INSIGHT 13

AI AGENTS COULD ACT AS A PERSONAL ASSISTANT WITH MINIMAL GUIDANCE

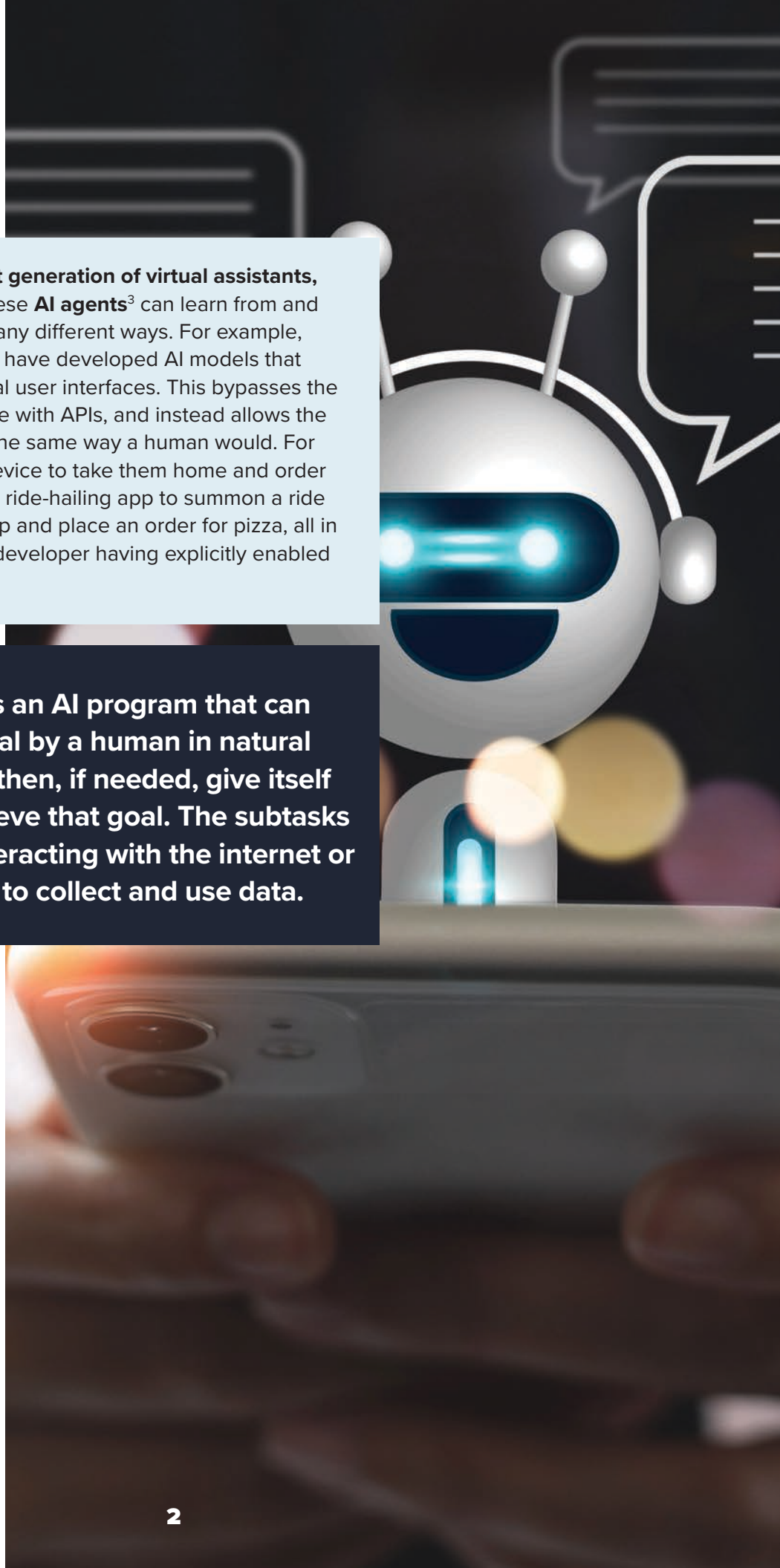
In the future, people could have a general-purpose AI agent acting as a personal assistant, capable of performing multi-step tasks for its user, 24/7. Impacts could include improved access to task automation, greater productivity, disruption of advertising-based business models, and unforeseen harms.

