from the start. If the event is small, everyone can be involved, if the event is large, you may want to have a smaller group work on the social media together. Follow the steps here for any group consensus, with features for the social media policy - you can use for any other aspects of your data policy too.

START HERE

Step 1
Introduce and clarify the issue(s) to be decided
What social media might the participants and organisers use? How? Why?

Step 2
Explore the issue and look for ideas:
- gather thoughts and reactions, issues and concerns
- collect ideas for solutions
- create debate spaces where necessary
Are there different rules for the organisers and for participants? Do some participants want to remain anonymous? Are there certain sessions that should be kept private and others to promote?

Step 3
Look for emerging proposals:
Look for a proposal and solutions that bring together the best ideas and address the biggest concerns
Can you find a way to allow different participants to take different routes? Are there methods to allow people to sign up to anonymity? Are there ways to signal if a session is under Chatham House Rules*?

Step 4
Discuss, clarify, and amend your proposal:
Make a space and time for questions and amendments
Does everyone have any questions or see any gaps?
Are any social media platforms you might have missed?

Step 5
Test for agreement:
- blocks (fundamental disagreements)
- stand aside (I don’t agree but I won’t stop the group)
- agreement (I support the proposal)

Step 6
Implement your decisions:
Where do you display the policy? How do you alert people who arrive later to the policy? Do you have signs you can put up to show which sessions are no social media zones?

*Chatham House Rules means that people can use information they learn in the session but the names, and organisations, of speaker and participant’s will not be revealed. You may choose more or less restrictions than this, but it can be a good starting point.
To prevent sharing more information with potential adversaries than you would like to, make sure to check the metadata of photos or screenshots you take at an event before you share them. The following instructions are a guide and may differ for your device.

How to edit or delete photo metadata:

On Windows: in the “details” tab, click on Remove Properties and Personal Information -> “remove the following properties from this file”, select specific properties or click “select all” and click “OK”

On a Mac: in OS X you’ll have to resort to third-party software (e.g. ImageOptim) if you want to completely strip the metadata out of your photos. You can remove the location data from photos in Preview. Open your photo, select Tools > Show Inspector or press Command+I on your keyboard. Then, click the “GPS” tab, and “Remove Location Info” at the bottom.

On Linux (with the command line tool):

# remove all metadata of a image file
exiftool -all=- -overwrite_original photo.jpg
# remove all metadata of all *jpg files in current dir
exiftool -all=- -overwrite_original -ext jpg .
# remove metadata for all *jpg files in current dir and subdirs
exiftool -all=- -r -overwrite_original -ext jpg .

On Android: You will need a third-party app e.g. Photo Metadata Remover Before you install a third-party app, first check your Camera app’s settings to see if you can disable EXIF data generation. Some camera apps may only let you disable location inclusion, while others may not allow you to disable EXIF data at all.

On iPhone: e.g. with the app Metapho this app requires an in-app purchase to unlock the ability to remove photo metadata, though.

How to check photo metadata:

On Windows: right-click a picture file, select “Properties,” and then click the “Details” tab in the properties window

On a Mac: right-click the image file (or Control+click it), and select “Get Info.”

On Linux (in the command line tool):

# install exiftool:
sudo apt-cache install libimage-exiftool-perl
# show metadata of a image file:
exiftool myPhoto.jpg
# show metadata for all *jpg files in current dir:
exiftool -ext jpg
# show metadata for all *jpg files in current dir and subdirs:
exiftool -r -ext jpg .

On Android: Open the picture and tap on Menu located at the top right corner of the screen (it’s the three horizontal dots). From the menu, tap on “Details” to see all metadata

On iPhone: To access the metadata of your iPhone pictures, you will need a third-party app, e.g. Exif Metadata

How to turn off location or the camera app’s permission to access location (so the geolocation won’t make its way into the photo’s metadata to begin with):

On Android: settings -> apps -> settings wheel icon -> “app permissions” -> “location” -> disable for your camera app

On iPhone: open your settings and tap the “Privacy” controls -> “Location Services” -> turn off all location services with the toggle, or tap “camera”-->allow location access: never
'NO PHOTO' BADGES OR STICKERS...

...can be an easy and helpful way to respect people’s privacy choices. Organisers and other participants may want to take photos during events for various reasons such as publicity, memories, and evaluation reports. However, some people may not wish to be photographed.

Online meetings also come with risks of people taking screen shots or recording the meeting - consider how you might use the following methods online, and record them in Your Data Policy.

There are different tools you can use to help protect people’s privacy:

- Stickers which say whether someone is happy to be photographed or not
- Different coloured lanyards for those who not want to be photographed
- Ribbons for those who are happy to be photographed
- A “no photos” policy unless people have signed consent
- Provide the photographer has a list of names and faces of those who can (or cannot) be photographed
SPACE FOR YOUR INNER CRITIC

Let all your negative thoughts out. Does trying to start a better data practice feel overwhelming? Unrealistic? Frustrating? What will be most difficult?

SPACE FOR YOUR INNER CHEERLEADER

Celebrate the progress you have made, the knowledge and skills you already have and the practices you’ve enjoyed learning about or implementing.

Bored of writing? Draw, colour, or doodle instead!
YOUR DATA POLICY

Now that you’ve completed Social Media and Publicising Your Event 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 need to share data 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, Space for Your Inner Critic and Inner Cheerleader, and 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
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.

*online meetings also have environmental costs
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.

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

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

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.

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.
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.*
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 information.

---

Limits of End-to-End encryption

End-to-end encryption 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 encryption vs transport encryption

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 encryption. 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.

```
PLQDO = _______ _______  
   a voice and text end to end encryption tool
```

```
PLODHORSH = _______ _______  
   a tool for applying encryption to emails
```

```
YHDFUBSW = _______ _______  
   a tool for encrypting files
```

```
ZLUH = _______ _______ _______ _______ 
   allows for end to end encrypted group voice calls
```

---

Answers:
1. Signal
2. Mailvelope
3. Wire
4. Veracrpyt

This uses a caesar cipher moving all letters three times forward in the alphabet:
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.
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/contact address
5. Phone: Information about the device and browser
6. Notepad: Any texts sent in the chat

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.
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.
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
THE LIVING DATA POLICY

It's time to wrap it up, look at everything you learnt about, the practices you discovered and the ones you planned for, collect your conclusions!

Go back through the ends of each chapter where you filled out the “data policy” cards. Are there any new findings, learnings, overall principles or guiding ideas you find when looking at them all together?

Consider how you can build them into your work. Perhaps you cut out the cards and create your own data policy poster with them to stick beside your laptop or desk.

Or you create a spreadsheet which you share with colleagues which describes the types of data and the questions you have for the data.

<table>
<thead>
<tr>
<th>Names</th>
<th>Email addresses</th>
<th>Social Media metrics</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where do you host the information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Who needs access to the information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What do you use the information for?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When will you delete the information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Feel free to organize the information however you want such as by timelines, different themes or different uses of the data. Maybe you want to highlight surprising or hard to remember information.

Maybe you want to write it into a policy, or perhaps create an visual info-sheet, or a video on your values. Consider who needs to use this information, who else is using data, who it affect and how they would best access this information.

Remember the policy itself may contain data that is sensitive and you may want to keep only the general principles in public spaces.
DATA & ACTIVISM

Activities collection

Events

TACTICAL TECH
The Organiser’s Activity Book