

Solving Problems

(Design Ethnography, Participatory Design, and Value-Sensitive Design)

Mo El-Haj



What's the point?

- Computer science is about solving problems (not about programming)
- Employers expect you to be able to:
 - Look at the whole picture in planning a solution
 - Understand the problem that has been set (and why)
 - Understand the environment its being designed for
 - Understand the limitations
 - Create a solution that meets all essential criteria (and even some non-essential ones!)

Previously – Design Process Overview

- **Initial Research & Prototype Development**
- Completed with **surveys, personas, and initial design.**
- Prototype built based on early insights and tested in a controlled environment.

What you will learn today


Part 1: Design Ethnography

- Observe how users interact with the prototype in real settings, uncovering real-world challenges.

Part 2: Participatory Design

- Actively involve users in refining the design, using their insights to minimise risks.

Part 3: Value-Sensitive Design

- Integrate ethical and social values into the design to align with broader success criteria.
- 

PART 1: Design Ethnography

**Case study on: Avoiding silly mistakes and seeing opportunities
for innovation**

Smart Yoga Mat



Power on the Mat



Pair the Mat with the YogiFi App



Select a Program or Class



Follow the Instructions and Practice the Poses

Design Ethnography



*A professional
observer of the
ordinary.*

Design Ethnography

- Design Ethnography is:
 - A method that involves studying people in their natural environment
 - Earliest step in development lifecycle, informs whole process
 - Avoiding silly mistakes and seeing opportunities for innovation
- It involves:
 - Being embedded in an environment (fieldwork)
 - Observing / documenting
 - Asking questions (Interviewing)
 - Exploring solutions with users (co-design)
 - Analysing (reflection, creativity)
 - Communicating insights to a development team
 - Steering the design process

Question your assumptions

1. Is the environment different from where the device has been previously tested and deployed successfully? (e.g. Smart Yoga Mat)

- **Example:** The smart yoga mat was tested in a quiet studio with stable Wi-Fi, but now it's being used outdoors or in areas with less reliable connectivity.

Question your assumptions

2. Which rules are flexible and open to change in this context?

- **Example:** In a home setting, users may want personalised data collection with fewer privacy restrictions, whereas a gym might have stricter data protection rules.

Question your assumptions

3. What are the diverse motivations of the people involved or impacted?

- **Example:** A beginner might be focused on improving flexibility and enjoying the practice, while an advanced yogi may want detailed posture feedback to perfect their alignment (remember diversifying your users/personas to avoid bias).

Question your assumptions

4. Are you addressing the right problem, or could there be a more critical one to solve?

- **Example:** The initial design might focus on tracking postures precisely, but users might be more concerned with comfort and usability (how easy the mat is to set up or clean).

Question your assumptions

5. If you solved a related problem, could it eliminate the need to address this one?

- **Example:** Instead of improving the mat's accuracy in detecting tiny alignment errors, focusing on teaching users how to adjust their alignment intuitively could reduce the need for high precision (we are not all shaped the same)

The solution (and why it worked)

•Problem Before

- Strict alignment cues frustrated users (we're not all shaped the same).


•Key Insight

- Users wanted flexible feedback that could adapt to their own pace and comfort.

