Advanced AI for Everyone

Pavol Chvala

Director, AI Innovation & Systems Development

IST

UNIVERSITY OF WATERLOO

Welcome!

Goals

- Understand how to choose the right tool, and get the most out of it
- Explore the people side of AI adoption
- Learn about the role AI plays in automation, and its risks

Question

What AI tools have you used in your work or personal life?

MANAGING CONTEXT

Understand how to choose the right tool, and get the most out of it

Tool selection

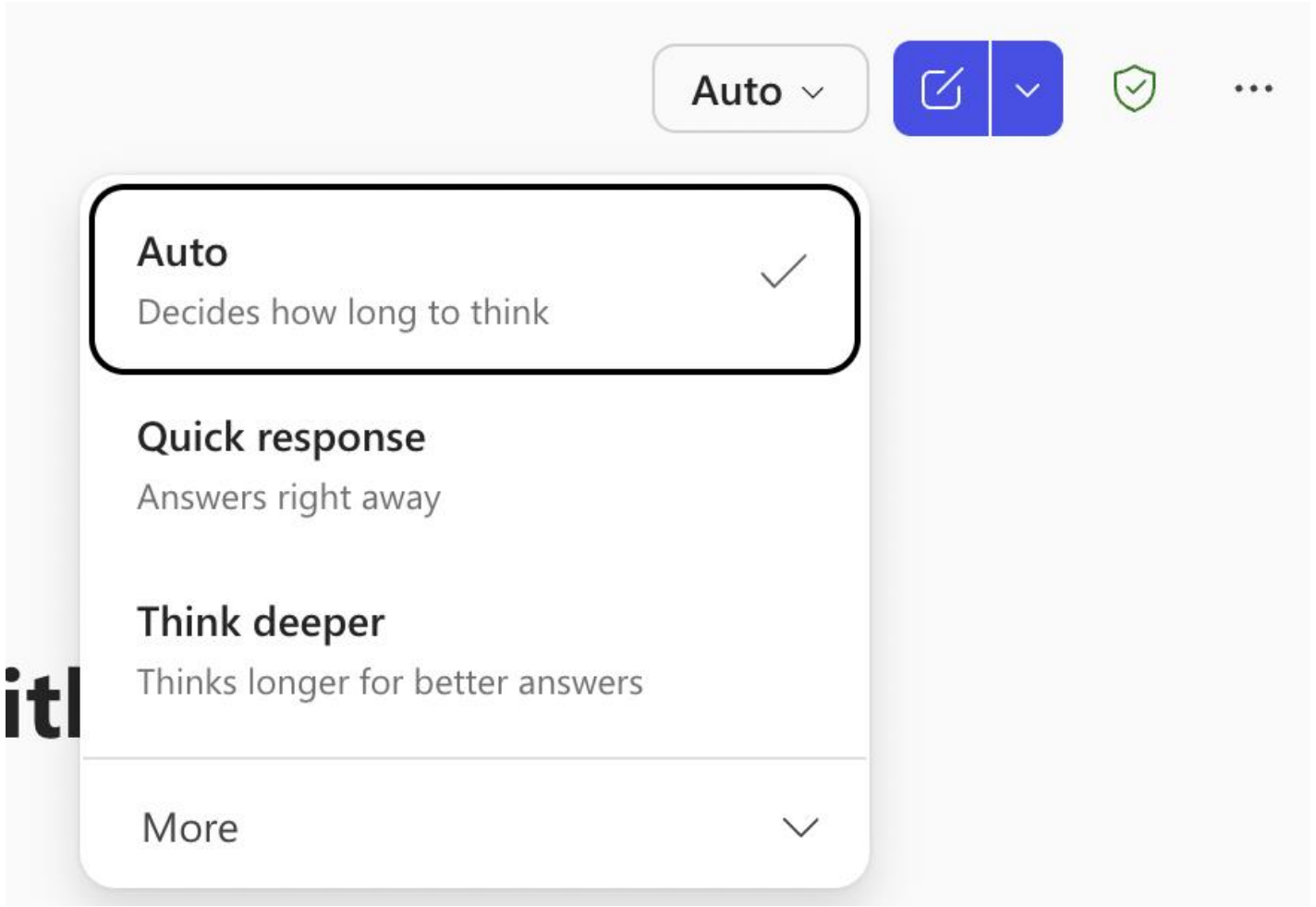
Tool types

- **Assistant** – simple QnA (text, images, music, videos, code…)
- **Reasoner** – complex “thinking” (multi-step QnA) (+ deep research)
- **Agent** – any combination of the above, with the ability to act by using tools
- **AI enabled applications** – browsers, media generators, …

