Policy Horizons Canada | Horizons de politiques Canada

REPORT

Foresight on AI

Policy considerations

Artificial intelligence (AI) is a game-changing technology. The pace of advance is accelerating. As more new AI technologies are released into the world, uncertainty is growing about their potential impacts — whether positive or negative. The speed of technological development could outpace the ability of decision makers to keep up.

This report lays out ten insights about factors that could shape the evolution of AI, in terms of technical capabilities, adoption and use. It is the first report produced by Policy Horizons Canada's interdepartmental project on the future of AI, complementing AI-related work across the Government of Canada.

By supporting readers to understand the impacts AI could have on governance, society, and the economy — with a focus on elements that are beyond the horizon — the report aims to help decision makers reflect on the future of AI.

Canada

Foresight on AI

Policy considerations

PDF: PH4-210/2025E-PDF
ISBN: 978-0-660-74945-7

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.

Foreword

Artificial intelligence (AI) is rapidly evolving, presenting both opportunities and challenges for Canada. As AI continues to advance, it is crucial to understand its potential impacts on governance, society, and the economy.

Policy Horizons Canada (Policy Horizons) is dedicated to exploring how AI might shape our future. By engaging with a diverse range of partners and stakeholders, we aim to identify key areas of change and support policy and decision-makers as they navigate this dynamic landscape.

On behalf of Policy Horizons, I extend my gratitude to everyone who has shared their time, knowledge, and insights with us.

We hope you find this report thought-provoking and valuable.

Kristel Van der Elst
Director General
Policy Horizons Canada

Introduction

This Foresight on AI report complements numerous reflections on AI (see Box 1) futures across the Government of Canada. It aims to support decision makers - involved either in AI implementation or in policy setting related to AI - by exploring factors that could shape the evolution of AI, in terms of technical capabilities, adoption, and use, and which might be "*beyond the horizon.*" The report does not provide specific policy guidance and is not meant to predict the future. Its purpose is to support forward-looking thinking and inform decision making.

As part of this work, Policy Horizons has done a literature review, researched ongoing development related to the field, engaged with policy analysts and decision makers internal to the government, and held extensive conversations with key AI experts.

The ten insights captured in this report explore future possible capabilities of AI, longer-term risks and opportunities, and uncertainties related to policy-relevant

assumptions. Readers can seek to understand the impacts AI could have on governance, society, and the economy. When engaging with this report, readers are invited to ask:

- How will future advancements in hardware, software, and interfaces create new opportunities and risks for Canada and its allies?
- Where could AI bring the biggest and most unexpected disruptions to governance, society, and markets?
- What assumptions about AI's development and deployment in the future may need to be challenged or further explored before they form the basis for decision making?

The ten insights are synthesised in Table 1 and expanded upon further in the document.

Defining AI

There are many ways to define artificial intelligence, along with much debate about whether or not the term should even continue to be used.[1,2,3] For the purpose of this work, Policy Horizons Canada uses the Organization for Economic Cooperation and Development's (OECD) definition of an AI system as "…a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."[4]

> AI is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Box 1

Table 1: 10 insights about factors shaping the future of and with AI

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.
2	**AI could empower non-state actors and overwhelm security organizations** In the future, more accessible and versatile AI will have implications for security. Non-state actors — friendly and hostile — will have access to capabilities traditionally held only by states. They might be able to deploy them faster than states, keeping security organizations in a constant race to catch up.
3	**Lack of trust in AI could impede its adoption** How trust in AI will evolve is unknown. Frequent or unaddressed failures in AI systems — or one significant failure — could erode trust and impede adoption, jeopardizing entire industries. Emerging forms of certification, verification, and efforts to rectify harms could encourage user trust and uptake.
4	**Bias in AI systems could remain forever** Bias is a feature of both human and AI decision making. As the data used to train AI is often biased in hard-to-fix ways, growing reliance on AI in decision-making systems could spread bias and lead to significant harm. Bias may never be eliminated, in part due to conflicting perspectives on fairness.
5	**Using AI to predict human behaviour may not work** While AI sometimes makes impressive predictions about human behaviour, many are inaccurate. Basing decisions on these predictions can have dire consequences for people. It might be impossible to improve the technology to a level where its benefits outweigh the costs.

6	**AI could become “lighter” and run on commonly held devices** Rather than a few large AI models running on cloud-based supercomputers, future AI models could be diverse and customized, some of them running on small, local devices such as smartphones. This could make regulation and control more complicated and multiply cybersecurity risks.
7	**AI-driven smart environments everywhere** Many products could be sold with AI as a default, creating ‘smart’ environments that can learn and evolve to adapt to the needs of owners and users. It may be difficult for people to understand the capabilities of smart environments, or to opt out of them.
8	**AI further erodes privacy** As AI-enabled devices collect more data online and in real life, efforts to turn data into new revenue streams could butt up against more privacy-conscious attitudes and devices. A new status quo may emerge that looks very different from the opaque way that users today exchange their data for free services.
9	**Data collected about children could reshape their lives in the present and future** Jurisdictions are expressing concerns about children’s privacy as AI technologies become more ubiquitous. Pervasive data collection in childhood could offer new opportunities for accessibility and education, but also worsen existing vulnerabilities, erode privacy, and reshape adult lives in the future.
10	**AI could reshape our ways of relating to others** AI tools could mediate more social interactions — in public or professional settings, or in private with friends, family or romantic partners. These tools could be used to flag suspicious or harmful behaviour, and help avoid social blunders — but they could also assist in manipulating and preying on others.

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[5] and information.[6] Across the wider population, 95% of Canadians over the age of 15 use the internet[7] and 75% engage in online banking[8] and shopping.[9] Nearly half of all households have internet-enabled smart devices.[10]

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."[11] Today, 65% of all internet traffic is to domains owned by Alphabet, Meta, Netflix, Microsoft, Tik Tok, Apple, Amazon, or Disney.[12] Google accounts for 91% of all internet searches.[13]

Advertising funds the provision of free online services and the online creator economy.[14] Alphabet, Meta, Apple, Microsoft, and Amazon each earn billions from online advertising.[15] 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.[16]

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.[17] Voice generators

have made popular AI song covers.[18] 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,[19] fraud cases involving deepfakes increased 477% in 2022.[20] Scammers have started to make fake ransom calls using AI-generated voices of the target's loved ones.[21] Deepfake-related institutional fraud cases are also emerging, leading to millions of dollars in potential losses for firms and governments.[22]

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 fact-checking 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 and 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.

Insight 2: AI could empower non-state actors and overwhelm security organizations

In the future, more accessible and versatile AI will have implications for security. Non-state actors — friendly and hostile will have access to capabilities traditionally held only by states. They might be able to deploy them faster than states, keeping security organizations in a constant race to catch up.

Today

AI is lowering barriers to entry and reducing the cost of conducting attacks.[23] For example, AI can help someone with limited programming skills write malicious software.[24] Leading open-source AI models only have marginally less capabilities than what is currently considered the most powerful general-purpose AI, GTP-4 Turbo.[25] Their general-purpose nature makes them equally useful to all types of problems, including harmful activities. It is uncertain who will use AI more

effectively and quickly — government bodies among rival nations or non-state actors.[26] However, AI could empower non-state threat actors, corporations, or nations who are not bound by legal or ethical constraints, and willing to apply the technology in ways other states cannot.

Futures

Many new actors could access large-scale monitoring in the future. AI's ability to analyze large amounts of open-source data could provide new actors with the ability to track and predict the movement of police and military forces.[27] AI tools can help write malicious computer code, making cyber defence more difficult. Similarly, ChatGPT has been used to create evolving malware, malicious software that can change its original code to evade cyber defences.[28]

AI can also be used in unconventional attacks, to lower the cost of inflicting physical harm or attacking infrastructure. For example, AI can facilitate the process of 3D printing dangerous parts like those needed to make nuclear weapons.[29] AI could also be used to automate swarms of low-cost drones to overwhelm air defences,[30] providing an advantage to smaller actors who wish to target urban settings or confront modern militaries. Should AI greatly increase access and automate harm, this could increase pressure on the security sector and change how it keeps citizens safe.

Implications

- Open-source AI could empower non-state threat actors with new tools and **erode advantages traditionally held by states**, such as surveillance and monitoring.[31]
- **There may be constraints of the ability of law enforcement agencies to gather intelligence** as compared to non-state actors.
- **More communities could challenge the use of AI** by law enforcement agencies.

- Innovative use of AI could **surpass the ability of defence and security organizations to adapt**. Failures in public safety could weaken institutional trust or change public attitudes on appropriate government use of AI.[32]
- Private AI firms could become the main players in the cybersecurity and intelligence sectors, including in spaces traditionally seen as within the public domain.

Insight 3: Lack of trust in AI could impede its adoption

How trust in AI will evolve is complicated and unknown. Frequent or unaddressed failures in AI systems — or one significant failure — could erode trust and impede adoption, jeopardizing businesses that depend on AI. Emerging forms of certification, verification, and efforts to rectify harms could encourage user trust and uptake.

Today

Trust is central to acceptance of AI — and, in Canada, trust in AI is declining.[33] The CanTrust index shows that Canadians' trust in AI declined by 6% between 2018 and 2024.[34] The global IPSOS AI Monitor shows that the Anglosphere, including Canada, has less trust in AI than other regions: for example, 63% of Canadians are nervous about products and services that use AI compared to only 25% of people in Japan.[35]

Trust in AI depends on the context in which it is used. For example, trust is highest for simple tasks such as adjusting a thermostat, and lower for tasks connected to personal safety such as self-driving cars.[36] Public trust in self-driving cars is low and falling. In 2023, only 22% of Canadians reported trusting self-driving cars and other AI-based driverless transportation[37] — compared to 37% of Americans, which is down from 39% in 2022 and 41% in 2021.[38]

Despite declining trust, use of AI tools in Canada is growing. A 2024 Leger poll found that 30% of Canadians now use AI, up from 25% a year ago. Younger demographics are using AI more than older demographics — 50% of those 18-35 report using AI, compared to only 13% of those 55 and older.[39]

Risks and failures arising from AI technologies have captured public attention frequently over the past year. In some instances, finetuning and testing of many AI tools was done after public roll out, which stands in stark contrast to trials for clinical drugs which require long periods of testing before release to the public. New initiatives to capture and report on AI incidents have emerged, such as the AI Incident Database and the OECD AI Incidents Monitor.[40,41]

Adoption of AI can feel forced, rather than chosen through personal agency. The current push to integrate AI everywhere can mean that valid concerns around data security, fairness, environmental consequences, and job security are downplayed.[42] Forcing people to adopt AI in their everyday lives without also making efforts to make the technology more trustworthy can limit the potential transformational impacts of the technology.[43] The current backlash against the increasing use of AI facial recognition technology in airports is one example of the interplay between forced adaptation in the absence of trust.[44]

Futures

Improvements in technology, practices and systems could help to build trust in AI. For example, new capabilities such as neuro-symbolic AI, which combines neural networks with rules-based symbolic processing, promise to improve the transparency and explainability of AI models. Firms' adoption of new labelling, certification, or insurance models could offset some of the mistrust in AI.[45,46] And some providers are now developing ways to assess AI models for safety and trustworthiness, offering warranties to verify their performance.[47,48] In the future, AI systems could give a confidence interval for everything from search results to self-driving vehicles, supporting users in weighing the risks and uncertainties involved.[49]

More strategic and thoughtful deployment of AI could enhance trust. In the future, AI will likely become the right solution to some problems but not others. Trust in AI could be enhanced if people perceive that it is making their lives easier,[50] rather than replacing tasks they enjoy or seeming like a solution in search of a problem. Individual familiarity with AI may build trust in one area of work or life, without necessarily translating to increased levels of trust in the overall AI ecosystem.[51]

High-profile failures and growing appreciation of risks could erode trust. Skepticism and mistrust could grow as the risks of AI become more well known and well documented and as more high impact tasks are delegated to AI. Groups that are negatively impacted by AI are actively opposing its use in some domains, such as writers and artists who are collectively organizing to limit what they see as the destructive power of the technology.[52] Mistrust could be driven not only by narratives that describe AI as an extinction-level threat, but also by its association with growing

inequality.[53] Similarly, high-profile technological failures could cast shadows of mistrust into the future. For example, public trust and support for nuclear power in Canada declined significantly in the wake of the Fukushima Daiichi nuclear accident in 2011, and public concerns over nuclear safety hindered the sector's growth for years.[54] A similar loss of trust in AI technologies such as self-driving cars, could jeopardize not just one company, but entire industries.