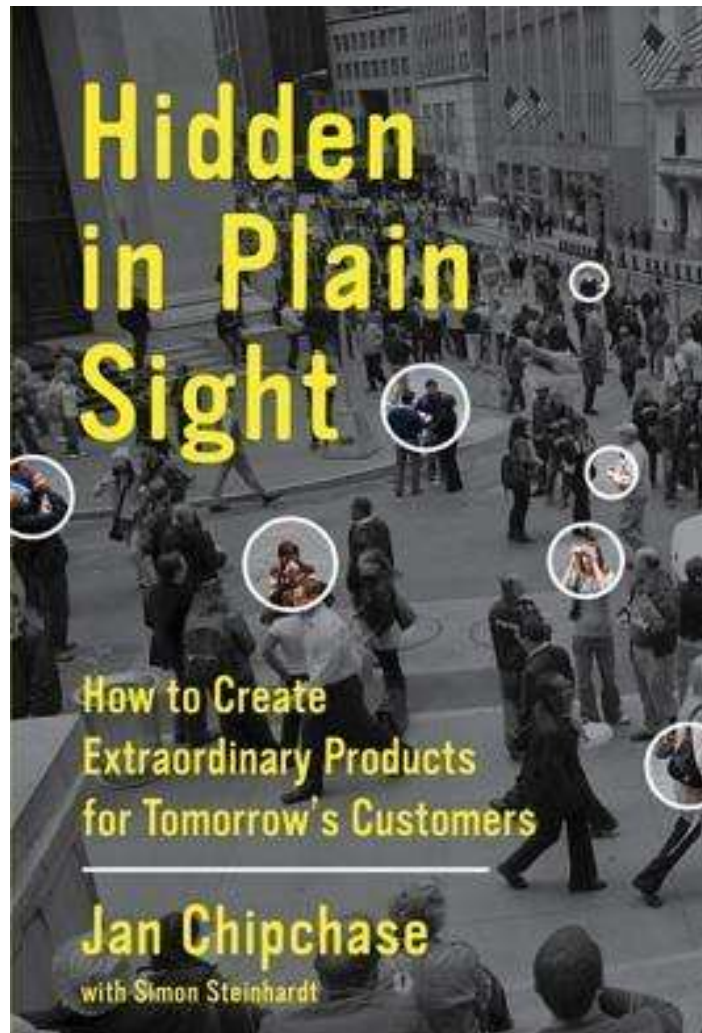
•Our Solution

- Added personalised alignment ranges to allow for “ideal” and “comfort” zones, offering supportive rather than prescriptive guidance.

•Outcome

- Increased user satisfaction, reduced injury, and higher engagement by adapting to individual needs.
- 

Design Ethnography