Service types

- **Free SaaS** – good to get started, but typically restricted in some way
- **Paid Saas** – more advanced features and/or higher capacities
- **Open source** – free with full control over infrastructure and software, but high complexity

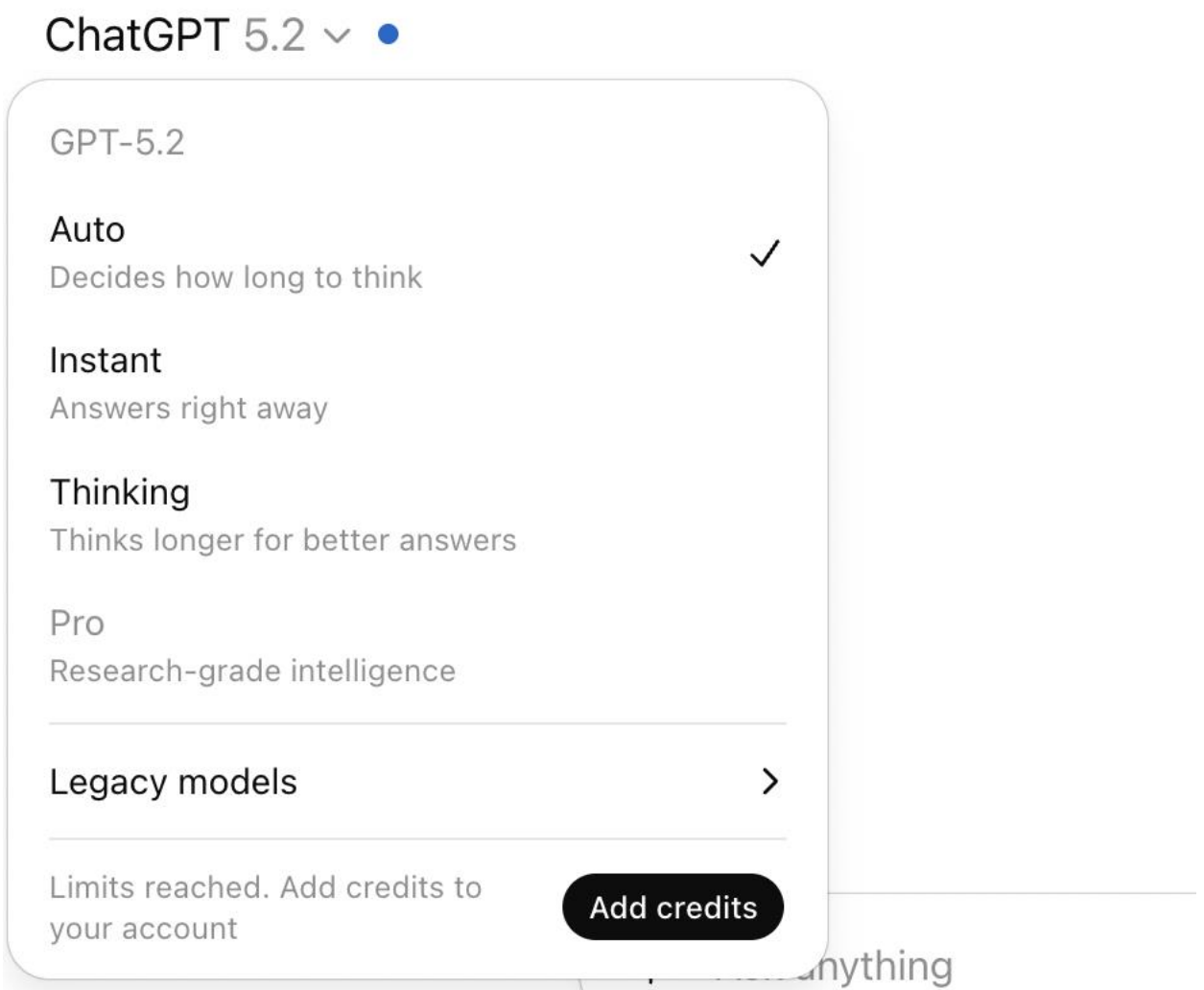
Microsoft Copilot



https://office.com

UNIVERSITY OF WATERLOO

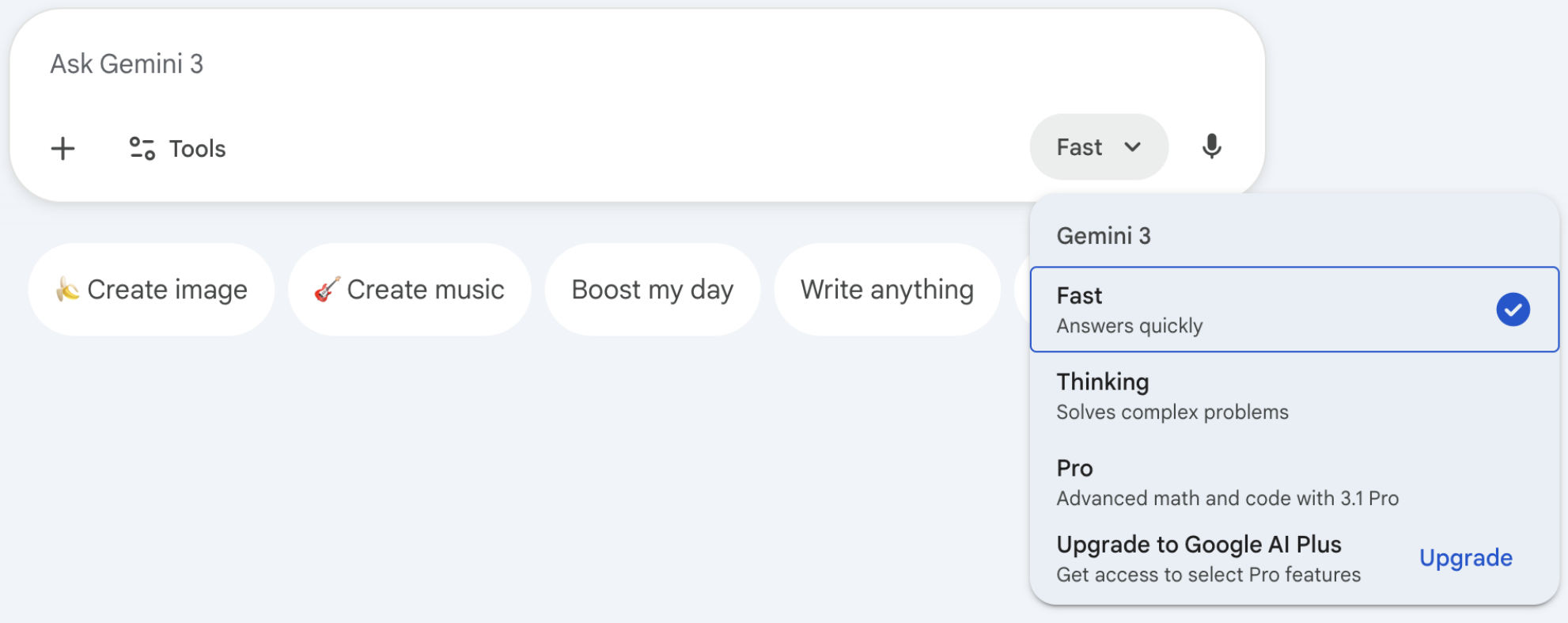
OpenAI ChatGPT



https://chatgpt.com

UNIVERSITY OF WATERLOO

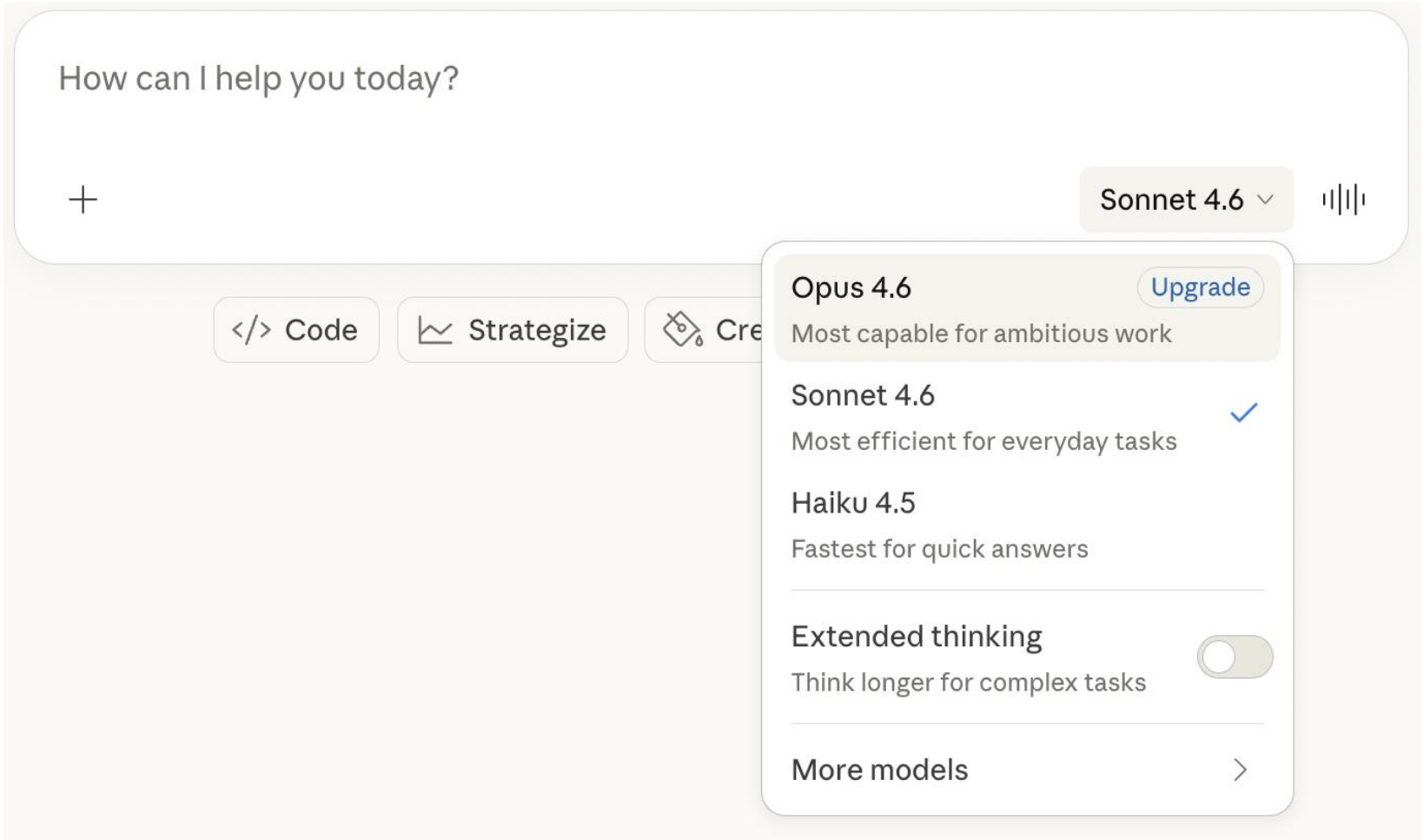
Google Gemini



https://gemini.google.com

UNIVERSITY OF WATERLOO

Anthropic Claude



https://claude.ai

UNIVERSITY OF WATERLOO

Open source (Ollama)

https://ollama.com

UNIVERSITY OF WATERLOO

Question

What are your favourite AI use-cases?

Some examples: Search, Draft, Refine, Finalize, Explore, Condense, Transform

PROMPTING TECHNIQUES

Exercise

Summarize a long document, transcript, email thread…

2025 UWaterloo Financial Report

Be clear, concise, and specific

Bad	Good
Tell me about climate change.	Summarize the main causes and effects of climate change on coastal cities and include recent scientific data if possible.
Write something about AI.	Write a 150-word blog post explaining how generative AI is being used in university classrooms in 2025.
Provide culinary procedural insights regarding starch-based Italian fare under 30 minutes.	Can you give me an easy pasta recipe that takes less than 30 minutes to cook?
Don’t make the presentation too long or too technical. Don’t use jargon. Don’t forget to make it interesting.	Create a 10-slide presentation for a general audience explaining AI basics. Keep the language simple, use visuals to explain key ideas, and aim for an engaging, story-driven flow.