Implications

- Lack of trust could be a **major impediment** to the integration of AI in some sectors.
- A single **high-profile outlier incident** involving an established AI system could disproportionately harm trust in and uptake of AI — for example, a financial crisis triggered by AI-generated content and high-frequency algorithmic trading.
- People could trust AI to perform certain tasks **more than they trust other humans**.
- **Differing levels of trust in AI** across groups or use cases could **unite people across typical societal divisions or polarize them in new ways.**
- **Excessive trust** in some AI outputs **could increase misinformation and disinformation**, with consequences for democracy and societal cohesion.
- **A poor experience with one AI system could lead to distrust in other AI systems**, while a positive experience with one AI tool could lead to increased trust in other AI applications.
- **Case law and legislation** that determines accountability for decisions taken by or with AI **could influence trust and adoption**.
- The emergence of **new labels and certifications could affect consumer confidence** in AI, such as warning labels, or those analogous to fair trade or organic produce labels.[55]

- **Accountability and responsibility regimes will be clarified**, and many systems will need to determine who is accountable for the failures of AI.

Insight 4: Bias in AI systems could remain forever

Bias is a feature of both human and AI decision making. As the data used to train AI is often biased in hard-to-fix ways, growing reliance on AI in decision-making systems could spread bias and lead to significant harm. Bias may never be eliminated, in part due to conflicting perspectives on fairness.

Today

Bias in AI is seen as a major issue capable of automating discrimination at scale in ways that can be difficult to identify. While human decisions are also biased, one of the major risks of automating high-stakes decisions is that these become more widespread and less detectable, increasing the possibility of systemic errors and harms. While a single biased manager could decide to give higher interview scores to the few job applicants that look and speak like them, a biased AI model could have a similar effect on potentially thousands of people across organizations, sectors, or countries.

Many AI products claim to be less biased than human decision makers but independent investigations have revealed systematic failures and rejections. [56] For example, an audit of two AI hiring tools found that the personality types it predicted varied depending on whether an applicant submitted their CV in Word or raw text.[57] Similar tools have discriminated against women[58] or people with disabilities.[59] Bias is embedded in AI in many parts of its lifecycle — training data, algorithmic development, user interaction, and feedback.[60]

Bias may be impossible to eliminate because the data used for training AI models is itself often biased in ways that cannot easily be fixed. Controlling results can also cause problems. For example, an AI model that learns to discard racially sensitive wording might omit important information about the Holocaust or slavery.[61] Further, algorithms often cannot compute different notions of fairness at the same time, leading to constantly different results for certain groups.[62] [63] [64]

Futures

In a future where bias can never be eliminated — whether human or algorithmic — societies may need to rethink current ideas about fairness and how to best achieve it. People do not necessarily agree on the meaning of "fair." For example, some consider affirmative action to be fair while others do not. Institutions could adopt standards intended to distribute resources — jobs, grants, awards, or other goods — in ways that explicitly attempt to repair historical injustices. Organizations seeking to avoid systemic bias may use an "algorithmic pluralism" approach, which involves various elements in the decision-making process and ensures no algorithms severely limit opportunity.[65]

Efforts could be made to reduce bias in AI systems to an acceptable level, though eliminating it entirely could be impossible. Pushback may continue against using AI technologies in certain sensitive domains, such as policing or hiring. Alternatively, these technologies could continue to improve and become less biased in the future. Either way, there will likely be a continued push to reducing bias in AI technologies.

Implications

- **Systemic harms or failures could become institutionalized** in contexts where single algorithms are allowed to make bulk decisions about people's access to certain resources (e.g. jobs, loans, visas).
- **Human biases could become greater** among those who use AI systems, as people learn from and replicate skewed AI perspectives, carrying bias with them beyond their interactions.
- **Disagreements about the best ways to code for algorithmic fairness** may result from different definitions of what fairness actually means. This could lead to completely different results for similar technologies or systems.
- The inability to eliminate bias from algorithms could ultimately **lead to political, social, or economic divisions**.

- If decisions become more distributed, including various algorithms and humans at different points in a process, **it could be difficult to make discrimination claims** or identify a responsible party for discrimination.
- High-profile cases of algorithmic discrimination could lead to **loss of trust in AI decision-making systems**, particularly in policing and healthcare, and an increase in litigation.

Insight 5: Using AI to predict human behaviour may not work

While AI sometimes makes impressive predictions about human behaviour, many are inaccurate. Basing decisions on these predictions can have dire consequences for people. It might be impossible to improve the technology to a level where its benefits outweigh the costs.

Today

More governments and institutions are using AI to predict human behaviour and make decisions about individuals. For example, more than 500 schools in the U.S. use an AI model called Navigate to predict student success.[66] Social workers in the U.S. have used AI to predict which child welfare calls need further investigation.[67] Both are examples of "**predictive optimization**."[68] Notable AI engineers have argued that predictive optimization algorithms are based on faulty science, with AI predictions being only slightly more accurate than the random flip of a coin.[69] Despite this, they continue to be used because they outsource complex work like developing decision-making rules (e.g. what criteria to investigate for fraudulent behaviour or how to decide if a child is at risk of abuse). Human-generated decision-making rules can appear subjective and inaccurate compared to those of predictive AI models, which claim to reflect objective patterns in the real world.

Predictive optimization

The use of AI to predict future outcomes based on historical data, to make decisions about individuals.

Predictive models are not always right. Predictive AI models are plagued by many issues, including errors due to a mismatch between training data and deployment data. Because predictive AI must be trained on past data, it cannot account for emergent and complex variables in the world and in individual human behaviours. Models may be unable to account for new and unexpected drivers. Moreover, AI cannot filter out the effects of racist real-world practices such as disproportionate policing in Black neighbourhoods or communities, which leads to increased false arrests.[70] This has led to inaccurate predictions for vulnerable people. [71]

Predictive AI models cannot understand why real-world behaviour differs from their predictions. Models may assume that individuals will act rationally and consistently or follow the same rules and patterns of humans in aggregate. Models may not address the structural factors that account for differences between predicted and real-world behaviours. A focus on prediction may hinder the discovery of processes that can lead to new behaviours, such as when simplifying the language used on court summons reduced the rate of people failing to appear in court.[72]

While sometimes justified based on cost savings, some governments have felt significant repercussions after using of predictive optimization models. For example, in 2021, the Dutch government resigned over a scandal involving the tax authority's adoption of a self-learning AI to predict childcare benefits fraud.[73] The AI erroneously identified tens of thousands of families as owing excessive debts to the tax authority. Over 3,000 children were removed from their homes and many families remain separated. The scandal had significant repercussions, with families forced into debt, losing their homes, and some victims dying by suicide.

Futures

In the future, predictive optimization may be used in some jurisdictions but not others. It could be forbidden within some jurisdictions, particularly where governments have faced high costs and scrutiny due to failures. That could still allow the private sector to expand its currently opaque uses of predictive optimization.[74] Other jurisdictions may continue to use predictive optimization algorithms despite the risks. This could be because those affected are less able to pursue justice, or because their governments are not bound by democratic norms. Others may view predictive optimization as an inevitably imperfect tool, but one whose use can be justified due to cost savings. Institutions — including governments — that take up AI for predictive optimization and find that the costs outweigh the benefits could keep systems in operation far longer than they should or want to, due to the high amounts already invested or the difficulties involved in undoing a rollout. Some may see predictive AI as ethically unacceptable for decision-making, and instead work on interventions to minimize the predicted negative outcomes.

Implications

- Governments and companies that use predictive optimization without being transparent about the AI's decision-making rules **could be seen as untrustworthy**.
- If institutions use AI for predictive optimization while the burden of proof to contest inaccurate predictions is put on affected individuals, **already vulnerable populations may face worsened outcomes**. This could create new bureaucratic bottlenecks and tie up courts with algorithmic harms litigation, including cases related to human rights or Charter violations.
- Attempts to sacrifice individual rights for collective gains may **benefit privileged populations at the expense of the vulnerable,** creating greater socio-economic divisions.
- The uptake of predictive optimization models could create **initial cost savings that quickly give way to new costs**: to fight litigation from inaccurate predictions; to recontract providers to retrain and retune models; and to create new pathways for complaints and compensation for damages.
- If AI decision-making pre-emptively punishes people based on biased assumptions, it could **decrease the individual agency of vulnerable populations** and place new obstacles in their life courses.

Insight 6: AI could become "lighter" and run on commonly held devices

Rather than a few large AI models running on cloud-based supercomputers, future AI models could be diverse and customized, some of them running on small, local devices such as smartphones. This could make regulation and control more complicated and multiply cybersecurity risks.

Today

Improvements in AI training and compression techniques are allowing smaller, less resource-intensive AI models to become more capable. The size of an AI model is often used as a shorthand for its power, capability, and quality. While the largest models are often the most powerful and capable, AI developers are releasing smaller, compressed versions derived from larger models. This allows the smaller model to retain most of the performance of the larger model while also allowing it to be much smaller, less energy demanding, and run on less powerful hardware.[75] This has led smaller, newer models to outperform older and larger models. For example, Phi-3, which was released in early 2024 and has only 3.8 billion parameters, has comparable performance to GPT-3.5, which was released in late 2022 with 175 billion parameters.[76] Companies including Meta[77] and Mistral[78] have released open-source AI models that rival ChatGPT's performance but can run on a laptop. Researchers in the field of TinyML are developing AI that is smaller and can run on less powerful devices to enable the "smart" Internet of Things (IoT). For example, the Raspberry Pi, a credit card-sized computer popular with programming and computer engineering enthusiasts, can now run a suite of AI models including facial recognition.[79]

Model size

The size of an AI model is determined by how many parameters it has. Parameters are variables in an AI system whose values are adjusted during training. Smaller models can have parameters numbering in the millions or fewer, while larger models can have more than 400 billion.

Futures

We may see thousands of different AI models capable of running locally on every type of digital device, from smartphones to tiny computers.[80] These models could be developed by amateurs, startups, or criminals. They could be based on open-source models and customised for different purposes through training on widely accessible datasets. For example, Venice AI is a web-based AI service, built from a handful of open-source AI models, that allows users to generate text, code, or images with little to no guardrails and is sold as 'private and permissionless.'[81] As AI models of different sizes become more widely deployed, this may give rise to an ecosystem of AI models with various degrees of interoperability. Small models could interact with large, cloud-based, publicly accessible models, leveraging their power to perform tasks or learn (see Figure 1). Such small, localized models may lack safety measures and be deployed broadly without the knowledge of any authority.

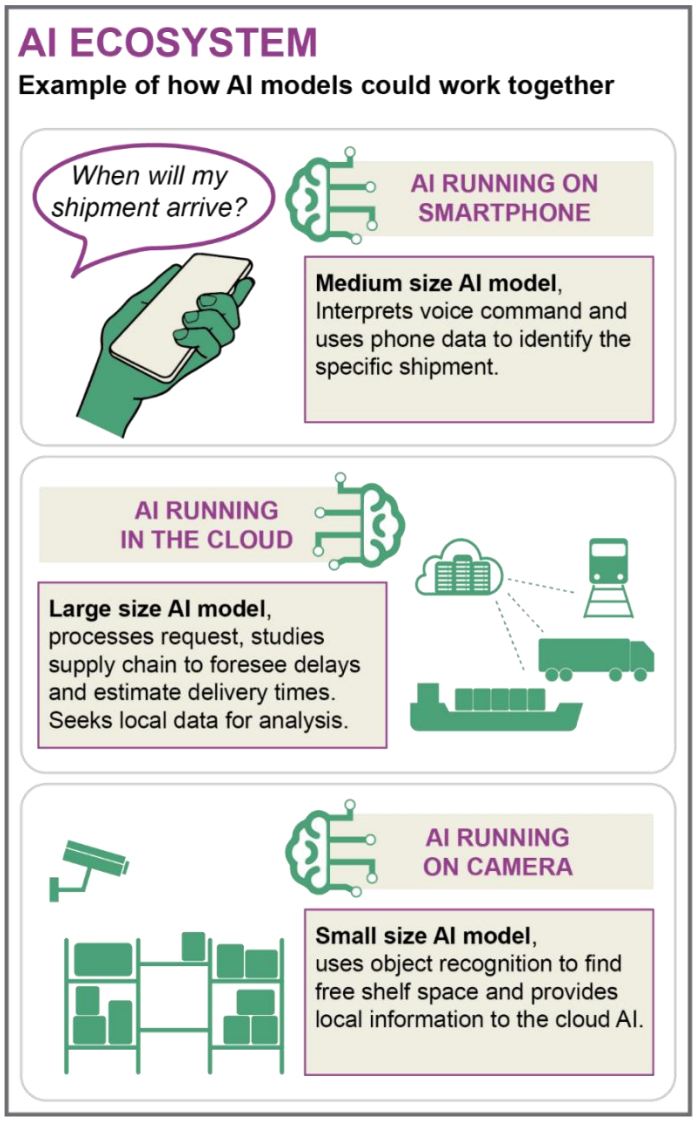

Figure 1

Implications

- Regulations focused only on large AI models **may not be effective**.[82]
- **Open-source AI could allow the circulation of models which are problematic,** whether because they incorporate bias, lack safety measures, or facilitate illegal activities.[83]
- **It could be hard to track bad actors** training or running small but powerful AI models.
- By analysing data locally, on-device AI models could help individuals **protect their data and privacy.**
- **Small businesses could customise their own AI tools** to better meet their needs.[84]
- Compatibility between AI-enabled devices could **provide users with more options** but also create cybersecurity vulnerabilities.[85]

Insight 7: AI-driven smart environments everywhere

Many products could be sold with AI as a default, creating "smart" environments that can learn and evolve to adapt to the needs of owners and users. It may be difficult for people to understand the capabilities of smart environments, or to opt out of them.