TODAY

Virtual assistants currently have limited functionality. Products like Siri or Alexa can only perform tasks that they are specifically programmed to do in response to carefully worded prompts. Although they are promoted as having a wide array of capabilities, they are mostly used to ask for weather forecasts or information on local businesses.[1] Their ability to integrate with third-party apps depends on the developers of those apps voluntarily incorporating the assistants' API (application programming interface), a way for different pieces of software to exchange data.[2] Even when third-party apps and virtual assistants are designed to work together, the assistants often cannot act fully autonomously. For example, when ChatGPT enabled Instacart to create a shopping list after planning a meal, the ChatGPT user still had to step in to actually buy the items.

AI agents are emerging as the next generation of virtual assistants, capable of independent action. These **AI agents**[3] can learn from and interact with their environment in many different ways. For example, companies like Apple[4] and OpenAI[5] have developed AI models that can parse and interact with graphical user interfaces. This bypasses the need for app developers to integrate with APIs, and instead allows the AI model to interact with an app in the same way a human would. For example, the user could ask their device to take them home and order pizza, and an AI agent could open a ride-hailing app to summon a ride home, then open a food delivery app and place an order for pizza, all in a single command without the app developer having explicitly enabled such integrations.

An AI agent is an AI program that can be given a goal by a human in natural language, and then, if needed, give itself subtasks to achieve that goal. The subtasks could involve interacting with the internet or other agents to collect and use data.



FUTURES

AI agents could become more commonplace and capable of acting as a personal assistant. For instance, a user could ask their AI agent to organize a dinner with a friend at a certain restaurant. The user's AI agent could reach out to the friend's AI agent, compare calendars to find available times, create a calendar entry, contact the restaurant to make a reservation, then schedule a rideshare to pick up the friends before dinner. Agents could also be given standing orders, such as filling out and returning an attendance form whenever it is sent by their child's daycare.

AI agents could make automating tasks more accessible. Rather than requiring the use of complex or intimidating specialised software or the ability to write in programming language, a human could simply describe what they want in natural language and let the agent work out the technicalities of implementing the request.

AI agents could make chatbots feel more like people. Instead of being a passive participant in a conversation – only responding to the user, but never initiating or leading the conversation – chatbots powered by AI agents could feel more like a person with desires, preferences and the ability to take autonomous action. For instance, the AI agent could ask the user, unprompted, if they would like to play a video game while chatting. Interacting with a chatbot may not feel different from how one interacts with their friends online. This could blur the lines between AI assistant and companion or even friend (see the insight on relationships).

AI agents could transform business and the workplace. Agents could be used to automate elements of an employee's job, like email and calendar management or taking meeting notes. For instance, Google Workspace's AI Teammate let's businesses assign an AI agent to a team that can monitor projects, provide status updates, draft documents, and answer questions.[6] A more sophisticated agent could generate reports and liaise with clients, potentially automating entire roles. In the future, it may not be uncommon to work with AI tools and collaborate with AI coworkers. Agents could handle things like marketing, accounting and finances, liaising with suppliers, filing taxes, and ensuring regulatory compliance. Advanced AI agents could potentially manage a business entirely on their own, allowing the owner to simply enjoy the profits.

IMPLICATIONS

- AI agents could **improve accessibility** by helping people navigate complex systems
  - AI agents could improve government consultations and benefits access by automating participation
- AI agents could significantly **improve worker productivity** by automating low-level tasks like filing paperwork, managing email inboxes and calendars, and liaising with clients
  - AI agents could **displace workers**, especially those in support, intermediary or middleperson roles, like salespeople, brokers, caseworkers, or assistants. As a result, people could work alongside AI agents, who act as coworkers
  - Powerful AI agents might perform more complex tasks, **like managing a business**
- Certain forms of **advertising may become less effective on humans** if AI assistants increasingly replace human shoppers online
  - Advertisers may shift to target agents instead of people directly.
  - It could be increasingly difficult for websites to **ensure a real human** is accessing their services
- As AI agents take more actions and make more decisions, it may become challenging to determine **where, when, and why errors made by AI agents happen, and who is responsible**
  - AI assistants could undertake **unauthorized actions** without their user's knowledge – for example, ordering an unwanted item. They could fail to take action when expected. Or they could **take the wrong action** – for example, placing an order for bandages instead of calling an ambulance