UNIVERSITY OF WATERLOO

Providing examples

No examples (zero-shot)

- Quick and easy – high reliance on the model's knowledge to complete task

One example (one-shot)

- Requires a bit more effort, but useful in bounding the response (type, format, etc)

Multiple examples (few-shot)

- Requires much more effort, but can bound the context, format, match patterns, etc.
- Generally, 3-5 examples, depending on…
  - Complexity of task, quality of examples, capabilities of the model

UNIVERSITY OF WATERLOO

Setting up context

Role prompting

- Start by telling the model what role it is to assume: “You are a helpful writing assistant…”, “You are a marketing agent…”, “You are a senior software developer…”, “You are a travel agent…”

Context prompting

- Provide the context in which you are asking the question. The more details the better:

  “Context: You are building a website for the University of Waterloo which will promote an event for international students…

  Suggest some design ideas for the layout…”

UNIVERSITY OF WATERLOO

Step-back prompting

Get the model to answer a general question about your ask first and then feed that context into your specific question.

- “You are an HR assistant. Give me a job description for a senior web developer based on the following format {attached document}”

- “What are some of the most important skills that a senior web developer should possess, both technical and non-technical?”
  - “Context: {response from before, maybe modified}

    Give me a job description for a senior web developer based on the following format {attached document}”

UNIVERSITY OF WATERLOO

Exercise

Summarize a long document, transcript, email thread…

2025 UWaterloo Financial Report

BONUS: Prompt generation

Get the model to generate prompts for you!

- “I need to generate a new job description for a senior web developer. Give me 10 different prompts I can use with an LLM”
  - “Give me the strengths and drawbacks of these prompts”

Ask for prompts that combine any of the previous techniques

UNIVERSITY OF WATERLOO

BONUS: Code

While you may not be a software developer, LLMs are very good at writing code.

Need to script/automate something? Need to write a complex Excel formula?

- "I have the following table in Excel {rough table structure}. How do I highlight anomalous values?"
- "I have 2 excel spreadsheets with the following columns… and some sample data… I need to find out what users from sheet A appear in sheet B. How would I approach this problem?"
- "I copy a file from a network share every morning to a new folder, help me write code to automate this process.
  Now walk me through what I do with this code."

Explain code; translate code to a new language; look over code for issues …

UNIVERSITY OF WATERLOO

BONUS: Reusable prompts

If you are reusing a prompt often and just need to tweak some elements, use a **variables** section.

VARIABLES

{project} = "student information system upgrade”

{stakeholder} = "faculty administrators”

PROMPT

You are a senior project manager.

Provide a status update for the {project} tailored to {stakeholder}.

Highlight current progress, key risks, and upcoming milestones for the {project}.

Then recommend communication strategies to keep {stakeholder} engaged and informed throughout the remainder of the {project}.

UNIVERSITY OF WATERLOO

ADOPTION & TRUST

Explore the people side of AI adoption

The journey to an AI Enabled Team

1. **Learn**: foundational AI training + use-case identification
2. **Iterate**: habit forming and use-case scaling
3. **Standardize**: team transformation with confident AI use – The AI Enabled Team

1. Learn

What does it look like?

- Online courses
- Use-case trial and error
- Personal experimentation

Roadblock	Countermeasure
Lack of interest	Make it relevant Leadership & peer engagement Adoption curve (some individuals might need more time)
Lack of time	Empower champions Protected learning time & give challenges
Fear of making mistakes	Leadership messaging (experimentation is expected) Sandbox environments or use-cases

UNIVERSITY OF WATERLOO

2. Iterate

What does it look like?

- Repeated use leading to use-case refinement
- Understanding differences in AI tools & techniques
- Starting to understand the intersection of AI and automation (agents)

Roadblock	Countermeasure
Increase in productivity doesn't equate to quality	Definition of done Spot checks/peer review Set quality benchmarks
Data access	Green light zones
Tools & integrations	Approved tools list

UNIVERSITY OF WATERLOO

3. Standardize

What does it look like?

- Usage is habitual
- Team starts to self evaluate and iterate
- Adoption of new tools & techniques is openly discussed

Responsible AI Principles

AI tools and data guidelines

UNIVERSITY OF WATERLOO

Wrap-up

- The tech is accelerating, and nobody is an expert
- Use-case discovery is hard work
  - Must make time for experimentation
  - Share amongst team to accelerate
  - Green light zones & approved tool lists
- AI Enabled Team
  - Leadership must be engaged
  - Empower champions
  - Definition of done to set quality benchmarks

AUTOMATION & AUTONOMY

Learn about the role AI plays in automation, and its risks

Wouldn’t it be great if AI could…

Curricular overlap analysis with ChatGPT Agent

https://chatgpt.com/share/e/68dc2400-b1d8-8004-a128-808f845cac82

Question

If you could get AI to automate away any part of your work, freeing you up to do more valuable things, what would it be?

