

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



10–16 years



35–50 min



8–30 participants

Card sorting, decision-making and discussion

OVERVIEW

Participants consider what information different AI-powered systems may collect and decide what they would or would not be comfortable sharing. By tracing how data can be collected, combined, stored and used, they explore privacy, consent and the trade-offs between personalized services and control over personal information.

LEARNING OBJECTIVES

Participants will:

- identify different types of personal data
- understand why many AI systems depend on data
- distinguish between data needed for a service and data collected for additional purposes
- recognize that combining separate pieces of data can reveal sensitive information
- explore the meaning of privacy, consent and data protection
- develop questions to ask before sharing personal information



MATERIALS

- Personal data cards
- AI system or service cards
- Purpose cards
- Three category signs: SHARE, SHARE WITH CONDITIONS and DO NOT SHARE
- A board, flip chart or large sheet of paper
- Markers
- String, arrows or adhesive notes for creating data trails
- Optional privacy decision worksheets
- Optional role cards for the challenging variation

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



MATERIALS

Suggested personal data cards include:

- first name
- age
- photograph
- voice recording
- location
- school or workplace
- search history
- messages
- contacts
- shopping history
- health information
- heart rate
- sleeping patterns
- fingerprints
- facial image
- favourite music
- device information
- movement inside the home
- food preferences

Suggested AI system cards include:

- homework assistant
- fitness application
- smart speaker
- video platform
- navigation application
- health-monitoring bathroom
- smart kitchen
- social-media platform
- online shop
- emotion-recognition system
- hospital diagnostic system
- household robot



MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



PREPARATION

Place the three category signs in different parts of the room or on a large table:

- **SHARE**
- **SHARE WITH CONDITIONS**
- **DO NOT SHARE**

Prepare four or five fictional service scenarios. Each should explain:

- what the service promises to do
- which data it requests
- why it says the data are needed
- whether the data may be stored or shared

For example:

A smart bathroom monitors heart rhythm and other health information. It can alert the user to possible health concerns. The company also asks permission to store the information to improve future products.

Do not ask participants to reveal whether they personally use particular services or disclose real private information.

INTRODUCTION

Ask the participants:

- What does the word “data” mean?
- What information might a phone or application know about someone?
- Why do AI systems need data?
- Is all personal data equally sensitive?
- Does agreeing to share one piece of information mean it can be used for every purpose?

Explain: Data can help AI systems recognize patterns, personalize services and make predictions. However, personal data can also reveal information about our identities, behaviour, health, interests and relationships. Today, we will decide what information different systems genuinely need and what conditions should apply.

Emphasize that participants may have different privacy preferences. The purpose is to explain and examine decisions, not to establish one correct answer for every situation.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



INSTRUCTIONS

1) SORT INDIVIDUAL DATA CARDS

Show one data card at a time, beginning with relatively simple examples such as favourite colour, first name or music preference.

Ask participants to place each card under:

- **SHARE**
- **SHARE WITH CONDITIONS**
- **DO NOT SHARE**

Invite several participants to explain their choices.

For **SHARE WITH CONDITIONS**, ask what the conditions might be:

- only with permission
- only for a specific purpose
- only with a trusted organization
- only for a limited time
- only if it is not shared with others
- only if it is protected securely
- only if it can be deleted later

Point out that the same information may be harmless in one context and sensitive in another.

2) MATCH DATA WITH A SERVICE

Divide participants into small groups. Give each group one AI system card and a selection of data cards.

Ask groups to sort the information into three categories:

- Necessary for the service
- Possibly useful but not necessary
- Unrelated to the service

For example, a navigation application may require the device's current location to provide directions. It probably does not need health information or private messages.

Groups present their decisions.

3) INTRODUCE THE PURPOSE

Give each group a purpose card that changes how the data will be used.

Possible purposes include:

- provide the requested service
- improve the AI system
- personalize recommendations
- display targeted advertisements
- conduct scientific research
- sell or share information with business partners
- keep information for future unspecified uses

Ask whether participants' willingness to share changes when the purpose changes. Explain that consent should relate to a clear purpose. Data provided for one reason should not automatically be used for every other reason.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



INSTRUCTIONS

4) TRACE A DATA JOURNEY

Choose one fictional service, such as a health-monitoring bathroom.

Create a data trail on the board:

1. A sensor collects health information.
2. The information is sent to the service provider.
3. An AI system analyses it.
4. The system produces a health alert.
5. The information is stored.
6. It may be accessed by authorized staff or another organization.

Ask at each stage:

Who has the data now?

Why do they need it?

How long should they keep it?

What could happen if it were inaccurate?

What could happen if an unauthorized person accessed it?

Should the user be able to delete it?

Use string or arrows to show how quickly one piece of information can move between several actors.

5) COMBINE DIFFERENT PIECES OF DATA

Display several apparently ordinary data cards:

- location
- shopping history
- sleeping patterns
- search history
- food preferences

Ask what might be inferred when these data are combined.

Possible inferences include:

- where someone lives or spends time
- daily routines
- interests
- possible health concerns
- religious or cultural practices
- relationships or social connections

Explain that an AI system may make predictions from combinations of data, even when the person never directly provided that conclusion.