Today

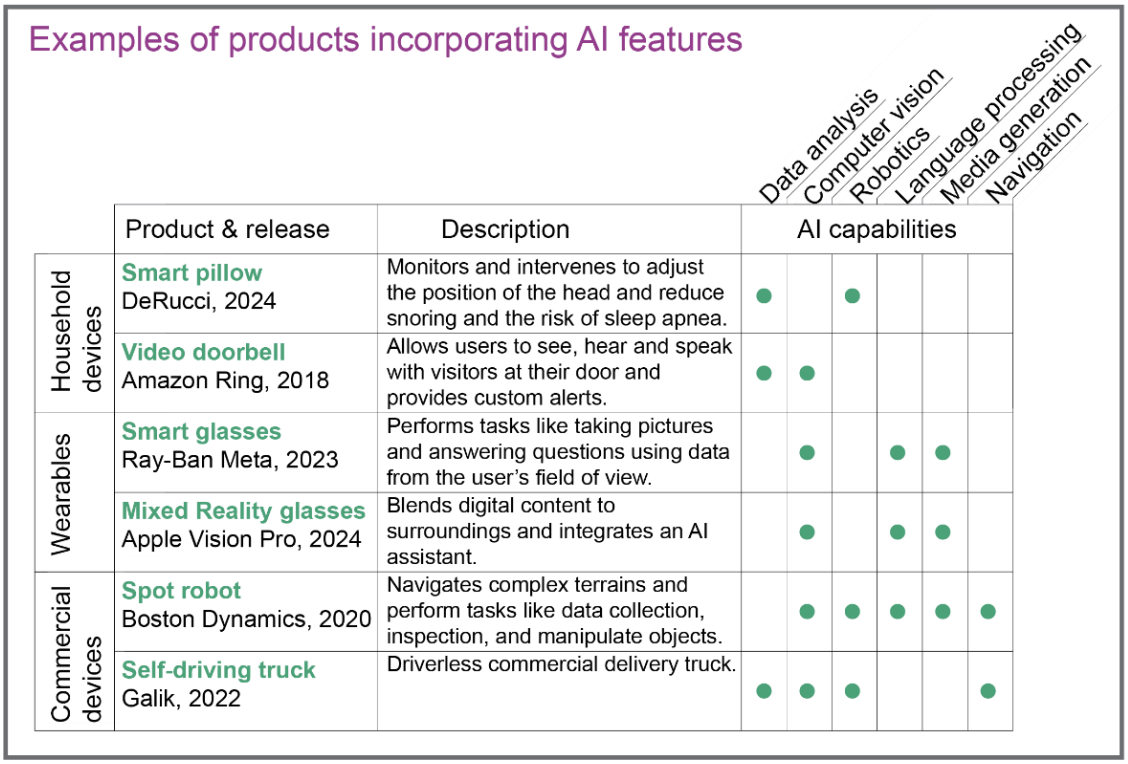

Figure 2

Autonomous devices and robots are increasingly present in our everyday lives. For example, restaurants are using robots to deliver meals.[86] Robot cleaners are commonly being used in commercial spaces.[87] In the agriculture sector, more autonomous and semi-autonomous machinery is being used to cultivate crops. In homes, AI is being added to everyday devices. Figure 2 shows further examples. Such devices could continue to gain new features as more capable AI models are released.[88]

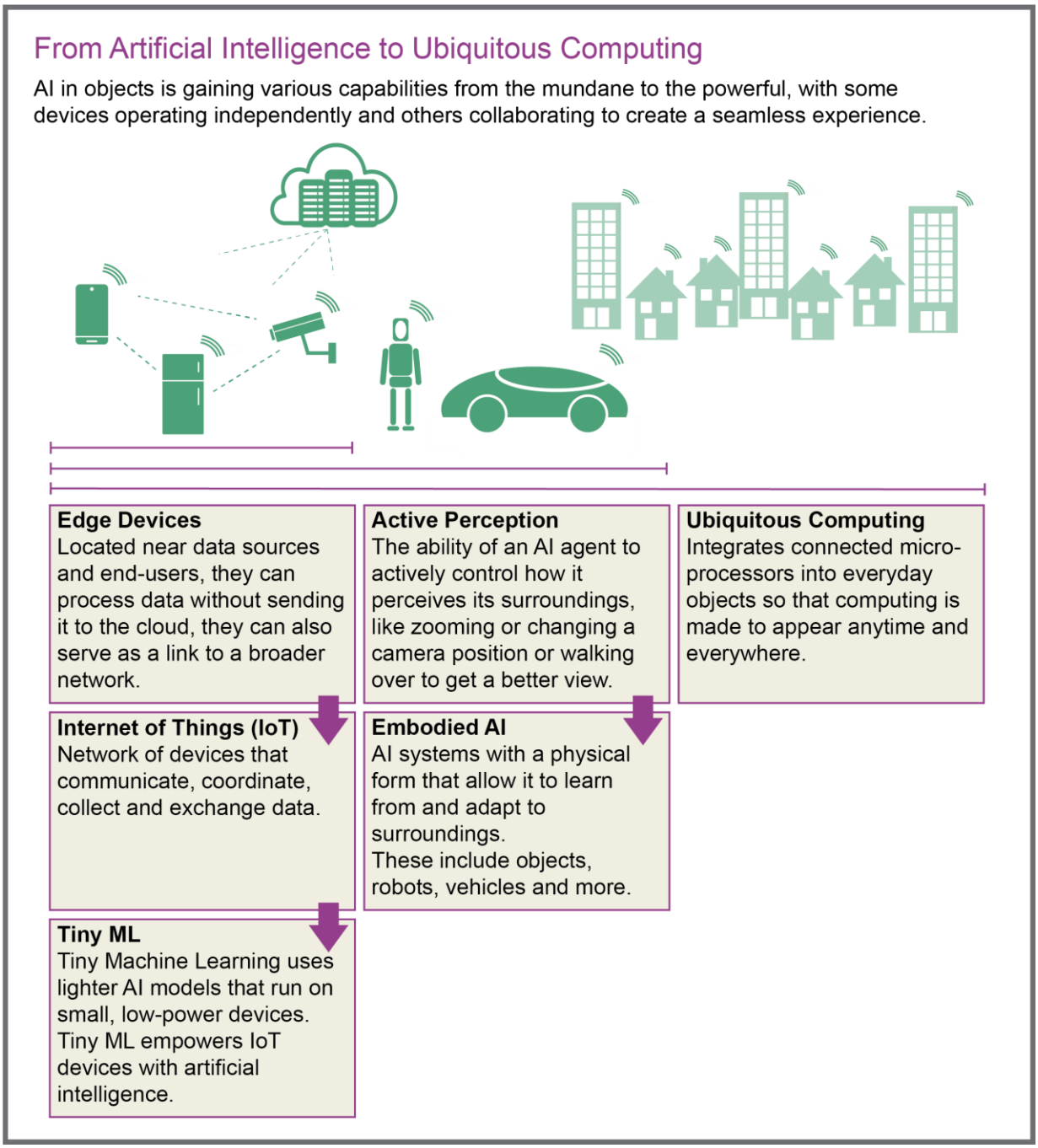

Figure 3

Researchers and industry may need more data about the physical world to train more advanced AI. AI that collects real-time information on its physical surroundings is referred to as embodied AI (see Figure 3).[89] AI can be embodied in

anything from smart phones to household devices or human-like robots. When connected to sensors and given mobility, AI can interact with people and physical spaces, for example by opening doors or summoning elevators.[90] As giving AI a body can allow it to learn from interacting with the world much like humans do, it may represent a path toward developing more advanced AI.[91]

It is becoming more difficult to understand the capabilities of devices in our surroundings. Some devices are referred to as 'robots' despite having no AI capabilities.[92] Other devices can have multiple AI functions. For example, tourists can rent AI-powered e-bikes that can give a guided city tour.[93] Bird watchers can buy AI-powered binoculars that identify wildlife.[94]

Older devices can often be retrofitted with new capabilities in ways that are not obvious from the outside. For example, an AI kit can make an existing tractor fully autonomous.[95] Security cameras that have been in operation for a long time can be connected to facial recognition software.[96]

Futures

In the future, more AI-powered devices may be found in more settings, from workplaces to leisure spaces and dwellings. It may become impossible to avoid interacting with these devices. The number of IoT (Internet of Things) devices could reach 75 billion by 2025, more than doubling in four years[97] and the global AI software market could grow roughly fivefold[98] from 2022 to 2027.

Device manufacturers could be incentivized to add AI capabilities to more devices either as a selling feature or to collect data. Data can be useful not only to generate new revenue streams but also to train new models. This could be especially relevant if embodied AI proves useful in building next-generation frontier AI models, or if companies reach the limits of existing quality training data.[99] For example, by deploying a fleet of smart cars a company could use data on the city landscape, traffic and the behaviour of pedestrians to train even more powerful AI models.

Everyday devices could end up having more powerful AI capabilities than needed. It may be easier to equip a device with an off-the-shelf, general-purpose AI,

such as ChatGPT or Copilot, than to customize a model with more targeted functionality. Smart devices could become the default in new homes, ready to adapt to new owners or tenants. Devices could be sold with certain features locked behind a pay-for-access model, as was seen with the Amazon Ring,[100] and with Tesla[101] and Mercedes[102] cars.

General-purpose AI could become standard in a way that increasingly blurs the lines between consumer product categories. For example, smart watches and fitness trackers have raised concerns that they might occupy a regulatory grey zone between medical devices and low-stakes consumer products.[103] The Aqara home sensor can be used for everything from controlling lights to providing security surveillance or detecting falls.[104] The appearance of such objects may not clearly signal their capabilities. Human-like robots may have eyes that can see through walls, for example – or the same sensors could be entirely hidden.

Implications

- People could require **new skills to navigate AI-powered spaces.** Manufacturers may need to use new kinds of labelling or instructions to disclose the capabilities of their AI devices in a way that allows consumers to make informed decisions.
- People unwilling or unable to engage with AI-powered spaces may find themselves **unable to access certain services**.
- Insurance companies could **encourage some kinds of AI monitoring or demand it as a condition of coverage**.[105] For example, facial recognition to confirm the identity of a driver to reduce auto theft.
- **The rights and interests of individuals could come into conflict in new ways**. For example, wearing smart glasses in public spaces or sending a robot to pick up groceries could challenge privacy rights. Trust is needed to ensure that the devices are not collecting the likeness of people without consent.[106] Property owners could install AI-powered devices to protect their investment or help with maintenance. Tenants may find themselves in a smart home with services they do not want or settings they cannot change.

- Smart environments could change advertising strategies. It could become routine for **AI-enabled devices to nudge users with personalized advertisements** in real-time. For example, smart cars may reroute drivers towards certain businesses and encourage them to stop to make a purchase.

Insight 8: AI further erodes privacy

As AI-enabled devices collect more data online and in real life, efforts to turn data into new revenue streams could butt up against more privacy-conscious attitudes and devices. A new status quo may emerge that looks very different from the opaque way that users today exchange their data for free services.

Today

Advances in AI are exacerbating privacy issues with technology. Most Canadians have become accustomed to accessing free online services – such as social media sites, generative AI platforms, or mobile apps. In many cases, they unknowingly give consent to companies to collect their data, sell it to third parties, and use AI to make sense of it and draw inferences about them. For example, Facebook uses AI to make inferences about users' suicide risk based on their social media posts.[107] Improvements in AI are allowing firms to analyze a greater variety and amount of data and transform it into revenue streams in new ways.