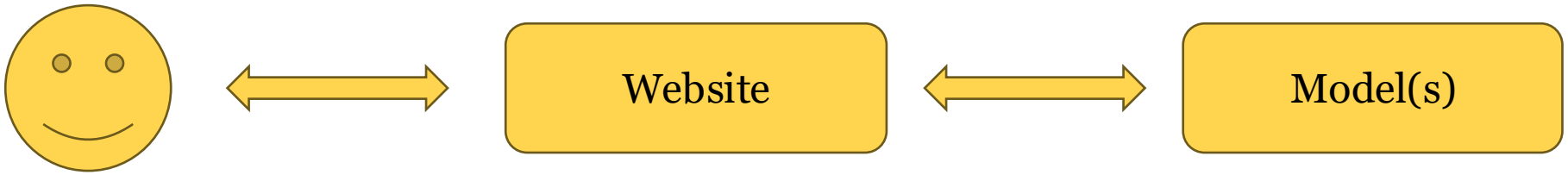
Let's back up for a moment...

Copilot, ChatGPT, Gemini, Claude, etc

The Chatbot Recipe

- 1 part - LLM trained on trillions of pieces of data
  gpt-5.2, claude opus 4.6, deepseek r1, qwen, llama, gemini 3, etc
- 1 part - website or desktop interface to make it functional for the average user
  chatgpt.com, gemini.google.com, etc

Chatbot

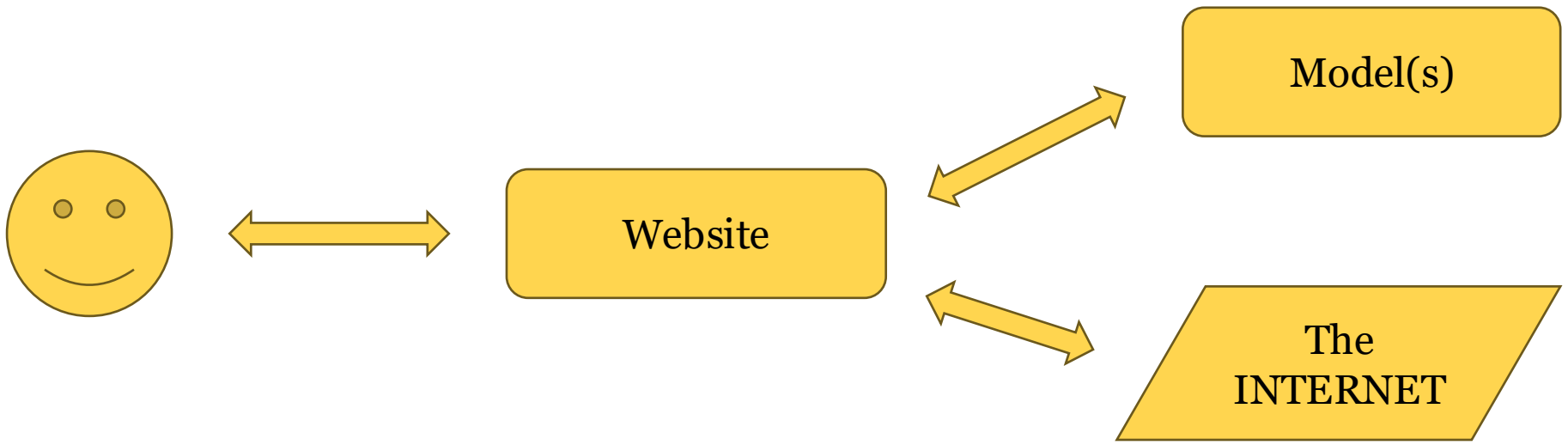


“Who is the President of the University of Waterloo?”

