We negate the resolution Resolved: In the United States, the benefits of the use of generative artificial intelligence in education outweigh the harms.

Generative AI: MIT in 2023 https://news.mit.edu/2023/explained-generative-ai-1109 defines: **Generative AI** can be thought of as a machine-learning model that is **trained to create new data,** rather than making a prediction about a specific dataset. A generative AI system is **one that learns to generate more objects** that look like the data it was trained on.

Education: Cambridge https://dictionary.cambridge.org/us/dictionary/english/education defines: the process of teaching or learning, especially in a school or college, or the knowledge that you get from

Overview: Effectiveness

First – You should be skeptical of AI's effectiveness – almost no research supports it, and those studies which do are corporate-funded and have methodological flaws.

Williamson 24 (Ben Williamson is a Chancellor's Fellow at the Centre for Research in Digital Education and the Edinburgh Futures Institute at the University of Edinburgh. Alex Molnar is a Research Professor at the University of Colorado Boulder. Faith Boninger is NEPC's Publications Manager and Co-Director of NEPC's Commercialism in Education Research Unit and holds a PhD from Ohio State University. Williamson, B. Molnar, A., & Boninger, F. (2024). "Time for a pause: Without effective public oversight, AI in schools will do more harm than good." Boulder, CO: National Education Policy Center. http://nepc.colorado.edu/publication/ai)

AI in Education Since the 1960s, scientists and technology companies have explored ways to apply AI in education. AI in Education (AIED) is a major field of research and development.55 The AI applications being promoted to schools today were preceded in the 1960s and 1970s by "Intelligent Tutoring Systems" and "Computer Assisted Instruction" systems.56 Since the early 2000s, researchers have gathered, stored, and analyzed massive quantities of educational data with the intention of informing institutional and instructional strategies.57 These approaches are now routinely considered synonymous with AIED, and have also been rapidly commercialized by the ed tech industry.58 Most AIED applications employ big data and machine learning to produce various predictions and automated actions—such as predicting that a student may fail an assessment or creating a "personalized" intervention intended to produce a desired learning outcome.59 Research on AI in education has developed and tested various approaches and reported modest effectiveness on measurable learning achievement—performance on quizzes and tests, for example.60 Current excitement about its potential is motivating both public and private sources to generously fund researchers trying to find ways to improve learning outcomes using AI.61 However, the assumption that AI in education can be understood primarily as a technical matter best addressed by scientists and companies is increasingly challenged by researchers who argue that a narrowly technical perspective may lead to both bad policy and bad pedagogy.62 They point out that AI exists in social, economic, and political contexts that shape its development and uses.63 How AI is adopted by different educational stakeholders (including AIED researchers, ed tech entrepreneurs, corporate leaders, and policymakers) will have significant implications for its use in schools.64 The fact that entrepreneurs and corporations funded by venture capital and private equity are rushing to promote AI in education will inevitably narrow possible applications to those preferred by stakeholders with financial interests.65 Small-scale ed tech start-ups and Big Tech corporations alike see AI as an opportunity,66 lev eraging popular hype to market such education products as personalized learning programs, automated lesson plan generators, and AI tutoring chatbots, called "tutorbots," to schools.67 **Compelling evidence** for the effectiveness of tutorbots in education **remains scarce**,68 though this does not prevent entrepreneurs and researchers from proclaiming their usefulness.69 Policymakers routinely invoke AI rhetorically, calling on schools to embark on "digital transformation," 70 often with little attention to social, economic, legal, or ethical implications.71 These calls dovetail with existing political priorities on performance monitoring, account, ability, efficiency, and effectiveness—all of which require extensive collection of data about students.72 Although systems of test-based accountability have existed in schools since the 1990s,73 they will expand and intensify as AI is used to continuously monitor and assess student learning.74 As a result, commercial AI systems will increasingly serve as private actors in public education as schools, districts, and governments relinquish key tasks, functions, and responsibilities to third-party technology vendors.75 Existing and potential uses of AI in education are not merely innovative technical add-ons to teaching and learning practices or engineering solutions to schools' existing pedagogic and administrative problems. Rather, AI in education has been spurred by multiple forces: longstanding efforts by scientists to measure, predict, and support learning processes and outcomes; commercial aspirations to profit from selling products to schools; and the political objective of being perceived as having improved school efficiency and accountability while cutting costs. As things currently stand, these ambitions have begun to coalesce into a vision of AI-driven schooling in which commercial products assess student learning, automate teaching, and make decisions about student progress. Inadequate Research Base Despite the extensive research in the field of AI in Education (AIED) and the burgeoning research on machine learning, there is **remarkably little** evidence to support claims of AI's ability to "transform" schools.76 While AIED researchers have produced many research findings, their studies tend to focus primarily on measures of individual student engagement and performance (assessed by standardized achievements tests), or on "engineering" problems such as designing increasingly sophisticated algorithms and enhancing machine learning effectiveness.77 Overall, AIED studies tend to find ambiguous results, lack independence and scale, and fail to address more fundamental