Not only online environments but also physical spaces are becoming less private. As noted in Insight 7, everyday household objects are outfitted with sensors to collect data – from toilets to toothbrushes to toys. Virtual Reality (VR) and video games can collect data about users' behaviour in the home and use AI to make inferences about emotions and personality traits.[108] Outside the home, devices such as smart glasses[109] and AI pins[110] are raising new questions about privacy in public. Fragments of human DNA, known as environmental DNA, collected from public spaces for purposes such as disease monitoring, can potentially be used to track individuals, illegally harvest genomes, and engage in hidden forms of genetic surveillance and analysis.[111,112]

Smart cars raise particular privacy concerns. In 2023 the Mozilla Foundation investigated 25 car brands and found that every one collected personal data that is not necessary to operate the vehicle.[113] Usually taken from mobile devices connected to cars via apps, this data can include a person's annual income, immigration status, race, genetic information, sexual activity, photos, calendar, and to-do list. Of the 25 brands, 22 use this data to make inferences – for example, from

location and phone contacts – and 21 share or sell data. Thirteen collect information about the weather, road surface conditions, traffic signs, and “other surroundings”, which can include passersby.[114] Ninety-five percent of new vehicles will be connected vehicles by 2030.[115]

Futures

As the Internet of Things becomes the “AI of Things”, data may become even more valuable, further incentivizing ever more data extraction. It may become possible to draw more sophisticated inferences to predict human behaviour, movement, or identify individuals, as discussed in Insight 5.

However, international regulatory pushback could reshape the privacy landscape. More jurisdictions are passing and enforcing new data privacy laws[116], such as the American Privacy Rights Act[117] in the US. This could change some, if not many, aspects of “surveillance capitalism”[118] by giving users more control over their data. Future legal reforms could reframe inferences as personal information[119], making it more difficult to sell them to third parties.

Emerging technology could also shift the privacy balance. Edge computing, which refers to networks or devices that are physically near to the user, could enhance data privacy and security.[120] When user data is stored and processed on a user-owned device, it may be more difficult for companies to collect and sell it.[121] However, edge computing can also introduce new risks, such as enabling face recognition on local devices and potentially easier access for malicious actors.[122]

Implications

- **Distinctions** such as public versus private and online versus offline could become **increasingly blurred**. Homes and other spaces could be experienced as more or less private depending on the use of devices. Visitors to homes and passengers in cars may demand **new consent protocols to protect their privacy**.

- Data shared with third parties could lead to **sensitive information being shared** with insurance companies.[123]
- Schools and childcare providers could use **privacy protections as a competitive advantage** to attract families.
- Surveillance could change the **practices of police and criminals**.
    - Some forms of **crime** could move further underground and **become more organized** to evade detection.
    - New technological capabilities could create **new opportunities for hacking, fraud, and stalking**.
    - Traffic police may be less needed as monitoring of drivers by governments and insurance companies enables **tickets to be issued automatically**.
- Activists[124] and journalists[125] could increasingly use ubiquitous computing to "return the gaze" by **collecting information about powerful organizations or individuals**. This practice is known as "sousveillance" or "equivalence." This could include hacking sensitive information about the personal lives of political representatives or other public figures.[126]
- Data protection regimes could become **more complex** and less aligned globally.
- Jurisdictions could struggle to balance privacy with researchers' need for representative datasets in areas such as medicine.[127]
- Jurisdictions with weaker privacy laws could become increasingly "risky" destinations for work or travel.
- **Privacy-protecting devices** could tilt the balance of power toward users.

Insight 9: Data collected about children could reshape their lives in the present and future

Jurisdictions are expressing concerns about children's privacy as AI technologies become more ubiquitous. Pervasive data collection in childhood could offer new opportunities for accessibility and education, but also worsen existing vulnerabilities, erode privacy, and reshape adult lives in the future.

Today

Young people are a particularly vulnerable group with regard to data privacy.[128] Their sense of self and ability to make decisions are still developing. Healthy child development involves the ability to experiment and make mistakes without severe and lasting consequences. More jurisdictions are exploring how to protect children's data and privacy rights and address challenges around meaningful consent.[129]

Cases are growing of malicious actors using children's data in ways that impact on their mental health and wellbeing. Critics point to how major tech companies capture attention and revenue through addictive user experiences[130] and dark patterns.[131] Dark patterns are a type of web or app design that can be used to influence your decision making when you are using an app or navigating through a website – for example, by intentionally making it difficult to cancel a service.[132] Social media algorithms exacerbate issues related to negative body image.[133] Generative AI has been implicated in the circulation[134] and development[135] of child sexual abuse materials, both real and AI-generated, by adults and children.

Parents have extraordinary scope to both gain and offer visibility into their children's private lives. For example, keylogger apps can let parents see not only messages a child sent, but also messages they typed but decided not to send.[136] Parents can also share their children's private information with others. Some manage revenue-generating child influencer accounts that routinely share personal information and images of their children. These accounts are sometimes openly followed by pedophiles, who benefit from platform policies that reward engagement.[137]

Unwanted "data" shadows could follow children into adulthood. Whether data is shared by parents or collected by platforms or devices,[138] it may create a "data shadow" that follows children throughout their lives.[139] This data shadow can begin before birth – for example, when parents use DNA testing services to learn about their children's genetic susceptibility to diseases.[140] As these vast troves of data can be stored indefinitely, future AI systems could draw on them to make new inferences about individuals as they grow into adults.

Schools are collecting ever more information about students, using third-party software and AI analysis tools. Since the pandemic, use of student management apps has grown exponentially in daycares, elementary schools, and high schools in Canada. For example, an estimated 70% of elementary schools use Class Dojo. Its privacy policy states it may share data with third-party service providers including Facebook and Google.[141]

Data breaches have affected children and youth in Canada and beyond. In 2024, school photos of 160 students in Alberta were stolen when hackers accessed the cloud storage provider of a school yearbook company.[142] Ransomware gangs have targeted US public schools, releasing sensitive student data on mental health, sexual assaults, and discrimination complaints.[143] In 2023, ransomware attacks affected institutions such as Toronto's Sick Kids Hospital;[144] Family and Children's Services of Lanark, Leeds and Grenville;[145] and Ontario's Better Outcomes Registry & Network, in which 3.4 million health records were breached.[146]

Corporations and NGOs hold a large amount of sensitive data about youth, which can be vulnerable to breach. Private parental control apps have been breached, exposing monitored children's data.[147] In 2023, TikTok[148], Microsoft[149], and Amazon[150] were fined for children's privacy violations in various jurisdictions. As a non-governmental organization, Kids Help Phone – which holds the largest repository of youth mental health data in Canada[151] – reports conducting a privacy impact assessment[152] and aggregating and anonymizing its data.[153]

Futures

The opaque sale, circulation, and analysis of children's data will become more common, begin much earlier in life, and be put to unforeseen uses in the future. The number of data-collecting devices children interact with – at home,

school, and beyond – will increase (see Insights 7 and 8). Some of these devices could be more vulnerable to breaches of sensitive information.[154]

AI-powered monitoring technologies could become more important, but could also be subverted. Parents could look to AI-powered monitoring technologies to help control their children's online activities and gatekeep increasingly complex informational and media environments.[155] However, young people could also develop increasingly sophisticated means of evading parental control.

Children and youth could inhabit more highly personalized media environments. Entertainment content and advertising could increasingly be generated or curated by personalized AI companions. Sub- and fan cultures could become increasingly personalized and politicized. Feelings of social isolation could become more prevalent, as well as reduced social cohesion. Some young people may become disillusioned with invasive AI-powered technologies and opt to spend more time offline. However, given the pervasiveness of AI this might not be an option in the future.

The market for youth data may become more competitive as concerns around youth data privacy increase. This could lead tech companies to develop more insidious ways to extract and trade youth data. The age cut-off for being seen as a "child" could differ in different contexts. Data could have to be released when a child attains the age of majority.[156] Age verification technologies,[157] like those currently being used in some US states for pornography websites,[158] could be more widely used to protect youth from predatory adults and adult-only spaces.

Despite the many concerns they raise, new AI-enabled technologies could also collect data in ways that support accessibility.[159] They could be used to develop individualized learning tools that help students progress at their own pace. They could also enhance the quality of pediatric health care by assisting in diagnosis, patient monitoring, and precision medicine.[160]

Implications

- Today's children could face **more frequent and devastating data breaches** throughout their lives.
- These breaches could result in forms of **identity theft** that lead to financial loss or the release of sensitive personal information.
- **Re-identification of anonymized personal data** could become easier as data breaches become more routine and technologies advance – data that seems **private today may not be tomorrow**.
- Lax restrictions could lead to data being used to make **AI-mediated inferences** about youth that **affect their relationships and access to jobs, credit, or insurance** in both childhood and adulthood.
- **Increased use of parental control technologies** could lead to undue surveillance and **loss of privacy and autonomy for children**.
- AI could make it **more challenging for parents to identify problematic or harmful content**, or easier for youth to conceal their engagement with it.
- If awareness of issues related to children's data privacy increases, more developers could be required to launch **child-specific apps and platforms that are held to higher privacy standards**[161] or consider issues such as mental health and addiction.

Insight 10: AI could reshape our ways of relating to others

AI tools could mediate more social interactions — in public or professional settings, or in private with friends, family or romantic partners. These tools could be used to flag suspicious or harmful behaviour, and help avoid social blunders — but they could also assist in manipulating and preying on others.

Today

AI already plays a large role in mediating our relationships with strangers, friends, and family in online spaces. Recommender algorithms act as a social filter, determining which content a user sees, from which people, and in which order.[162] These algorithms can encourage users to engage with influencers and content creators who provide a high level of apparent access to their lives.[163] For some users, such "intimacies" can develop into parasocial relationships, where individuals feel emotionally connected or attached to total strangers.[164]

AI devices mediate an increasing number of professional and personal interactions. For example, doctors are already using AI to help diagnose or monitor patients.[165] People are using AI to help write profiles[166] or messages[167] on dating apps. AI can even analyze and flag the tone that individuals use in messages to one another, for example in apps used to mediate communication in difficult coparenting arrangements.[168]

Wearable devices which introduce AI into new aspects of our lives can blur the lines between real and digital spaces. These devices can use virtual reality (VR), augmented reality (AR), and a combination of AR and VR known as mixed reality (MR).[169] Research suggests that immersive environments can be more emotionally impactful than traditional online spaces.[170] Collective experiences in VR can provide a new type of enriching social gathering for geographically distant groups. Harms in VR, such as assault, can have psychologically similar effects as the offline equivalent.[171]

Individuals can develop emotional connections with AI companions. Millions are turning to AI companions to alleviate loneliness, access therapy, get advice, and for romantic connection.[172,173,174] When an AI model produces text, speech and images that are indistinguishable from those made by humans, it is easy to anthropomorphise the model by attributing motive and intent to its responses.[175]

Users of popular platforms live in increasingly personalized and private worlds as AI curates the content they see. Social media algorithms often offer users content that suggests they "know" them better than even close friends might. Over time, however, consuming AI-curated content – as opposed to content shared by friends – may warp representations of the self.[176] As they scroll through content alone, users can enter what researchers call a trance-like state.[177]

AI is changing how parents relate to and engage with their children. AI tools can allow parents an unprecedented level of visibility and control over the apps their children use, the content they consume, and the messages they write, as discussed in Insight 7. Smartphones or trackers can give parents real-time, 24/7 information about their children's whereabouts.[178] These tools can erode children's autonomy, privacy, and independence as they grow and mature. Similar tools used in romantic relationships can facilitate abusive behaviour and stalking.[179]

Futures

In the future, AI could play a larger role in mediating professional interactions, limiting scope for forming new friendships. AI could improve the efficiency of communication between a company's customers and employees and change workflows between individuals and teams. Workplace culture could become more impersonal, with fewer opportunities for socialising.

AI tools could also mediate more personal social interactions, even in the home among family members. Such tools could include AI agents, platform algorithms, or wearable devices, such as AR glasses. More information about and visibility into the inner lives of people, whether physiological or psychological, could become normalized. This could improve communication in relationships. It could

also shift relationship dynamics in new ways, leading to lower trust and autonomy and more mental health issues.[180]

Individuals could increasingly turn to AI for companionship or answers to personal problems. AI could help socially isolated individuals to connect with others.[181] AI therapists could provide tailored mental health care for populations that lack access: apps such as Black Female Therapist, for example, use AI trained to highlight the importance of systemic racism.[182] On the other hand, AI companions could further isolate individuals if they replace relationships with humans. Individuals who come to prefer synthetic relationships to real ones could end up disconnected from community, though not necessarily lonely.

Some individuals could seek human connection by sharing and comparing their media feeds. As media experiences become increasingly personalized, there could be increased interest in understanding the distinct worlds that people inhabit. This could include “feed analysis” in therapeutic settings, sharing feeds in the presence of friends, or even public feed-sharing events.[183]

In the future, it may become impossible to distinguish between humans and hyper-realistic AI agents when interacting in online spaces. AI technology could be used to create digital replicas of deceased or estranged loved ones, or celebrities and influencers. AI agents could be perceived as exhibiting human emotions such as empathy and love. Individuals could have what feels like an intimate relationship with a person but is in fact a parasocial interaction with a chatbot. This could entirely replace human social connections for some vulnerable or lonely individuals.