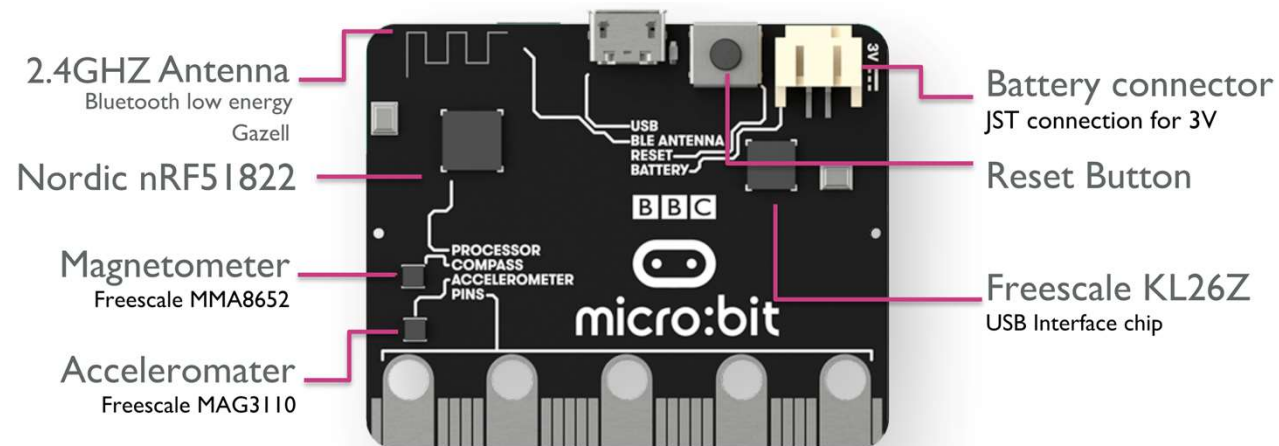
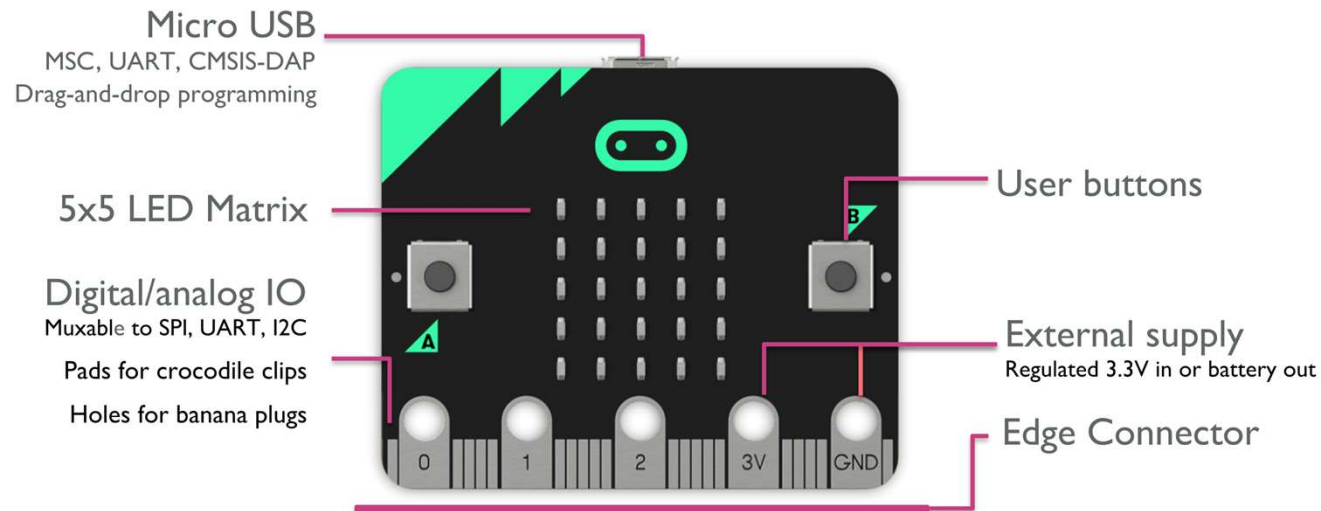
"Every new technology put out on the market is introduced with assertions and assumptions about how it will be used, but it's only through actual experience that 'use' is defined, shaped by any number of factors including context, personality, motivation, and income."