questions about educational goals.78 AIED research therefore often promotes a view of education transformation as improving measurable individual outcomes despite very limited evidence that AI "works."79 In effect, such studies reduce well-researched and nuanced theories of how humans learn to whatever can be made into a mathematical model (however complex), and they ignore the contested terrain of exactly which goals and curriculum public schools should embrace.80 Moreover, claims that AI can solve major educational problems—such as lack of qualified teachers, student underachievement, and educational inequalities—rely to a considerable extent on **conjecture rather than evidence.**81¶ Even more problematic are the serious methodological flaws in machine learning research that call into question the validity of hundreds of studies.82 The nature of the flaws, in general, leads toward "over optimism" with respect to the usefulness and value of machine learning applications in a variety of fields.83 These findings are particularly concerning because they call into question not only commercial marketing claims, but also the scientific evidence base supporting the widespread implementation of AI systems in all sectors,84 including education. Finally, because of the very high computing costs associated with running machine learning models, most researchers have to rely on systems from the dominant AI companies themselves in order to conduct research85—the same corporations that often fund AI studies.86 This makes research dependent on corporate resources, funds, and business practices, giving AI firms considerable influence over not only AI development, but also the academic research that depends on their systems.87 It also compromises an important part of the research process, which is reproducing findings to verify their validity. When a company changes or stops supporting a particular model, researchers cannot reproduce studies conducted earlier.88 This renders the research base unstable and unverifiable—and thus unusable as a basis for assessing subsequent models.

Contention 1: Cost

Integration of gen AI is a blatant attempt at corporate takeover of schools

Williamson 2024 (Ben Williamson is a Chancellor's Fellow at the Centre for Research in Digital Education and the Edinburgh Futures Institute at the University of Edinburgh. Alex Molnar is a Research Professor at the University of Colorado Boulder. Faith Boninger is NEPC's Publications Manager and Co-Director of NEPC's Commercialism in Education Research Unit and holds a PhD from Ohio State University. Williamson, B. Molnar, A., & Boninger, F. (2024). "Time for a pause: Without effective public oversight, AI in schools will do more harm than good." Boulder, CO: National Education Policy Center. http://nepc.colorado.edu/publication/ai)

School administrators and teachers already use an array of digital educational technologies in teaching and management.10 Their use has increasingly **obscured educational decision-making**, made a mockery of student privacy rights, and allowed student data to be exploited for non-school purposes.11 In the absence of effective public oversight, the introduction of AI systems and applications in education will likely intensify these problems and **create many more.**12,13 As existing school-focused platforms and applications are updated to include AI, the immediate danger facing educators is not a future apocalypse. Instead, the danger is that AI models and applications will become enmeshed in school processes and procedures in ways that allow **private entities** to **increasingly control** the structure and content of public education, to **reinforce surveillance** practices, and to **amplify existing biases** and inequalities.14 For decades, academic researchers have worked on AI models for use in schools.15 Today, however, it is commercial enterprises that are **aggressively pushing AI** (and its attendant risks) into classrooms.16 The campaign to promote AI in education follows the logic of a half century of commercial, political, and ideological efforts to privatize and **commercialize education.**17 Given this logic it is not surprising that, despite the known dangers, corporations, private researchers, and governments are aggressively promoting the use of AI18 before a statutory and regulatory framework has been put in place to ensure that AI programs are transparent and subject to effective public scrutiny and control.19 This puts schools under tremendous pressure to accept AI as an inevitable upgrade to existing processes.20 Computer scientists and software developers focus primarily on technical engineering questions21 and corporate leaders and **investors prioritize profit** 22 over the common good. Nevertheless, educators are being asked to trust that these people, who have **no educational expertise** and who stand to **financially benefit** when AI is used in schools, are best suited to imagine and lead educational transformation.