- AI agents could be used to **automate crime, fraud or harassment**
  - People could use **“shell agents”**, like shell companies, to obfuscate where the ultimate ownership and responsibility for an AI agent lies in an attempt to **avoid taxation, sanctions**, or otherwise **mask harmful or illegal activity**. For example, a person selling drugs on the dark web could use a series of intermediary agents to hide their connection with the AI agent that runs the operation
- AI agents could **force integration between pieces of software** that do not natively play together – for example, an agent could force a reminder app on a Mac to sync with a different reminder app on an Android phone
  - This could potentially increase competition in software as developers would no longer be able to artificially limit what their software can integrate with.
  - AI agents could make it more difficult for developers to control the user experience of their software and prevent malicious use
- **New social norms** may emerge about when it is considered acceptable to delegate communications to an AI agent, and when people still expect to be interacting directly with another person

VIGNETTE

Anju sits down, takes her first sip of coffee, and opens her work laptop. She's had this laptop for a month, and it still has that new computer shine. Her previous laptop worked just fine, but her employer decided to upgrade her to a top-of-the-line model with a fancy new processor that can run an AI assistant. The assistant's avatar appears on the screen and waves at Anju.

> **"Morning, Artemis," says Anju. "What's new?"**

> **"Good morning, Anju. Since you logged off yesterday you received seven emails. Five were routine, and I responded to them for you."**

A summary of the emails appears on the screen. Where is this file stored? Status update on report. Reschedule client call. Anju smiles to herself. She remembers how much she used to hate spending time on routine emails like this. She feels like an executive, having someone else to handle them for her.

> **"One email was a newsletter," continues Artemis. "I will summarize it as part of our afternoon news update. The last was from Jiafei asking for feedback on the product launch plan. I prepared a draft response for you to work from."**

Anju skims the draft and nods. "Great, I'll get to that in a bit. Can you schedule a meeting with Magnus, Chris, and Anastasia? I had an idea last night for the Xerxes Expo. Also see if Anatasia wants to go for lunch today."

> **"Of course," says Artemis. "If she's free, should I book a reservation at the usual place?"**

Anju looks out of the window and sighs. She loves how much easier and more productive her work life has become. But she also feels strangely guilty about it. She knows that Artemis will be able to help her process her feelings. She makes a mental note to bring up the subject later.

Endnotes

1 Statista. 'U.S.: Most Common Voice Assisted Searches 2022'. Accessed 22 August 2024.

2 Amazon Web Services, Inc. 'What Is an API? – Application Programming Interface Explained – AWS'. Accessed 22 August 2024.

3 Amazon Web Services, Inc. 'What Are AI Agents? – Agents in Artificial Intelligence Explained – AWS'. Accessed 22 August 2024.

4 Schwaiger, Christoph. 'Apple Just Unveiled New Ferret-UI LLM — This AI Can Read Your iPhone Screen'. Tom's Guide, 10 April 2024.

5 Zeff, Maxwell. 'OpenAI Wants to Control Your Computer'. Gizmodo, 8 February 2024.

6 David, Emilia. 'Learn to Work with Your AI Teammate.' The Verge, 14 May 2024.

© His Majesty the King in Right of Canada, 2025

For information regarding reproduction rights: https://horizons.gc.ca/en/contact-us/

PDF: PH4-223/2025E-PDF
ISBN: 978-0-660-76907-3

Aussi disponible en français sous le titre : Les agents d'IA pourraient agir en tant qu'assistants personnels avec un minimum d'orientation.

DISCLAIMER
Policy Horizons Canada (Policy Horizons) is the Government of Canada's centre of excellence in foresight. Our mandate is to empower the Government of Canada with a future-oriented mindset and outlook to strengthen decision making. The content of this document does not necessarily represent the views of the Government of Canada, or participating departments and agencies.