PART 2: Participatory Design

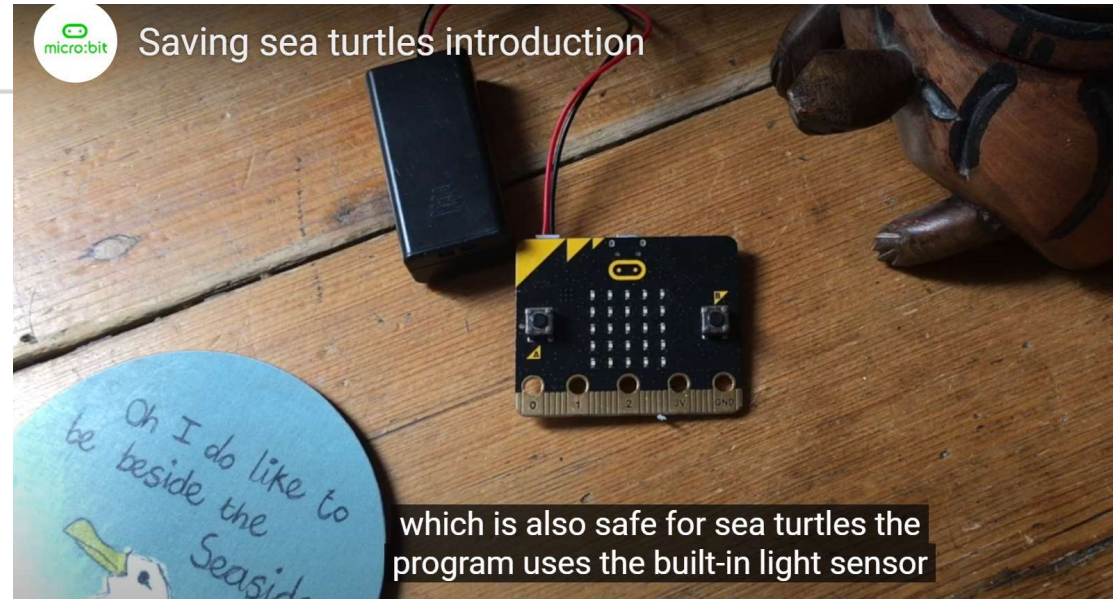
Case study on: Risk mitigation

The micro:bit

<https://microbit.org/>

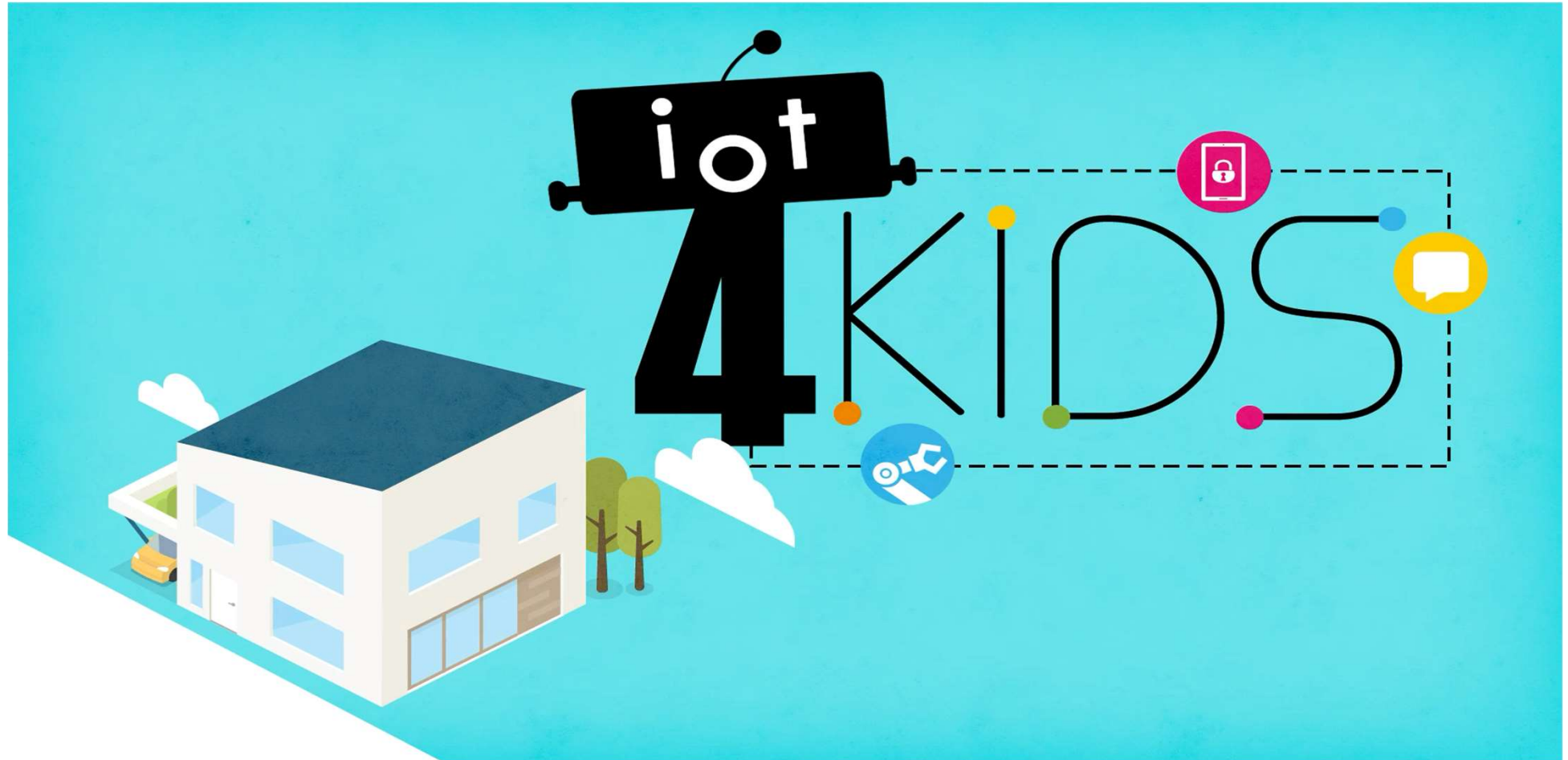


The micro:bit



- **Safe Beach Lighting:** The micro uses LED light sensors to guide people along beach paths at night without distracting sea turtle hatchlings from reaching the sea.
- **Adaptive Lighting:** The micro activates based on low light levels, demonstrating technology's role in protecting wildlife through sustainable design.