Clarify that predictions can also be wrong.

6) EXAMINE CONSENT

Present a fictional request:

To use this homework assistant, you must allow it to collect your location, contacts, voice recordings and browsing history.

- Ask:
- Is all this information necessary?
- Is the choice genuinely voluntary if the service cannot be used otherwise?
- Is the request understandable?
- Could the service collect less information?
- Should children and adults receive the same consent request?
- Who should protect children's data?

Groups rewrite the request so that it is clearer and collects only what is necessary.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



INSTRUCTIONS

7) CREATE A PRIVACY CHECKLIST Develop a shared checklist titled **BEFORE I SHARE**:

1. What information is being requested?
2. Why is it needed?
3. Is all of it necessary?
4. Who will receive it?
5. How long will it be stored?
6. Will it be shared with anyone else?
7. Can I refuse without losing an essential service?
8. Can I correct or delete it?
9. What could happen if it is inaccurate or exposed?
10. Who can help me decide?

DISCUSSION AND REFLECTION

Ask the participants:

- Did your decisions change depending on the service?
- Which types of data felt most sensitive?
- Can ordinary information become sensitive when combined?
- Should a system collect data simply because it may be useful later?
- What makes consent meaningful?
- Who benefits when data are collected?
- Who carries the risk?
- Can an AI prediction reveal something a person never directly shared?
- What happens if the prediction is wrong?
- Should people be able to use a service without accepting unnecessary data collection?
- Who should be responsible for protecting personal data?

Conclude with the key idea: Data can make AI services useful, but people should understand what is collected, why it is needed and what happens to it. Responsible systems should collect only the necessary data and protect the people represented by those data.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



CONNECTION TO ARTIFICIAL INTELLIGENCE

AI systems use data to identify patterns, make predictions and personalize results. Depending on the application, the data may include:

- images and voice recordings
- location and movement
- health measurements;
- searches and viewing history
- purchases and preferences
- interactions with connected devices
- information generated by sensors

Some systems process data immediately on the device, while others send it to remote servers. Data may also be stored to improve a service or train future systems.

AI can infer additional information by combining data. For example, location patterns may suggest where someone lives or works. Shopping and search histories may be used to predict interests. Sensor data may indicate possible health changes.

These predictions are not guaranteed to be correct. Nevertheless, they can influence recommendations, advertising, access to services or decisions about people. Privacy protection therefore involves both the original data and the conclusions drawn from them.

EASIER VARIATION

Use three familiar services:

- a map application
- a video-recommendation service
- a fitness tracker

Give groups six data cards and ask which information each service needs.

Use simple questions:

- Does it need this information to work?
- Would you ask a trusted adult before sharing it?
- What could happen after it is shared?

Limit the activity to SHARE, ASK FIRST and DO NOT SHARE.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



MORE CHALLENGING VARIATION

Assign participants different roles in a fictional smart-home project:

- resident
- technology company
- doctor
- parent or caregiver
- researcher
- advertiser
- data-protection representative

Each role decides:

- which data it wants
- why it wants them
- what benefit this may provide
- what risk it creates
- what limits should apply

The smart home can monitor:

- energy use
- food consumption
- sleep
- movement
- heart rate
- voice commands

The group then negotiates a shared data agreement covering:

- purpose
- access
- storage period
- security
- deletion
- human review
- use for training future AI systems

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



FACILITATOR NOTES

- Do not ask participants to disclose real health information, passwords, locations or personal experiences.
- Use fictional scenarios throughout the activity.
- Accept that privacy preferences vary between individuals and cultures.
- Avoid implying that users carry all responsibility. Organizations that design and operate systems also have duties.
- Distinguish between data necessary to provide a service and data collected for secondary purposes.
- Explain that removing names does not always make data completely anonymous, particularly when several datasets can be combined.
- Do not suggest that all data collection is harmful. Discuss both benefits and risks.
- Emphasize that consent should be informed, understandable and freely given where consent is the appropriate basis.
- For younger participants, encourage consultation with a trusted adult before sharing personal information.
- Avoid providing specific legal advice, as privacy laws differ between countries.
- Explain that security reduces risk but cannot guarantee that data will never be exposed.
- Reinforce that children's personal data require particular care and protection.

MY DATA, MY CHOICE

PRIVACY AND SURVEILLANCE



KEY WORDS

PERSONAL DATA

Information connected to an identifiable person.

SENSITIVE DATA

Information that could create particular risks if misused, such as health or biometric data.

PRIVACY

A person's ability to control access to information about themselves.

CONSENT

A clear and informed agreement to a particular use of data.

PURPOSE

The specific reason for collecting or using data.

DATA MINIMIZATION

Collecting only the information necessary for a defined purpose.

INFERENCE

A conclusion or prediction drawn from available data.

BIOMETRIC DATA

Measurements connected to physical or behavioural characteristics, such as fingerprints, facial features or voice patterns.

DATA SECURITY

Measures used to protect information from unauthorized access, loss or misuse.

