Privacy

Responsible AI: Human-Centered Design

Course 1
Fundamentals of TinyML

- **What** am I building?
- **Who** am I building this for?
- What are the **consequences** for the user if it ***fails***?

Course 2
Applications of TinyML

- **What data** will be collected to train the model?
- Is the dataset **biased**?
- How can we **ensure** the model is **fair**?

Course 3
Deploying TinyML

- How will model drift be monitored?
- How should security breaches be addressed?
- How should the user's **privacy** be protected?

Why is privacy **valuable**?

- Prevent **information-based harms**
  - Minimize opportunities for hackers to gain inappropriate access to data
- Prevent informational **injustice** and **discrimination**
  - Consider the context, the type of information, and who has access
- Preserve **autonomy** and **human dignity**
  - Obtain informed consent

How can **privacy be preserved**?

- **Minimize**
  - Avoid collecting unnecessary data, and dispose or delete data periodically
- **Protect**
  - Use encryption techniques to protect data
- **Map the flow of information**
  - Context, the type of information, and who has access
- **Informed consent**
  - Be transparent with users about how their data is being collected and used