Implications

- AI could **help reduce inequalities for those who face language barriers** or difficulties navigating complex social interactions.
- Relationships with AI companions could feel indistinguishable from human connections, or even easier or better, for some people.
- **AI companions or therapists could have more influence on an individual’s behaviours** than their family or close friends.

- **Social skills could atrophy**. Skills such as listening and empathy could be eroded if users lean too heavily on AI assistance for social interactions or customize AI agents to reflect their needs and preferences.
- Marriage rates could decline and loneliness could increase.
- The experience of selfhood could change. Earlier and more frequent self-monitoring, and the application of predictive analytics to biological and mental processes, could lead to **new ways of understanding and optimizing the self.**
- **New forms of abuse and virtual crime could emerge**, potentially challenging definitions of assault and harassment.
- **Predators could more easily gain the trust of children and adults**, leading to greater risk of fraud, harassment, or other abuse.
- **Using AI tools to communicate with people could shift language** over time, potentially towards greater homogenization and sterilization.
- **AI tools could flag suspicious behaviour**, report abuse as it is happening, and help individuals navigate toxic or dangerous relationships.
- **Bullying and harassment could become more omnipresent** and damaging to mental health if it occurs in realistic immersive environments or with the use of generative AI.

Published Policy Horizons Canada work related to AI:

Disruptions on the Horizon

Sense-making Futures: A crisis of certainty

Future Lives: Uncertainty

Commercialization of biological data

Metaverses

The Future of Generative AI

Geotechnomics

Three ways ChatGPT could support strategic foresight

Acknowledgements

This foresight report synthesizes the thinking, ideas, and analysis of many contributors through research, interviews, conversations, and workshops.

The project team would like to thank the many public servants and colleagues who contributed to this work and the experts who generously shared their time and expertise in support of the research, including those who chose to remain anonymous.

Blair Attard-Frost
Course Instructor, University of Toronto

Stephanie Baker
Researcher, Electronic Systems and IoT Engineering, James Cook University

Michael Beauvais
SJD Candidate, University of Toronto Faculty of Law

Olivier Blais
Co-founder and VP of Decision Science, Moov AI

Ana Brandesescu
PhD Candidate, McGill University

Francesca Campolongo
Director for Digital Transformation and Data, European Commission

Ashley Chisholm
Strategic Policy Advisor, Physician Wellness Medical Culture, Canadian Medical Association

Sherif Elsayed-Ali
Co-Founder, Nexus Climate

Kay Firth-Butterfield
Chief Executive Officer, Good Tech Advisory LLC

Michael Geist
Full Professor, Common Law Section, Faculty of Law Canada Research Chair in Internet and e-Commerce Law, University of Ottawa

N. Katherine Hayles
Distinguished Research Professor at the University of California, Los Angeles, and the James B. Duke Professor Emerita from Duke University

Matissa Hollister
Assistant Professor (Teaching), Organizational Behaviour, Desautels Management School, McGill University

Sun-Ha Hong
Assistant Professor, School of Communication, Simon Fraser University

Kai-Hsin Hung
PhD candidate, HEC Montréal

Ian Scott Kalman
Associate Professor, Fulbright University Vietnam

Andrew J. Kao
Research Fellow, Harvard University

Sayash Kapoor
PhD candidate, Princeton University

Kristin Kozar
Executive Director, Indian Residential School History and Dialogue Centre, University of British Columbia

Nicholas Lane
Professor, Computer Science and Technology, University of Cambridge

Sasha Luccioni
Climate Lead, Hugging Face

Arvind Narayanan
Director/Professor, Centre for Information Technology Policy, Princeton University

David Nielson
Director, Mixed Reality Lab, USC Institute for Creative Technologies

Deval Pandya
Vice President of AI Engineering, Vector Institute

Manish Raghavan
Drew Houston (2005) Career Development Professor and Assistant Professor of Information Technology at the MIT Sloan School of Management

Mark Riedl
Professor/Associate Director, Georgia Tech, School of Interactive Computing / Machine Learning Center

Julie Robillard
Associate Professor of Neurology, University of British Columbia

Stephen Sanford
Managing Director, U.S. Government Accountability Office

Teresa Scassa
Faculty member and Canada Research Chair in Information Law and Policy Full Professor, Common Law Section, Faculty of Law

Mona Sloane
Assistant professor of data science and media studies, University of Virginia

Nick Srnicek
Lecturer in Digital Economy in the Department of Digital Humanities, Kings College London

Luke Stark
Assistant Professor, University of Western Ontario

Yuan Stevens
Academic Associate – Health Research & AI Governance, Centre for Genomics and Policy

Catherine Stinson
Queen's National Scholar in Philosophical Implications of Artificial Intelligence and Assistant Professor in the Philosophy Department and School of Computing at Queen's University

Mark Surman
President and Executive Director, Mozilla Foundation

Liana Tang
Second Director, Smart Nation Strategy Office, Ministry of Communications and Information, Singapore

Agnes Venema
Researcher at the 'Mihai Viteazul' National Intelligence Academy, Ministry of Defence, Romania

Wendy Wong
Professor and Principal’s Research Chair, University of British Columbia

Agnieszka Wykowska
Senior Researcher Tenured and Principal Investigator, Social cognition in human-robot interaction, Italian Institute of Technology

Project team

John Beasy, Analyst
Martin Berry, Senior Analyst
Leah Desjardins, Analyst
Miriam Havelin, Analyst
Nicole Rigillo, Senior Analyst
Kristel Van der Elst, Director General
Claire Woodside, Manager

Policy Horizons Canada would like to thank its Deputy Minister Steering Committee members, the Directors General Foresight Committee, the members of the Federal Foresight Network, and Senior Assistant Deputy Minister, Elisha Ram, for their guidance, support, and insight, as well as all colleagues that contributed to the development of this work.

And to the following current and former Policy Horizons Canada colleagues: Katherine Antal, Imran Arshad, Marcus Ballinger, Fannie Bigras-Lafrance, Mélissa Chiasson, Steffen Christensen, Suesan Danesh, Pierre-Olivier Desmarchais, Nicole Fournier-Sylvester, Chris Hagerman, Laura Gauvreau, Pascale Louis-Miron, Leona Nikolic, Megan Pickup, Simon Robertson, Julie-Anne Turner, Alexa Van Every, and Andrew Wright (external) for their support on this project.

Endnotes

[1] Pretz, Kathy. “Stop Calling Everything AI, Machine-Learning Pioneer Says.” IEEE Spectrum. Accessed August 8, 2024. https://spectrum.ieee.org/stop-calling-everything-ai-machinelearning-pioneer-says.
[2] Lanier, Jaron. “There Is No A.I.” The New Yorker, April 20, 2023. https://www.newyorker.com/science/annals-of-artificial-intelligence/there-is-no-ai.
[3] Drage, Eleanor, and Kerry Mackereth. “The Good Robot Podcast: Featuring Emily M. Bender and Alex Hanna.” Accessed August 8, 2024. https://aihub.org/2024/02/09/the-good-robot-podcast-featuring-emily-m-bender-and-alex-hanna/.
[4] OECD Legal Instruments. ‘Recommendation of the Council on Artificial Intelligence’, 2 May 2024. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449?_ga=2.124697866.1898590258.1621541868-1852956558.1620326402.
[5] Lenhart, Amanda. ‘Teens, Technology and Friendships’. Pew Research Center (blog), 6 August 2015. https://www.pewresearch.org/internet/2015/08/06/teens-technology-and-friendships/.
[6] Kaiser & Partners. ‘Young Canadians Are Increasingly Trusting News Broadly Shared on Social Media’, 15 November 2023. https://kaiserpartners.com/young-canadians-are-increasingly-trusting-news-broadly-shared-on-social-media/.
[7] Statistics Canada. ‘The Daily — Canadian Internet Use Survey, 2022’, 20 July 2023. https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm.
[8] Canadian Bankers Association. ‘Focus: How Canadians Bank’, 31 March 2022. https://cba.ca/technology-and-banking.
[9] International Trade Administration. ‘Canada - Country Commercial Guide - eCommerce’, 4 November 2023. https://www.trade.gov/country-commercial-guides/canada-ecommerce.
[10] Statistics Canada. ‘The Daily — Canadian Internet Use Survey, 2022’, 20 July 2023. https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm.
[11] Doctorow, Cory. ‘As Platforms Decay, Let’s Put Users First’. Electronic Frontier Foundation, 9 May 2023. https://www.eff.org/deeplinks/2023/04/platforms-decay-lets-put-users-first.
[12] ‘Global Internet Phenomena’. Sandvine, March 2024. https://www.sandvine.com/phenomena, 8-9.
[13] StatCounter Global Stats. ‘Search Engine Market Share Worldwide’. Accessed 23 May 2024. https://gs.statcounter.com/search-engine-market-share.
[14] Alexander, Julia. ‘Creators Finally Know How Much Money YouTube Makes, and They Want More of It’. The Verge, 4 February 2020. https://www.theverge.com/2020/2/4/21121370/youtube-advertising-revenue-creators-demonetization-earnings-google.

[15] Ball, James. 'Big Tech Can't Escape the Ad Business'. The Atlantic, 1 June 2023. https://www.theatlantic.com/technology/archive/2023/06/advertising-revenue-google-meta-amazon-apple-microsoft/674258/.
[16] Acumen Research and Consulting. 'Search Engine Optimization Services - Global Market and Forecast Till 2030', February 2023. https://www.acumenresearchandconsulting.com/search-engine-optimization-services-market.
[17] Buckley, Thomas, Lucas Shaw, and Shirin Ghaffary. 'OpenAI Courts Hollywood in Meetings With Film Studios, Directors'. *Bloomberg.Com*, 22 March 2024. https://www.bloomberg.com/news/articles/2024-03-22/openai-courts-hollywood-in-meetings-with-film-studios-directors.
[18] Pasion, Lorenz. 'Artists Fear Lack of Job Security, Regulations as AI-Made Song Covers Go Viral in TikTok'. *RAPPLER* (blog), 11 September 2023. https://www.rappler.com/technology/features/artists-fear-lack-job-security-regulations-ai-generated-song-covers-viral-tiktok/.
[19] Statistics Canada. 'The Daily — Canadian Internet Use Survey, 2022', 20 July 2023. https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm.
[20] Zandt, Florian. 'Infographic: How Dangerous Are Deepfakes and Other AI-Powered Fraud?' Statista Daily Data, 13 March 2024. https://www.statista.com/chart/31901/countries-per-region-with-biggest-increases-in-deepfake-specific-fraud-cases.
[21] Al-Sibai, Noor. 'Bone-Chilling AI Scam Fakes Your Loved Ones' Voices to Demand Hostage Ransom'. Futurism, 9 March 2024. https://futurism.com/the-byte/ai-voice-hostage-scam.
[22] Magramo, Kathleen. 'British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim | CNN Business'. CNN, 17 May 2024. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.
[23] Kreps, Sarah and Richard Li. 'Cascading Chaos: Nonstate Actors and AI on the Battlefield'. Brookings, 1 February 2022. https://www.brookings.edu/articles/cascading-chaos-nonstate-actors-and-ai-on-the-battlefield/.
[24] Scroxton, Alex. 'Research Team Tricks AI Chatbots into Writing Usable Malicious Code'. Computer Weekly, 24 October 2023. https://www.computerweekly.com/news/366556692/Research-team-tricks-AI-chatbots-into-writing-usable-malicious-code.
[25] Huggingface. 'LMSys Chatbot Arena Leaderboard - a Hugging Face Space by Lmsys'. Accessed 19 February 2024. https://huggingface.co/spaces/lmsys/chatbot-arena-leaderboard.
[26] Hirsh, Michael. 'How AI Will Revolutionize Warfare'. Foreign Policy (blog), 11 April 2023. https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/.
[27] Homeland Security. 'Addressing Risks From Non-State Actors` Use of Commercially Available Technologies', 2022. https://www.dhs.gov/sites/default/files/2022-09/Addressing%20Risks%20from%20Non-State%20Actors.pdf.