IoT4Kids project

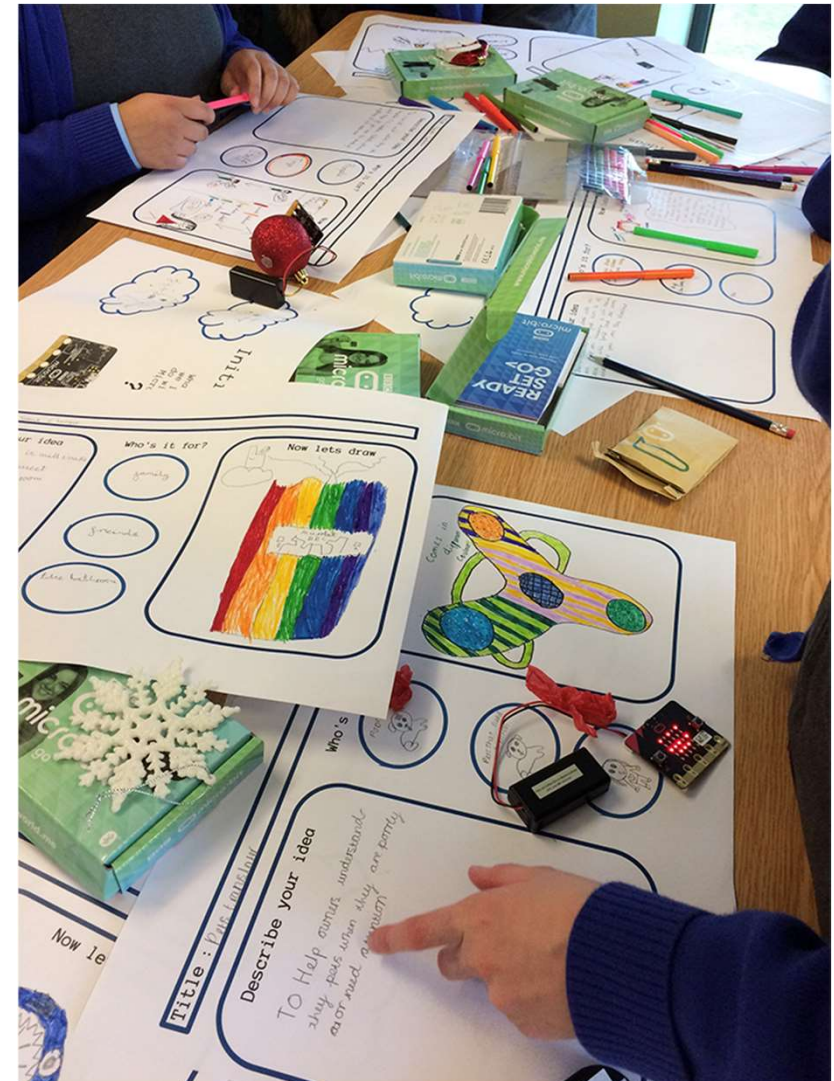


The micro:bit was created to teach children programming in a fun, engaging way, but it introduced privacy, safety, and security concerns, especially as children began programming Internet-of-Things devices.

<https://vimeo.com/255042078/2705892db4>

Children as participants

Understanding how children, aged 9-11, would use the micro and whether their ideas could lead to any safety or security risks.



Children as participants

- **Kids' Designs Reveal Potential Risks:** Children's creative ideas with micro, such as location tracking and reminders, highlighted possible privacy and security risks.
- **Identifying High-Risk Data:** Their designs often included sensitive data (audio, video, location), helping researchers spot privacy concerns early on.



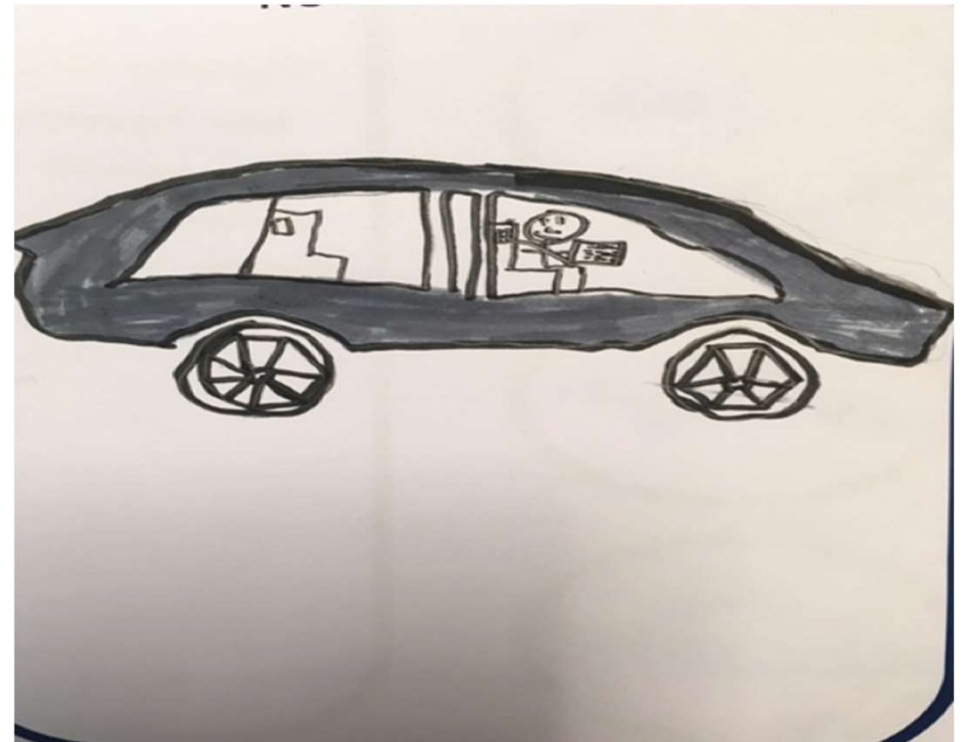
"Your Robot Helper"



"Micro:Voice"

Children as participants

- **Risky Play Interests:** Designs like virtual reality scenarios and remote control reflect children's curiosity about adult-like risky behaviour.
- **Understanding Morality:** These ideas highlight the need to guide children on responsible tech use, as they may not fully grasp consequences of unseen actions.