UNIVERSITY OF WATERLOO

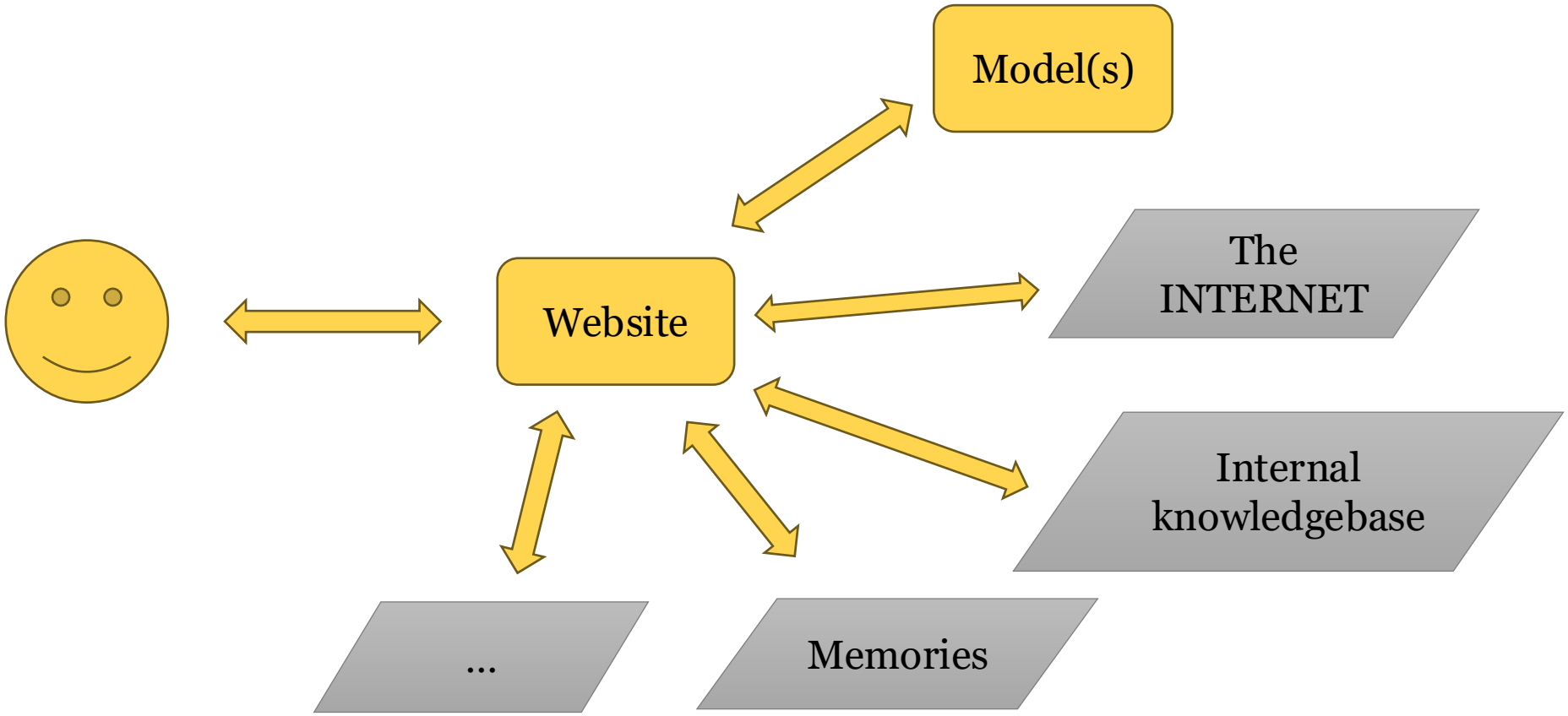
Chatbot

So, let's "fix" our chatbot…



Chatbot

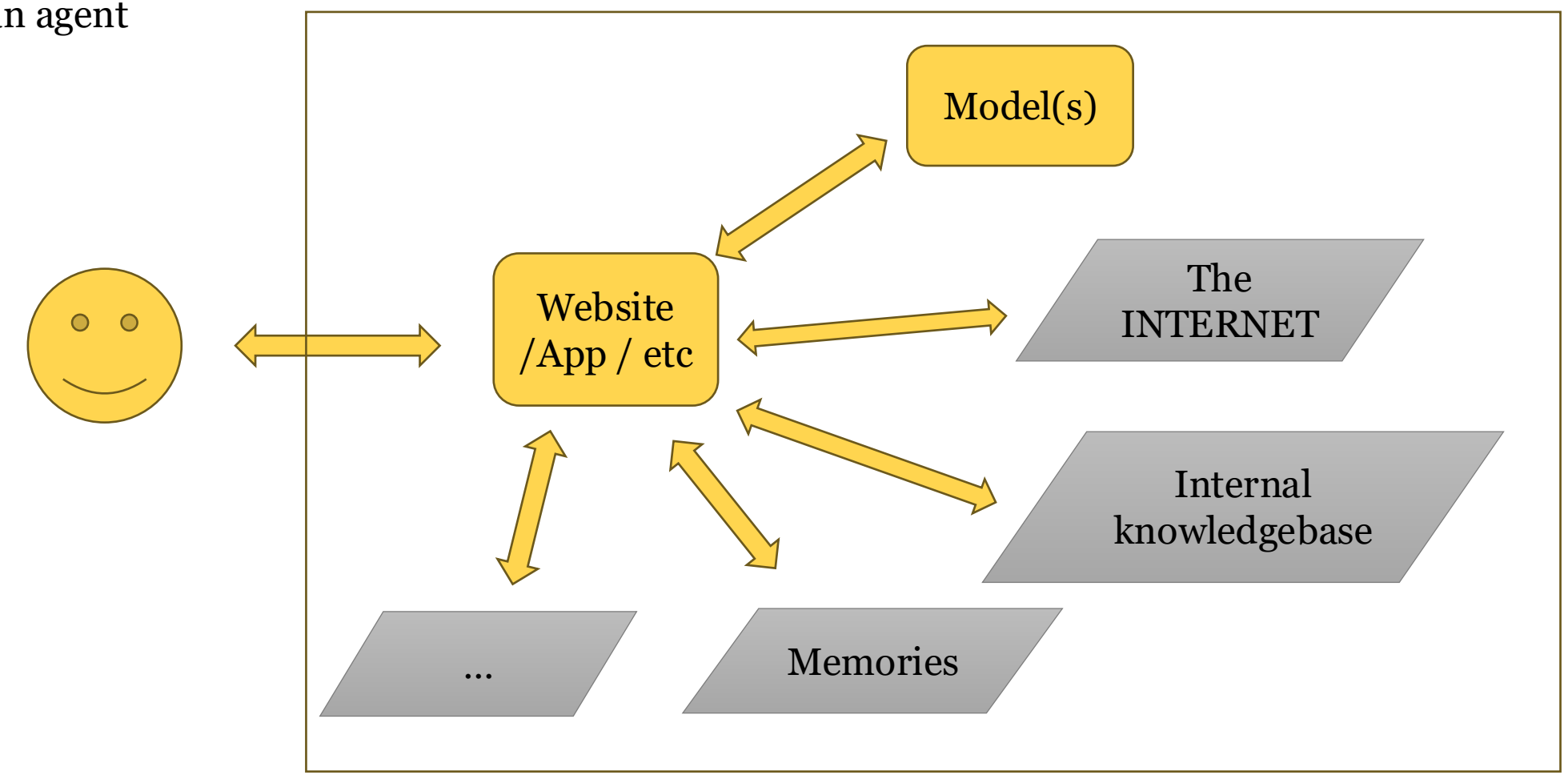
If we take it a few steps further…



Agent

Let's call this an agent

- Model
- Tools
- Data
- Memory



Risk Areas

- **Misaligned Goals**
  Agent optimizes the wrong objective or interprets intent incorrectly.
- **Uncontrolled Actions**
  Agent takes harmful or unauthorized actions.
- **Data Privacy & Security**
  Agent accesses or exposes sensitive information.
- **Lack of Accountability**
  Unclear ownership when the agent causes harm.
- **Over-Trust & Reduced Oversight**
  Overreliance on agent without sufficient review or judgement.

Responsible Principles

- **Misaligned Goals**
  Define clear objectives, constraints, and success criteria before deployment.
- **Uncontrolled Actions**
  Limit permissions and require approval for high-impact actions.
- **Data Privacy & Security**
  Apply least-privilege data access and continuous monitoring controls.
- **Lack of Accountability**
  Assign a named business, technical, and risk owner for every agent.
- **Over-Trust & Reduced Oversight**
  Design meaningful human review checkpoints and train users on limitations.

UNIVERSITY OF WATERLOO

Thank you!

pchvala@uwaterloo.ca

https://uwaterloo.ca/genai/