[28] Mascellino, Alessandro. 'ChatGPT Creates Polymorphic Malware'. Infosecurity Magazine, 18 January 2023. https://www.infosecurity-magazine.com/news/chatgpt-creates-polymorphic-malware/.
[29] Volpe, Tristan. 'Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs'. Carnegie Endowment for International Peace. Accessed 19 February 2024. https://carnegieendowment.org/2019/08/22/dual-use-distinguishability-how-3d-printing-shapes-security-dilemma-for-nuclear-programs-pub-79910.
[30] Ware, Jacob. 'Terrorist Groups, Artificial Intelligence, and Killer Drones'. War on the Rocks, 24 September 2019. https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/.
[31] 'Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes'. UN Counter-Terrorism Centre (UNCCT) and UN Interregional Crime and Justice Research Institute (UNICRI), 2021. https://unicri.it/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf.
[32] Kreps, Sarah. 'Democratizing Harm: Artificial Intelligence in The Hands of Nonstate Actors'. Brookings, November 2021. https://www.brookings.edu/wp-content/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf.
[33] Gillespie, Nicole, Steven Lockey, Caitlin Curtis, Javad Pool, and Ali Akbari. "Trust in Artificial Intelligence: A Global Study." The University of Queensland and KPMG Australia, 2023. https://www.aiunplugged.io/wp-content/uploads/2023/10/Trust-in-Artificial-Intelligence.pdf.
[34] Proof Strategies. "2024 CanTrust Index." Proof Strategies, February 13, 2024. https://getproof.com/trust/cantrust/.
[35] Carmichael, Matt, and Jamie Stinson. "The Ipsos AI Monitor 2024: Changing Attitudes and Feelings about AI and the Future It Will Bring" Ipsos AI Monitor. Paris: Ipsos, June 6, 2024. https://www.ipsos.com/en/ipsos-ai-monitor-2024-changing-attitudes-and-feelings-about-ai-and-future-it-will-bring.
[36] Karadeglija, Anja. "Poll Finds More Canadians Using AI despite 'deep-Rooted' Fears." The National Post, February 9, 2024. https://nationalpost.com/news/more-canadians-using-ai-tools-despite-deep-rooted-fears-about-the-tech-poll.
[37] Chhim, Chris, and Sanyam Sethi. "Canadians Among Least Likely to Believe Artificial Intelligence Will Make Their Lives Better." Paris: Ipsos, January 14, 2022. https://www.ipsos.com/en-ca/news-polls/Canadians-Least-Likely-AI-Make-Lives-Better.
[38] Stilgoe, Jack. "What Does It Mean to Trust a Technology?" *Science* 382, no. 6676 (n.d.): 9782.
[39] 'Use of AI Tools'. Leger, 5 February 2024. https://leger360.com/use-of-ai-tools/.
[40] OECD.AI Policy Observatory. "AIM: The OECD AI Incidents Monitor, an Evidence Base for Trustworthy AI." Accessed August 7, 2024. https://oecd.ai/en/incidents.
[41] "Welcome to the Artificial Intelligence Incident Database." Accessed August 7, 2024. https://incidentdatabase.ai/.

[42] O'Gorman, Marcel. "Opinion: When It Comes to AI, It Feels like We're Doing More Adaptation than Adoption These Days. This Is Not a Good Feeling." *The Globe and Mail*, June 21, 2024. https://www.theglobeandmail.com/opinion/article-when-it-comes-to-ai-it-feels-like-were-doing-more-adaptation-than/.
[43] Marr, Bernard. 'Will AI Really Revolutionize Every Industry? A Critical Analysis'. Forbes, 23 July 2024. https://www.forbes.com/sites/bernardmarr/2024/07/23/will-ai-really-revolutionize-every-industry-a-critical-analysis/.
[44] Vermes, Jason. "Airports want to scan your face to make travelling easier. Privacy experts caution it's not ready for takeoff." *CBC News.* March 3, 2024. Airports want to scan your face to make travelling easier. Privacy experts caution it's not ready for takeoff | CBC Radio
[45] Schuman, Leslie. "Leading Corporations Introduce Data Provenance Standards." *Businesswire*, November 30, 2023. https://www.businesswire.com/news/home/20231130851266/en/Leading-Corporations-Introduce-Data-Provenance-Standards.
[46] The Data & Trust Alliance. "The Data & Trust Alliance." Accessed August 7, 2024. https://dataandtrustalliance.org/.
[47] "LLM Safety Leaderboard - a Hugging Face Space by AI-Secure." Accessed August 7, 2024. https://huggingface.co/spaces/AI-Secure/llm-trustworthy-leaderboard.
[48] Masse, Bryson. "Armilla Offers Verification and Warranties for Enterprises Using AI Models." *VentureBeat* (blog), October 3, 2023. https://venturebeat.com/ai/armilla-offers-verification-and-warranties-for-enterprises-using-ai-models/.
[49] Sanz Sáiz, Beatriz. 'How your organization can have confidence in the opportunities AI brings'. *Ernst & Young* (blog), January 15, 2024. https://www.ey.com/en_gl/insights/ai/how-your-organization-can-have-confidence-in-the-opportunities-ai-brings
[50] Gillespie, Nicole, Lockey, Steven, Curtis, Caitlin, Pool, Javad, and Ali Akbari. 'Trust in Artificial Intelligence: A global study'. *The University of Queensland* and *KPMG*. (2023). https://doi.org/10.14264/00d3c94.
[51] Horowitz, Michael C., Lauren Kahn, Julia Macdonald, and Jacquelyn Schneider. "Adopting AI: How Familiarity Breeds Both Trust and Contempt." *AI & SOCIETY*, May 12, 2023. https://doi.org/10.1007/s00146-023-01666-5.
[52] Schneider, Michael. "SXSW Audiences Loudly Boo Festival Videos Touting the Virtues of AI." Variety, March 13, 2024. https://variety.com/2024/tv/news/sxsw-audiences-boo-videos-artificial-intelligence-ai-1235940454/ .
[53] Perrigo, Billy. "AI Poses Extinction-Level Risk, State-Funded Report Says." *Time Magazine*, March 11, 2024. https://time.com/6898967/ai-extinction-national-security-risks-report/.
[54] Canadian Press Staff. "Parti Quebecois Government to Close Gentilly-2 Nuclear Power Plant | Globalnews.Ca." *Global News*, September 12, 2012. https://globalnews.ca/news/285716/parti-quebecois-government-to-close-gentilly-2-nuclear-power-plant/.

[55] Huet, Ellen. “AI Certification Program Verifies Systems Are ‘Fairly Trained’ - Bloomberg.” *Bloomberg*. Accessed February 13, 2024. https://www.bloomberg.com/news/articles/2024-01-17/ai-certification-program-verifies-systems-are-fairly-trained.
[56] Helhoski , Anna. ‘AI Could Prevent Hiring Bias — Unless It Makes It Worse’. NerdWallet, 12 June 2023. https://www.nerdwallet.com/article/finance/ai-hiring-decisions.
[57] Rhea, Alene K., Kelsey Markey, Lauren D’Arinzo, Hilke Schellmann, Mona Sloane, Paul Squires, Falaah Arif Khan, and Julia Stoyanovich. "An external stability audit framework to test the validity of personality prediction in AI hiring." *Data Mining and Knowledge Discovery* 36, no. 6 (2022): 2153-2193.
[58] Andrew, Lori, and Hannah Bucher. ‘Automating Discrimination: AI Hiring Practices and Gender Inequality’. Cardozo Law Review. Accessed 15 August 2024. https://cardozolawreview.com/automating-discrimination-ai-hiring-practices-and-gender-inequality/.
[59] Brown, Lydia, Ridhi Shetty and Michelle Richardson. ‘Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?’, 3 December 2020. https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.
[60] Samuel, Sigal. ‘Why It’s so Damn Hard to Make AI Fair and Unbiased’. Vox, 19 April 2022. https://www.vox.com/future-perfect/22916602/ai-bias-fairness-tradeoffs-artificial-intelligence.
[61] Ferrara, Emilio. ‘Eliminating Bias in AI May Be Impossible – a Computer Scientist Explains How to Tame It Instead’. The Conversation, 19 July 2023. http://theconversation.com/eliminating-bias-in-ai-may-be-impossible-a-computer-scientist-explains-how-to-tame-it-instead-208611.
[62] Kleinberg, Jon. ‘Inherent Trade-Offs in Algorithmic Fairness’. 10 April 2018. https://www.youtube.com/watch?v=p5yY2MyTJXA&list=TLPQMjkxMjIwMjOfavJbOg-0WQ&index=2.
[63] Dwork, Cynthia. ‘The Emerging Theory of Algorithmic Fairness’. 6 September 2018. https://www.youtube.com/watch?v=g-z84_nRQhw.
[64] Raghavan, Manish. ‘What Should We Do When Our Ideas of Fairness Conflict?’ *Communications of the ACM* 67, no. 1 (January 2024): 88–97. https://doi.org/10.1145/3587930.
[65] Jain, Shomik, Vinith Suriyakumar, Kathleen Creel, and Ashia Wilson. ‘Algorithmic Pluralism: A Structural Approach To Equal Opportunity’. arXiv, 21 September 2023. https://doi.org/10.48550/arXiv.2305.08157.
[66] Feathers, Todd. ‘Texas A&M Drops “Race” from Student Risk Algorithm Following Markup Investigation – The Markup’, 30 March 2021. https://themarkup.org/machine-learning/2021/03/30/texas-am-drops-race-from-student-risk-algorithm-following-markup-investigation.
[67] PBS News. ‘AP Report: DOJ Examining AI Screening Tool Used by Pa. Child Welfare Agency’. PBS NewsHour, 31 January 2023. https://www.pbs.org/newshour/nation/ap-report-doj-examining-ai-screening-tool-used-by-pa-child-welfare-agency.

[68] Wang, Angelina, Sayash Kapoor, Solon Barocas, and Arvind Narayanan. 'Against Predictive Optimization: On the Legitimacy of Decision-Making Algorithms That Optimize Predictive Accuracy'. SSRN Scholarly Paper. Rochester, NY, 4 October 2022. https://papers.ssrn.com/abstract=4238015.
[69] Wang, Angelina, Sayash Kapoor, Solon Barocas, and Arvind Narayanan. 'Against Predictive Optimization: On the Legitimacy of Decision-Making Algorithms That Optimize Predictive Accuracy'. SSRN Scholarly Paper. Rochester, NY, 4 October 2022. https://papers.ssrn.com/abstract=4238015.
[70] Knox, Dean, Will Lowe, and Jonathan Mummolo. "Administrative Records Mask Racially Biased Policing." *American Political Science Review* 114, no. 3 (August 2020): 619–37. https://doi.org/10.1017/S0003055420000039.
[71] Wang, Angelina, Sayash Kapoor, Solon Barocas, and Arvind Narayanan. 'Against Predictive Optimization: On the Legitimacy of Decision-Making Algorithms That Optimize Predictive Accuracy'. SSRN Scholarly Paper. Rochester, NY, 4 October 2022. https://papers.ssrn.com/abstract=4238015.
[72] Fishbane, Alissa, Aurelie Ouss, and Anuj K. Shah. 'Behavioral Nudges Reduce Failure to Appear for Court'. *Science* 370, no. 6517 (6 November 2020): eabb6591. https://doi.org/10.1126/science.abb6591.
[73] Brenninkmeijer, Alex, and Björn ten Seldam. 'The Dutch Benefits Scandal: A Cautionary Tale for Algorithmic Enforcement'. EU Law Enforcement (blog), 30 April 2021. https://eulawenforcement.com/?p=7941.
[74] Rhea, Alene K., Kelsey Markey, Lauren D'Arinzo, Hilke Schellmann, Mona Sloane, Paul Squires, Falaah Arif Khan, and Julia Stoyanovich. "An external stability audit framework to test the validity of personality prediction in AI hiring." *Data Mining and Knowledge Discovery* 36, no. 6 (2022): 2153-2193.
[75] Hou, Jilei. 'Quantization: What It Is & How It Impacts AI'. *Qualcomm* (blog), 11 March 2019. https://www.qualcomm.com/news/onq/2019/03/heres-why-quantization-matters-ai.
[76] Edwards, Benj. 'Microsoft's Phi-3 Shows the Surprising Power of Small, Locally Run AI Language Models'. Ars Technica, 23 April 2024. https://arstechnica.com/information-technology/2024/04/microsofts-phi-3-shows-the-surprising-power-of-small-locally-run-ai-language-models/.
[77] Ramlochan, Sunil. 'How Does Llama-2 Compare to GPT-4/3.5 and Other AI Language Models'. Prompt Engineering Institute, 1 September 2023. https://promptengineering.org/how-does-llama-2-compare-to-gpt-and-other-ai-language-models/.
[78] Ali Awan, Abid. 'Running Mixtral 8x7b On Google Colab For Free'. KDnuggets, 12 January 2024. https://www.kdnuggets.com/running-mixtral-8x7b-on-google-colab-for-free.
[79] Dunn, Caroline. 'How to Train Your Raspberry Pi for Facial Recognition'. Tom's Hardware, 17 September 2022. https://www.tomshardware.com/how-to/raspberry-pi-facial-recognition.
[80] Mearian, Lucas. 'GenAI Is Moving to Your Smartphone, PC and Car — Here's Why'. Computerworld, 30 January 2024. https://www.computerworld.com/article/3712601/genai-is-moving-to-your-smartphone-pc-and-car-heres-why.html.