“The micro:bit Car VR”

Using personas

- **Creating Personas:**

Researchers developed fictional child characters based on the children's design ideas.

- **Detailed Scenarios:** Each persona included a backstory and motivations for their designs.

- **Identifying Risks:** Personas helped illustrate specific risks associated with different types of device use, like companionship risks.

Freya

Freya is twelve years old. Her father has left the family and she misses a male role model. Her mother is busy with the other younger children and work, so Freya spends much of her time in her bedroom on computers and has recently expanded her interest to include making and tinkering with gadgets. She is often lonely and has become withdrawn due to some recent incidents of having been bullied.

Freya has discovered online forums and YouTube videos on how to make and build physical computing concepts. She built her first interactive toy—a teddy bear that opened and closed its mouth using a micro:bit and servos—by following instructions provided to her in an online forum. For her next attempt, she followed online guidance to connect an audio interface, including a microphone and speaker into her soft toy shark, and with the code supplied by a forum contributor she was able to program the speech interface that enabled her to ask Sharkie a question and get a response. The device consists of a micro:bit, microphone and speakers, and uses blocks from an unlicensed code library extension to connect to Internet speech recognition and a search engine to return and speak back results.

“This highlight how early assumptions can reveal risks and inform the next stages of design. “

Risk Mitigation Checklist

Risk Zone 1: Authority and Discipline

- Will the technology undermine authority, and what might the consequences of this be?
- What might the technology enable children to see or do that they haven't been able to before? Are carers or other authority figures aware the child has these new capabilities? If not, would they approve if they were to find out?
- Does the technology afford covert interactions? Is it important that others are able to tell when a child is using the technology?
- Does the technology enable a child to escape punishment for something they would otherwise be punished for? What risky behavior might children engage in as a result that they otherwise wouldn't?
- Does use of the technology need to be supervised? How likely is it that an adult would be able to supervise this activity?
- Would that supervising adult be sufficiently knowledgeable to protect the child from risks?

Risk Mitigation Checklist

Risk Zone 2: Malevolence and Accidental Harm

- How might the technology or data produced by it be used by a malevolent actor? Is there any way to identify malevolent users? How will malevolent users be policed?
- For any given use of the technology, what would it look like if a user 'took it too far'?
- Are those with whom a user interacts able to determine that user is a child? What are the risks of those entities knowing they are interacting with a child? What are the risks of those entities not knowing?

Risk Mitigation Checklist

Risk Zone 3: Emotionality and Socialization

- Does the technology appeal to emotionally vulnerable children?
- If so, how might the technology intensify these vulnerabilities?
- Does the technology isolate children? If designed differently, how might it foster real world socialization?
- What emotional state does the technology foster? Is this conducive to deliberation and responsible decision making?

Risk Mitigation Checklist

Risk Zone 4: Governance and Accounting

- Will people be producing content or components that extend the original functionality of the technology? How will these individuals and content/components be vetted?
- What tools and services would users interact with as part of normal use of the technology (e.g. servers)? Is it preferable and possible to build a secure ecosystem that supports interaction from start to finish?
- Is it obvious to a child when they are generating data and where it is going? Is this information presented in a way that promotes informed consent?


PART 3: Value-Sensitive Design

Case study on: Questioning success criteria for AI systems

Value-Sensitive Design

- Designing a system “right” means making sure it respects and supports human values.

Example: Autonomy

- People should be able to make choices that help them reach their goals.
 - This includes giving users control over relevant features at the appropriate times.
 - Computer scientists should consider what values the system promotes and supports.
- 

Example: AI for granting loans

- **False positive (FP):** granting a loan to someone who turns out to be untrustworthy (who does not pay it back)
- **False negative (FN):** denying a loan to someone who would have been trustworthy (who would have paid it back)

FP	FN
0	0

IDEAL

Example: AI for granting loans

- **False positive (FP):** granting a loan to someone who turns out to be untrustworthy (who does not pay it back)
- **False negative (FN):** denying a loan to someone who would have been trustworthy (who would have paid it back)

