Policy Horizons Canada Horizons de politiques Canada

Canada

INSIGHT 1

AI COULD BREAK THE INTERNET AS WE CURRENTLY KNOW IT

Emerging AI tools have the potential to undermine the advertising business model that has served as the foundation for the internet for much of the last 20 years. The internet in the age of AI could be very different, one where people have more agency and control, but which is also less useful and secure.

TODAY

The internet is an integral part of Canadians' everyday lives. Young people, in particular, rely on it as a source of friendships[1] and information.[2] Across the wider population, 95% of Canadians over the age of 15 use the internet[3] and 75% engage in online banking[4] and shopping.[5] Nearly half of all households have internet-enabled smart devices.[6]

While more websites exist than ever before, most people's experience of the internet is dominated by a small handful of massive companies. As an online joke puts it, "the internet is five giant websites showing screenshots and text from the other four."[7] Today, 65% of all internet traffic is to domains owned by Alphabet, Meta, Netflix, Microsoft, Tik Tok, Apple, Amazon, or Disney.[8] Google accounts for 91% of all internet searches.[9]

Advertising funds the provision of free online services and the online creator economy.[10] Alphabet, Meta, Apple, Microsoft, and Amazon each earn billions from online advertising.[11] Companies invested US$46.7 billion in 2021 in optimizing their website design to rank more favourably on search engines, get more traffic, and generate more ad revenue.[12]

AI-generated content is rapidly becoming more realistic and human-like. Until recently, most online content was human-generated as computer-generated content was of generally low quality. This began to change in 2022 with the release of Dall-E 2, Midjourney, and ChatGPT. Large language models (LLMs) can produce high-quality human-like text. AI image generators can produce photorealistic images. AI video generators are advanced enough to interest Hollywood.[13] Voice generators have made popular AI song covers.[14] While most AI-generated content can still be identified through subtle telltale signs, it is becoming harder to distinguish from human-made content.

AI is not yet playing a significant role in undermining cybersecurity, but incidents are increasing. 70% of Canadians reported a cybersecurity incident in 2022, up from 58% in 2020. Although these are still mostly unsophisticated spam and phishing attempts,[15] fraud cases involving deepfakes increased 477% in 2022.[16] Scammers have started to make fake ransom calls using AI-generated voices of the target's loved ones.[17] Deepfake-related institutional fraud cases are also emerging, leading to millions of dollars in potential losses for firms and governments.[18]

FUTURES

AI-powered agents and search engines could transform how people interact with the internet. Instead of users going to specific websites, AI tools could create custom, personalized interfaces that are populated with content from across the internet. They could also help users find niche content and communities beyond major social media platforms.

These tools could disrupt internet ad-based business models. Should a significant portion of web traffic be made up of AI bots pulling information for their users, websites and search engines may earn less revenue from showing ads. They may need to find other ways of generating money, such as introducing subscriptions, paywalls, or the direct monetization of user data.

The internet could become dominated by AI-generated content, which may be indistinguishable from human-generated content. Online platforms could create multimedia content tailored to individual users. The internet could be awash with AI-generated websites filled with spam, misinformation, bots, and fake product reviews. It could become difficult for users to differentiate quality content from junk. If AI factchecking does not improve, this could become even more challenging.

The general sense of trust and security that Canadians feel online could be greatly diminished. When video calls can be convincingly deepfaked, it could be challenging for a person to know if a new online friend is a real person or an AI phishing scam. AI-powered disinformation campaigns could become more sophisticated, further undermining trust in institutions. As AI tools become more accessible and powerful, anyone with even the tiniest online presence could be exposed to a growing risk of harm.