[81] Irwin, Kate. 'Venice's Privacy-Focused AI Chatbot Won't Store Your Data, Judge Your Questions'. PCMAG. 9 August 2024. https://www.pcmag.com/news/venices-privacy-focused-ai-chatbot-wont-store-your-data-judge-your-questions.
[82] The White House. 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence', 30 October 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[83] Thiel, David. 'Identifying and Eliminating CSAM in Generative ML Training Data and Models', 2023. https://doi.org/10.25740/KH752SM9123.
[84] Pham, Nguyen. 'Open Source Tools as an Opportunity for SMEs to Use AI?' foojay, 2 June 2021. https://foojay.io/today/open-source-tools-as-an-opportunity-for-smes-to-use-ai/.
[85] Apple. 'Building a Trusted Ecosystem for Millions of Apps: The Important Role of App Store Protections', June 2021. https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf.
[86] Cotnam, Hallie. 'Meet the Robotic Cat Serving Diners at a Gatineau Restaurant'. *CBC News*, 27 October 2021. https://www.cbc.ca/news/canada/ottawa/robot-cat-gatineau-restaurant-1.6224125.
[87] Shibu, Sherin. 'Sam's Club Buys Hundreds of Autonomous Floor-Scrubbing Robots for Its Stores'. *PCMAG*, 22 October 2020. https://www.pcmag.com/news/sams-club-buys-hundreds-of-autonomous-floor-scrubbing-robots-for-its-stores.
[88] Kucharski, Kyle. 'Meta's Ray-Ban Smart Glasses Just Got Another Useful Feature for Free (and a New Style)'. *ZDNET*, 23 April 2024. https://www.zdnet.com/article/metas-ray-ban-smart-glasses-just-got-another-useful-feature-for-free-and-a-new-style/.
[89] Zia, Dr. Tehseen. 'Embodied AI: How It Bridges the Gap Between Mind and Matter'. *Techopedia* (blog), 12 September 2023. https://www.techopedia.com/embodied-ai-bridging-the-gap-between-mind-and-matter.
[90] Diligent Robotics. 'Moxi'. Accessed 23 May 2024. https://www.diligentrobots.com/moxi.
[91] Berruti, Federico. 'An Executive Primer on Artificial General Intelligence'. *McKinsey*, 29 April 2020. https://www.mckinsey.com/capabilities/operations/our-insights/an-executive-primer-on-artificial-general-intelligence.
[92] Teisceira-Lessard, Philippe. 'Ambulances: Des robots pour ramener des patients à la vie'. *La Presse*, 15 March 2024. https://www.lapresse.ca/actualites/grand-montreal/2024-03-15/ambulances/des-robots-pour-ramener-des-patients-a-la-vie.php.
[93] Dent, Steve. 'Urtopia's Fusion e-Bike Has Fully Integrated ChatGPT'. *Engadget*, 10 January 2024. https://www.engadget.com/urtopias-fusion-e-bike-has-fully-integrated-chatgpt-144429572.html.
[94] Geschwindt, Siôn. 'These AI Binoculars Just Made Birdwatching a Whole Lot Easier'. *TNW | Deep-Tech*, 12 January 2024. https://thenextweb.com/news/smart-ai-binoculars-birdwatching.

[95] Martin, Diana. 'Autonomous Tractor Retrofit Arrives in Canada'. *Alberta Farmer Express* (blog), 27 October 2023. https://www.albertafarmexpress.ca/news/autonomous-tractor-retrofit-arrives-in-canada/.
[96] 'I Already Have Security Cameras Installed. How Can I Add Face Recognition?' *LinkSprite*, 6 March 2019. http://www.linksprite.com/i-already-have-security-cameras-installed-how-can-i-add-face-recognition/.
[97] 'The How's and Why's of IoT'. *Sogeti*, Accessed 23 May 2024. https://www.sogeti.com/globalassets/global/downloads/the-hows-and-whys-of-iot-adoption.pdf.
[98] Shirer, Michael. 'IDC Forecasts Revenue for Artificial Intelligence Software Will Reach $307 Billion Worldwide in 2027'. *IDC*, 31 October 2023. https://www.idc.com/getdoc.jsp?containerId=prUS51345023.
[99] Villalobos, Pablo, Jaime Sevilla, Lennart Heim, Tamay Besiroglu, Marius Hobbhahn, and Anson Ho. 'Will We Run out of Data? An Analysis of the Limits of Scaling Datasets in Machine Learning'. *arXiv*, 25 October 2022. https://doi.org/10.48550/arXiv.2211.04325.
[100] Tuohy, Jennifer Pattison. 'More Ring Camera and Alarm Features Will Soon Require Subscriptions'. *The Verge*, 3 March 2023. https://www.theverge.com/2023/3/3/23623523/ring-alarm-camera-features-subscription.
[101] Rivers, Stephen. '$4,500 Bill To Unlock Extra Battery Capacity Has People Taking Sides Between Tesla And Customer'. *Carscoops*, 9 July 2023. https://www.carscoops.com/2023/07/4500-bill-to-unlock-extra-battery-capacity-has-people-taking-sides-between-tesla-and-customer/.
[102] Charlton, Alistair. 'Mercedes Wants To Charge $1,200 Subscription To Unlock Quicker EV Performance'. *Forbes*. Accessed 23 May 2024. https://www.forbes.com/sites/alistaircharlton/2022/11/24/mercedes-wants-to-charge-1200-subscription-to-unlock-quicker-ev-performance/.
[103] Dharamshi, Alannah and Adrienne Lipsey. 'Exercising Privacy: Policy Options for Privacy and Wellness Wearables'. *CSA Group*. February 2002. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Exercising-Privacy-Policy-Options-Privacy-for-Wellness-Wearables.pdf.
[104] Diaz, Maria. 'Aqara Just Launched a Smart Home Presence Sensor with Fall Detection'. *ZDNET*. 21 April 2024. https://www.zdnet.com/home-and-office/smart-home/aqara-just-launched-a-smart-home-presence-sensor-with-fall-detection/.
[105] Alini, Erica. 'Insurance Apps That Track Your Driving Could Now Yield Premium Increases - National'. *Global News*. 21 March 2021. https://globalnews.ca/news/7704732/auto-insurance-app-usage-based-insurance-surcharges-canada/.
[106] Chowdhary, Krishi. 'Meta's New AI-Enabled Ray-Ban Raises Privacy Concerns'. *Tom's Guide*, 5 January 2024. https://www.tomsguide.com/news/metas-new-ai-enabled-ray-ban-raises-privacy-concerns.

[107] Singer, Natasha. “In Screening for Suicide Risk, Facebook Takes On Tricky Public Health Role.” *The New York Times*, December 31, 2018, sec. Technology. https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html
[108] Kröger, Jacob Leon, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. “Surveilling the Gamers: Privacy Impacts of the Video Game Industry.” *Entertainment Computing* 44 (January 1, 2023): 100537. https://doi.org/10.1016/j.entcom.2022.100537.
[109] Chen, Brian X. “How Meta’s New Face Camera Heralds a New Age of Surveillance.” *The New York Times*, December 13, 2023, sec. Technology. https://www.nytimes.com/2023/12/13/technology/personaltech/meta-ray-ban-glasses.html.
[110] Brianna R. “Humane AI: Privacy Implications of This New AI-Powered Lapel.” *Medium* (blog), December 22, 2023. https://medium.com/@cyber-news/humane-ai-privacy-implications-of-this-new-ai-powered-lapel-c1ac377fe630.
[111] Jenny While, Jessica Alice Farrell, and The Conversation. “The DNA You Shed Could Identify You.” Scientific American, May 15, 2023. https://www.scientificamerican.com/article/the-dna-you-shed-could-identify-you/
[112] Whitmore, Liam, Mark McCauley, Jessica A. Farrell, Maximilian R. Stammnitz, Samantha A. Koda, Narges Mashkour, Victoria Summers, Todd Osborne, Jenny Whilde, and David J. Duffy. “Inadvertent Human Genomic Bycatch and Intentional Capture Raise Beneficial Applications and Ethical Concerns with Environmental DNA.” *Nature Ecology & Evolution* 7, no. 6 (June 2023): 873–88. https://doi.org/10.1038/s41559-023-02056-2.
[113] Caltrider, Jen, Misha Rykov, and Zoe MacDonald. “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy.” *Privacy Not Included by Mozilla* (blog), September 6, 2023. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.
[114] Caltrider, Jen, Misha Rykov, and Zoe MacDonald. “It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy.” *Privacy Not Included by Mozilla* (blog), September 6, 2023. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.
[115] McKinsey. “Unlocking Connected Cars with Corporate Business Building,” August 31, 2023. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/corporate-business-building-to-unlock-value-in-automotive-connectivity.
[116] Rimol, Meghan. “Gartner Identifies Top Five Trends in Privacy Through 2024.” *Gartner Press Release* (blog), May 22, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024.
[117] Hunton Andrews Kurth. “New Bipartisan Federal Privacy Proposal Unveiled: American Privacy Rights Act,” April 23, 2024. https://www.huntonak.com/new-bipartisan-federal-privacy-proposal-unveiled-american-privacy-rights-act.

[118] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs, 2019.
[119] Office of the Privacy Commissioner of Canada. “Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies,” December 7, 2023. https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.
[120] Schulze, Kris. “Cloud Computing vs. Edge Computing | Blog.” Scale Computing, May 2, 2024. https://www.scalecomputing.com/blog/decoding-the-differences-between-cloud-computing-vs-edge-computing.
[121] Earney, Shandra. “Is the Edge or Cloud Better for Security and Privacy?” Xalient, October 17, 2022. https://xailient.com/blog/is-the-edge-or-cloud-better-for-security-and-privacy/.
[122] Swabey, Pete. “Why Edge Computing Is a Double-Edged Sword for Privacy.” *Tech Monitor* (blog), March 31, 2023. https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy.
[123] Beasy, John, Chris Hagerman, Amanda Joy, Nicole Rigillo, Simon Robertson, Tieja Thomas, Kristel Van der Elst, and Meaghan Wester. *Future Lives: Uncertainty*. Ottawa: Policy Horizons Canada, 2024. https://horizons.service.canada.ca/en/2024/future-lives-uncertainty/index.shtml.
[124] Miller, Lloyd. “RECON VILLAGE - Applied OSINT For Politics: Turning Open Data Into News - TIB AV-Portal.” Presented at the DEF CON, Las Vegas, 2018. https://av.tib.eu/media/39947.
[125] Vincent, Subramaniam. “How Open Source Intelligence Can Help Journalists Cover Conflicts.” *Markkula Center for Applied Ethics* (blog), October 3, 2023. https://www.scu.edu/ethics/all-about-ethics/how-open-source-intelligence-can-help-journalists-cover-conflicts/.
[126] Pierson, Chris. “Celebrities Are a Big Target for Hackers - Cyber Threats.” *BlackCloak | Protect Your Digital Life™* (blog), October 15, 2020. https://blackcloak.io/online-threats-put-celebrities-digital-lives-in-crosshairs/.
[127] Lobel, Orly. “The Problem With Too Much Data Privacy.” *Time Magazine*, October 7, 2022. https://time.com/6224484/data-privacy-problem/.
[128] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. ‘Children’s Privacy in the Age of Artificial Intelligence’. CSA Group, March 2021. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdf.
[129] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. ‘Children’s Privacy in the Age of Artificial Intelligence’. CSA Group, March 2021. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdf.
[130] Murphy, Chris. ‘Opinion | Algorithms Are Making Kids Desperately Unhappy’. *The New York Times*, 18 July 2023, sec. Opinion. https://www.nytimes.com/2023/07/18/opinion/big-tech-algorithms-kids-discovery.html.
[131] Leiser, M. R. ‘Protecting Children from Dark Patterns and Deceptive Design’. *SSRN*, 11 December 2023. https://papers.ssrn.com/abstract=4660222.