FP	FN
0	0

IDEAL

FP	FN
0	10

OPTION 1

Example: AI for granting loans

- **False positive (FP):** granting a loan to someone who turns out to be untrustworthy (who does not pay it back)
- **False negative (FN):** denying a loan to someone who would have been trustworthy (who would have paid it back)

FP	FN
0	0

IDEAL

FP	FN
0	10

OPTION 1

FP	FN
10	0

OPTION 2

Example: AI for granting loans

- **False positive (FP):** granting a loan to someone who turns out to be untrustworthy (who does not pay it back)
- **False negative (FN):** denying a loan to someone who would have been trustworthy (who would have paid it back)

FP	FN
0	0

IDEAL

FP	FN
0	10

OPTION 1


FP	FN
10	0

OPTION 2

FP	FN
5	5

OPTION 3

Humble AI

- **Humble AI Concept:** An AI approach focused on ensuring trustworthy people are not unfairly distrusted, promoting fair, merit-based opportunities.
 - **Challenge:** Balancing fairness without increasing false positives (trusting untrustworthy individuals).
- 

Humble AI

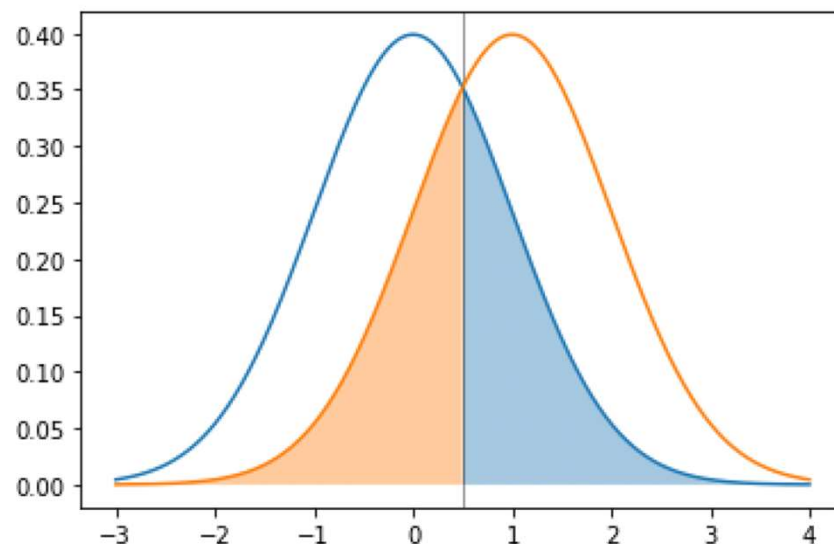
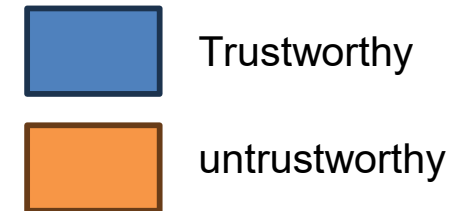
1. Principle of Skepticism

- Goal:** Assume AI might be missing critical information for decision-making.
- Approach:** Seek additional data, especially for cases near the decision threshold, to reduce errors.
- Example:** Non-traditional lenders like Indigenous Business Australia which grants loans based on a measure of how much a person has helped others in their community.

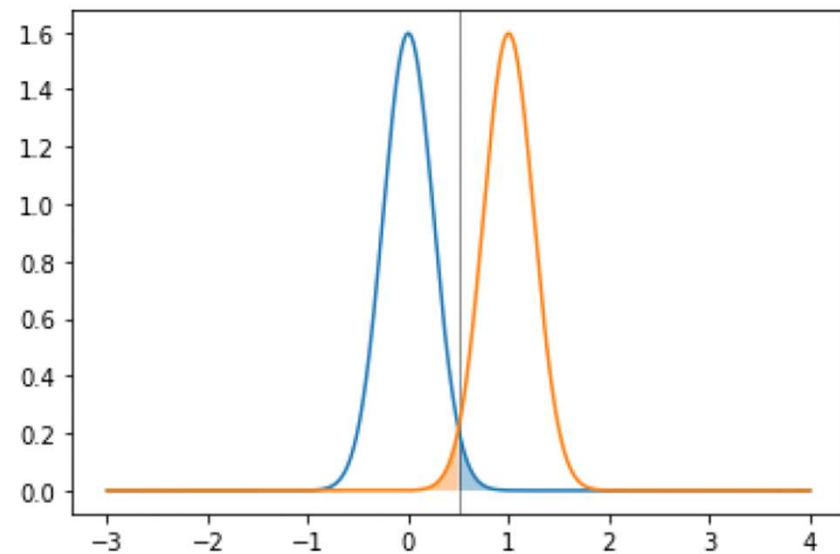
Humble AI (Principle of Skepticism)

•**Left Chart:** High overlap means the model struggles to separate trustworthy from untrustworthy individuals, leading to more errors (false positives and false negatives).