IMPLICATIONS

- **AI Search engines may be held accountable for results** that are displayed to users. This could have legal repercussions and damage trust particularly if results are erroneous and even dangerous
- Content and services that were **once free may be put behind paywalls** as AI tools undermine the online advertising business model
  - Websites may attempt to directly **monetize user data and content**, for example by licensing it as training material to AI companies
  - Sponsored content, product placement, and other forms of **advertising may become more common**
- While human-generated content is unlikely to disappear, **content creators may struggle to compete** with cheap and tailored AI-generated content
  - Content creators may feel more **pressure to monetize** their audiences
  - Human taste and curation could become highly valued. **Content creators may give way to content curators**, who amass followings based on their curation of online content
  - Unique, personalized content could lead people to **feel isolated with fewer cultural touchpoints**
- AI tools may **shift control of the design, layout, and experience of a website** from web designers to users. This could make it easier for users to avoid the addictive or manipulative designs known as “dark patterns”
  - Navigating the internet without AI tools **could become very difficult**
  - Websites may **cease to exist as they are currently known**, instead becoming repositories of data to be scraped by AI. Businesses may no longer need web designers
- **Distrust could be the prevailing attitude online** as cybersecurity risks increase and AI-generated content dominates the internet
  - **AI phishing schemes** could become more sophisticated
  - People may become more **selective with what information they share online**
  - **New authentication measures** may emerge in attempts to restore trust online
  - If trust in AI continues to decline (see Insight 3), people may **fear they are being manipulated** by AI-tailored feeds of content
- If search engines cannot effectively sort quality content from AI spam, they **may no longer be effective** go-to sources for all queries
  - People may rely on a **few trusted sources** for information online
- Existing models of e-commerce may be disrupted in unforeseen ways

Endnotes

1 Lenhart, Amanda. Teens, Technology and Friendships, Pew Research Center (blog), 6 August 2015.

2 Kaiser & Partners. Young Canadians Are Increasingly Trusting News Broadly Shared on Social Media, 15 November 2023.

3 Statistics Canada. The Daily — Canadian Internet Use Survey, 2022, 20 July 2023.

4 Canadian Bankers Association. Focus: How Canadians Bank, 31 March 2022.

5 International Trade Administration. Canada — Country Commercial Guide — eCommerce, 4 November 2023.

6 Statistics Canada. The Daily — Canadian Internet Use Survey, 2022, 20 July 2023.

7 Statistics Canada. The Daily — Canadian Internet Use Survey, 2022, 20 July 2023.

8 Global Internet Phenomena, Sandvine, March 2024, 8-9.

9 StatCounter Global Stats. Search Engine Market Share Worldwide, Accessed 23 May 2024.

10 Alexander, Julia. Creators Finally Know How Much Money YouTube Makes, and They Want More of It, The Verge, 4 February 2020.

11 Ball, James. Big Tech Can't Escape the Ad Business. The Atlantic, 1 June 2023.

12 Acumen Research and Consulting. Search Engine Optimization Services - Global Market and Forecast Till 2030, February 2023.

13 Buckley, Thomas, Lucas Shaw, and Shirin Ghaffary. OpenAI Courts Hollywood in Meetings With Film Studios, Directors. Bloomberg.Com, 22 March 2024.

14 Pasion, Lorenz. Artists Fear Lack of Job Security, Regulations as AI-Made Song Covers Go Viral in TikTok. RAPPLER (blog), 11 September 2023.

15 Statistics Canada. The Daily — Canadian Internet Use Survey, 2022, 20 July 2023.

16 Zandt, Florian. Infographic: How Dangerous Are Deepfakes and Other AI-Powered Fraud? Statista Daily ata, 13 March 2024.

17 Al-Sibai, Noor. Bone-Chilling AI Scam Fakes Your Loved Ones' Voices to Demand Hostage Ransom. Futurism, 9 March 2024.

18 Magramo, Kathleen. British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim | CNN Business. CNN, 17 May 2024.

PDF: PH4-211/2025E-PDF
ISBN: 978-0-660-76881-6

Aussi disponible en français sous le titre : L'IA pourrait briser Internet tel que nous le connaissons actuellement.

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.