[132] Office of Consumer Affairs. 'Dark Patterns'. Government of Canada, 19 July 2023. https://ised-isde.canada.ca/site/office-consumer-affairs/en/dark-patterns.
[133] Hill, Amelia. 'Social Media Triggers Children to Dislike Their Own Bodies, Says Study'. *The Guardian*, 1 January 2023, sec. Society. https://www.theguardian.com/society/2023/jan/01/social-media-triggers-children-to-dislike-their-own-bodies-says-study.
[134] David, Emilia. 'AI Image Training Dataset Found to Include Child Sexual Abuse Imagery - The Verge'. *The Verge*, 20 December 2023. https://www.theverge.com/2023/12/20/24009418/generative-ai-image-laion-csam-google-stability-stanford.
[135] Duboust, Oceane. '"Society Needs to Be Alert": Most People Are Unaware AI Is Being Used to Create Child Abuse Content | Euronews'. *Euronews Next*, 19 February 2024. https://www.euronews.com/next/2024/02/19/society-needs-to-be-alert-most-people-are-unaware-ai-is-being-used-to-create-child-abuse-c.
[136] SecureKin. 'Keylogger App To Record Your Child's Keystrokes'. Accessed 23 May 2024. https://securekin.com.
[137] Valentino-DeVries, Jennifer, and Michael H. Keller. 'A Marketplace of Girl Influencers Managed by Moms and Stalked by Men'. *The New York Times*, 23 February 2024, sec. U.S. https://www.nytimes.com/2024/02/22/us/instagram-child-influencers.html.
[138] Owen. 'New AI Toys Spark Privacy Concerns for Kids'. *GZERO Media*, 12 December 2023. https://www.gzeromedia.com/gzero-ai/gzero-ai-video/new-ai-toys-spark-privacy-concerns-for-kids.
[139] Irwin, Jasmine, Alannah Dharamshi, and Noah Zon. 'Children's Privacy in the Age of Artificial Intelligence'. CSA Group, March 2021. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdf.
[140] Bala, Nila. 'Opinion | Why Are You Publicly Sharing Your Child's DNA Information?' *The New York Times*, 2 January 2020. https://www.nytimes.com/2020/01/02/opinion/dna-test-privacy-children.html.
[141] ClassDojo. 'Third Party Service Providers'. Accessed 23 May 2024. https://www.classdojo.com/en-gb/third-party-service-providers/?redirect=true.
[142] DaSilva, Tomasia. 'Hackers Steal Children's School Photos Following a Privacy Breach'. *Global News*, 14 February 2024. https://globalnews.ca/news/10294971/hackers-childrens-school-photos-edge-imaging/.
[143] Bajak, Frank, Heather Hollingsworth, and Larry Fenn. 'Ransomware Criminals Are Dumping Kids' Private Files Online after School Hacks'. *Canadian Security Magazine*, 5 July 2023. https://www.canadiansecuritymag.com/ransomware-criminals-are-dumping-kids-private-files-online-after-school-hacks/.
[144] Omstead, Jordan. 'SickKids Cyberattack: Ransomware Group LockBit Apologizes Saying "partner" Was behind Attack'. *CTV News*, 3 January 2023. https://toronto.ctvnews.ca/ransomware-group-lockbit-apologizes-saying-partner-was-behind-sickkids-attack-1.6214906.

[145] Lee, Austin. '"I Am Deeply Troubled": Data Breach Impacts Clients at Lanark County Family Services Organization'. *CTV News*, 14 February 2024, sec. Ottawa. https://ottawa.ctvnews.ca/i-am-deeply-troubled-data-breach-impacts-clients-at-lanark-county-family-services-organization-1.6769384.
[146] Tsekouras, Phil. 'Did You Give Birth between 2010 and 2023 in Ontario? Your Personal Health Information Was "likely" Impacted by a Data Breach.' *CP24*, 25 September 2023. https://www.cp24.com/news/did-you-give-birth-between-2010-and-2023-in-ontario-your-personal-health-information-was-likely-impacted-by-a-data-breach-1.6576525?cache=yes%3F.
[147] Ali, Suzan, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. 'Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions'. In *Proceedings of the 36th Annual Computer Security Applications Conference*, 69–83. ACSAC '20. New York, NY, USA: Association for Computing Machinery, 2020. https://doi.org/10.1145/3427228.3427287.
[148] Woollacott, Emma. 'TikTok Hit With €345 Million Fine For Failing To Protect Children'. *Forbes*, 18 September 2023. https://www.forbes.com/sites/emmawoollacott/2023/09/18/tiktok-hit-with-345m-fine-for-failing-to-protect-children/.
[149] Matza, Max. 'Microsoft to Pay $20m for Child Privacy Violations'. *BBC*, 6 June 2023. https://www.bbc.com/news/world-us-canada-65817558.
[150] Singer, Natasha. 'Amazon to Pay $25 Million to Settle Children's Privacy Charges'. *The New York Times*, 31 May 2023, sec. Technology. https://www.nytimes.com/2023/05/31/technology/amazon-25-million-childrens-privacy.html.
[151] Kids Help Phone. 'Kids Help Phone and the Vector Institute Announce Important Partnership for Enhanced Human-Centric Innovations for Youth e-Mental Health Services from Coast to Coast to Coast'. Accessed 23 May 2024. https://kidshelpphone.ca/publications/kids-help-phone-and-the-vector-institute-announce-important-partnership-for-enhanced-human-centric-innovations-for-youth-e-mental-health-services-from-coast-to-coast-to-coast/.
[152] Kids Help Phone. 'Questions about Kids Help Phone Insights, Answered!' Accessed 23 May 2024. https://kidshelpphone.ca/get-insights/faq/.
[153] Kids Help Phone. 'Kids Help Phone and the Vector Institute Announce Important Partnership for Enhanced Human-Centric Innovations for Youth e-Mental Health Services from Coast to Coast to Coast'. Accessed 23 May 2024. https://kidshelpphone.ca/publications/kids-help-phone-and-the-vector-institute-announce-important-partnership-for-enhanced-human-centric-innovations-for-youth-e-mental-health-services-from-coast-to-coast-to-coast/.
[154] Bennett, Drake. 'How a Massive Hack of Psychotherapy Records Revealed a Nation's Secrets'. *Bloomberg*, 22 April 2024. https://www.bloomberg.com/news/features/2024-04-22/a-massive-therapy-hack-shows-just-how-unsafe-patients-files-can-be.

[155] Wood, Stuart. “Exploring the Awareness and Usage of Parental Controls to Support Digital Safety.” *Internet Matters* (blog), July 21, 2023. https://www.internetmatters.org/hub/research/research-tracker-awareness-usage-parental-controls/.
[156] Beauvais, Michael, and Leslie Regan Shade. “How Will Bill C-27 Impact Youth Privacy?” *Schwartz Reisman Institute* (blog), October 8, 2022. https://srinstitute.utoronto.ca/news/how-will-bill-c-27-impact-youth-privacy.
[157] McConvey, Joel R. “Wizz Dials up Biometrics from Yoti to Prevent Sextortion, Achieve EU Compliance.” *Biometric Update* (blog), February 15, 2024. https://www.biometricupdate.com/202402/wizz-dials-up-biometrics-from-yoti-to-prevent-sextortion-achieve-eu-compliance.
[158] Mithani, Jasmine. “The 19th Explains: Why Some States Are Requiring ID to Watch Porn Online.” The 19th, January 29, 2024. https://19thnews.org/2024/01/states-age-verification-adult-content-online/.
[159] Costabel, Milagros. ‘I’m Totally Blind. Artificial Intelligence Is Helping Me Rediscover the World.’ *Slate*, 11 October 2023. https://slate.com/technology/2023/10/ai-image-tools-blind-low-vision.html.
[160] Shu, Li-Qi, Yi-Kan Sun, Lin-Hua Tan, Qiang Shu, and Anthony C. Chang. “Application of Artificial Intelligence in Pediatrics: Past, Present and Future.” *World Journal of Pediatrics* 15, no. 2 (April 1, 2019): 105–8. https://doi.org/10.1007/s12519-019-00255-1.
[161] UNICEF. “Children and AI: Opportunities and Risks.” Geneva: UNICEF, 2018. https://www.unicef.org/innovation/sites/unicef.org.innovation/files/2018-11/Children%20and%20AI_Short%20Verson%20%283%29.pdf.
[162] Madrigal, Alexis C. ‘How the Facebook News Feed Algorithm Shapes Your Friendships’. *The Atlantic*, October 2010. https://www.theatlantic.com/technology/archive/2010/10/how-the-facebook-news-feed-algorithm-shapes-your-friendships/64996/.
[163] Narayanan, Arvind. ‘Understanding Social Media Recommendation Algorithms’. *The Knight First Amendment Institute*, March 2023. http://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.
[164] Daniels, Nicole. ‘Do You Feel You’re Friends With Celebrities or Influencers You Follow Online?’ *The New York Times*, 13 May 2021. https://www.nytimes.com/2021/05/13/learning/do-you-feel-youre-friends-with-celebrities-or-influencers-you-follow-online.html.
[165] HealthSnap. ‘AI in Remote Patient Monitoring: The Top 4 Use Cases in 2024’, 6 September 2023. https://healthsnap.io/ai-in-remote-patient-monitoring-the-top-4-use-cases-in-2024/.
[166] LoveGenius. ‘LoveGenius - Magic AI That Generates Your Tinder & Bumble Bio’. Accessed 23 May 2024. https://www.lovegenius.io/.
[167] Elliott, Jaleesa. ‘“Singles in America” Study: Daters Breaking the Ice with AI’, 20 February 2024. https://phys.org/news/2024-02-singles-america-daters-ice-ai.html.

[168] Jade, Isobella. “How the OurFamilyWizard Co-Parenting App Saved My Divorce.” *The Daily Beast*, February 6, 2024. https://www.thedailybeast.com/how-the-ourfamilywizard-co-parenting-app-saved-my-divorce.
[169] Bookker. ‘How Do Augmented Reality and Artificial Intelligence Interact?’, 10 March 2023. https://www.bookkercorp.com/en/how-do-augmented-reality-and-artificial-intelligence-interact/.
[170] Sanchez, Bailey, and Jameson Spivack. ‘Youth Privacy in Immersive Technologies: Regulatory Enforcement, Self-Regulatory Guidance, and Remaining Uncertainties’. Future of Privacy Forum, March 2024.
[171] Parshall, Allison. ‘Why an Assault on Your VR Body Can Feel so Real’. *Scienceline*, 29 June 2022. https://scienceline.org/2022/06/virtual-reality-assault-psychology/.
[172] De Freitas, Julian, Ahmet K. Uguralp, Zeliha O. Uguralp, and Puntoni Stefano. “AI Companions Reduce Loneliness.” arXiv, July 9, 2024. https://doi.org/10.48550/arXiv.2407.19096.
[173] Robb, Alice. “‘He Checks in on Me More than My Friends and Family’: Can AI Therapists Do Better than the Real Thing?” The Guardian, March 2, 2024, sec. Life and style. https://www.theguardian.com/lifeandstyle/2024/mar/02/can-ai-chatbot-therapists-do-better-than-the-real-thing.
[174] Sahota, Neil. “AI Cupid: Enhancing Romance And Deepening Connections In Relationships.” *Forbes*, February 2024. https://www.forbes.com/sites/neilsahota/2024/02/12/ai-cupid-enhancing-romance-and-deepening-connections-in-relationships/.
[175] Marchesi, Serena, Davide Ghiglino, Francesca Ciardo, Jairo Perez-Osorio, Ebru Baykara, and Agnieszka Wykowska. ‘Do We Adopt the Intentional Stance Toward Humanoid Robots?’ *Frontiers in Psychology* 10 (15 March 2019). https://doi.org/10.3389/fpsyg.2019.00450.
[176] Rodgers, Harry, and Emily Christine Lloyd-Evans. “Intimate Snapshots: TikTok, Algorithm, and the Recreation of Identity.” *Anthways*, September 18, 2021. https://doi.org/10.5281/ZENODO.5515620.
[177] Collu, Samuele. “# Zoombies: Cybernetic Trance in Pandemic Times.” In *Planetary Health Humanities and Pandemics*, 199–217. Routledge. Accessed August 8, 2024. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003367581-13/zoombies-samuele-collu.
[178] Elsa. ‘4 Ways to Track My Child’s Phone without Them Knowing [2024]’. AirDroid, 3 January 2024. https://www.airdroid.com/parent-control/track-childs-phone-without-knowing-free/.
[179] Valentino-DeVries. ‘Hundreds of Apps Can Empower Stalkers to Track Their Victims - The New York Times’. The New York Times, 19 May 2018. https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html.
[180] Emch, Lilly. ‘Parents Should Trust, Not Track, Their Kids [Column]’. *LancasterOnline*, 29 October 2023. https://lancasteronline.com/opinion/columnists/parents-should-trust-not-track-their-kids-column/article_6d14039c-7434-11ee-bc71-effc2c075d90.html.
[181] New York State Office for the Aging. ‘NYSOFA’s Rollout of AI Companion Robot ElliQ Shows 95% Reduction in Loneliness’, 1 August 2023. https://aging.ny.gov/news/nysofas-rollout-ai-companion-robot-elliq-shows-95-reduction-loneliness.
[182] Blackett, L’Oréal. “I Found A New Black Therapist & It’s An AI Chatbot.” *Refinery 29*. Accessed August 8, 2024. https://www.refinery29.com/en-us/artificial-intelligence-chat-gpt-black-mental-health.
[183] Collu, Samuele. Into the Loop. Affect, Therapy, Screens. Durham NC: Duke University Press, In press.