•**Right Chart:** Minimal overlap shows a more accurate model with fewer errors, achieved by adding extra data to improve decision-making.



Instead of this...



...you want this.

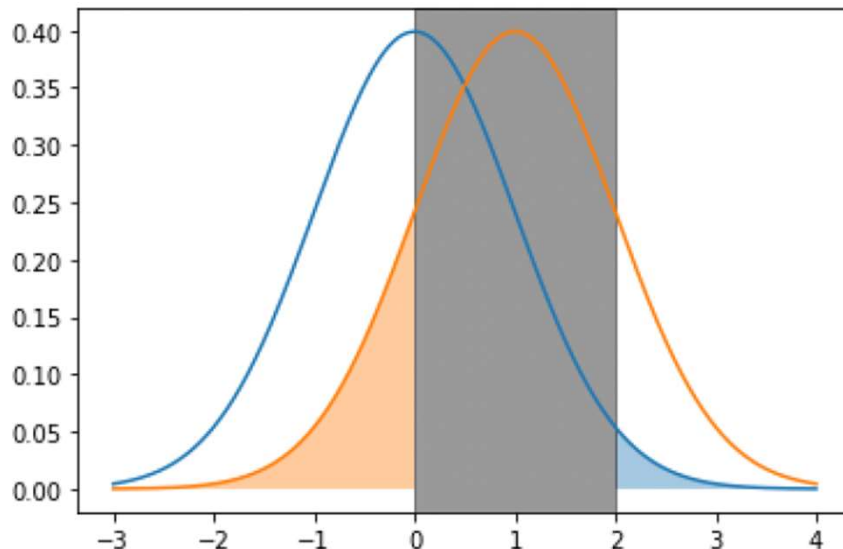
Humble AI

2. Principle of Curiosity

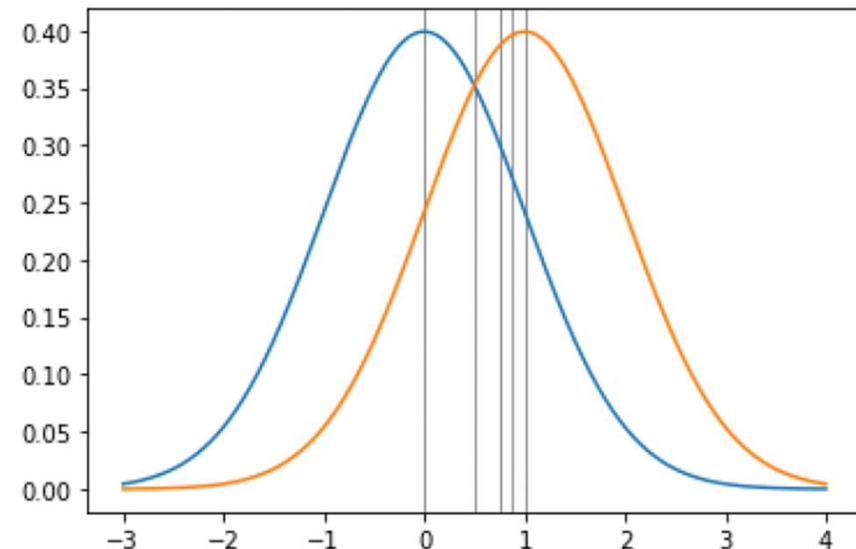
- Goal:** Learn from borderline cases by testing different decisions.
- Approach:** Use "safe exploration" to randomly grant opportunities (e.g., loans) to people close to the threshold and observe outcomes.
- Outcome:** Refines the decision threshold over time, helping the AI make more accurate, fair decisions.

Humble AI (Principle of Curiosity)

- **Left Chart ("Grey Area of Uncertainty"):** The threshold is treated as a flexible grey area, allowing the AI to test borderline cases and learn if they are trustworthy.
- **Right Chart ("Optimal Position"):** The AI refines the threshold over time, using data from the grey area to better separate trustworthy from untrustworthy cases, reducing errors.



Treat threshold as "grey area" of uncertainty



Threshold moves over time to optimal position

Win-Win

- Focusing on values does not necessarily mean you reduce profit
- Designing systems better in terms of values are often just all-around better