AI systems take money from poor districts.

Williamson et.al 24 (Ben Williamson is a Chancellor's Fellow at the Centre for Research in Digital Education and the Edinburgh Futures Institute at the University of Edinburgh. Alex Molnar is a Research Professor at the University of Colorado Boulder. Faith Boninger is NEPC's Publications Manager and Co-Director of NEPC's Commercialism in Education Research Unit and holds a PhD from Ohio State University. Williamson, B. Molnar, A., & Boninger, F. (2024). "Time for a pause: Without

effective public oversight, AI in schools will do more harm than good." Boulder, CO: National Education Policy Center. http://nepc.colorado.edu/publication/ai)

Dangers in Administration Increased Costs Learning management systems already used in many schools, such as Google Classroom, Blackboard, and Canvas, are beginning to integrate AI into their platforms.150 Google Classroom, with its suite of nominally "free" software and low-cost Chromebook hardware, dominates the market.151 It has already announced the launch of AI-based adaptive learning addons to Classroom, with associated additional costs for schools, as well as plans to upgrade Classroom further with generative language AI.152 "Practice Sets" is Google's AI-based adaptive learning system for education, and "Duet AI" is its "collaboration partner" for teachers.153 In addition to any pedagogical implications associated with using Google Classroom, its integration of further AI and automation into many aspects of school functioning also carries potentially significant administrative implications.154 The most significant of these is to obscure the rationale for administrative decisions about critical institutional issues when decision-making is ceded to opaque machine learning systems controlled by tech firms. Google Classroom, for example, integrates with hundreds of other ed tech products and can synchronize with a school's student information systems.155 It offers Google cloud services such as single sign-on, identity management, and device management, as well as plagiarism detection, automated grading, teaching templates, student grouping, and administrative analytics to facilitate "data-driven decisions."156 Such management systems facilitate the **transfer of control** of schools from the **public to private** corporations by acting as central conduits through which all of a school's digital activities must pass—making it hard for educators or administrators to see how any decisions based on the data have been made.157 Because running AI is costly, the use of AI programs in schools will necessarily require schools to pay for operating costs for an increasing number of pedagogic and administrative AI applications. The promise that AI can save schools money by reducing staffing costs is likely illusory, as schools will probably be required to pay costly fees for accessing AI facilities. In other words, rather than saving money, administrative applications are more likely to shift existing funds to monopolistic technology providers. Khanmigo and Google Classroom already illustrate how this works. Khan Academy, when it provides Khanmigo to districts, currently charges those districts **$60 per student** for annual use, citing high computing costs associated with OpenAI's GPT-4 as the justification for the charges.158 Likewise, districts must also pay for Google Classroom's AI upgrades. To access its latest adaptive learning application, Practice Sets, they must switch from the free basic¶ offering to a for-fee premium package.159 In other words, tech firms are **extracting value** from school budgets to defray the high computing costs associated with AI (and grow company value).160

Increased Threats to Student Privacy¶ AI applications collect and aggregate data in order to function. In so doing, they normalize digital surveillance and privacy invasions in school.161 In practice, education technology¶ companies use applications like Google Classroom to routinely collect as much data as possible, well beyond that required to perform their assigned tasks.162¶ Although proponents of using AI in education tend to emphasize the efficiency of data-driven¶ administrative systems, privacy-related threats to equity are inherent in it.163 This is because¶ AI models are built using massive data sets that can be used to profile, compare, and assess¶ individuals who are then subject to potentially discriminatory decisions based on "statistical¶ dossiers" of their personal lives.164 Thus, a significant danger of digital technology in general,¶ and of the privacy-invasive model of AI in particular, is that they can reproduce and amplify¶ existing forms of inequality in education by using datasets containing examples of historic¶ bias and discrimination.165 For example, if a big data set indicates that certain marginalized¶ groups have underperformed historically, then a software application may be biased against¶ individuals from such groups in the future, singling out and targeting them as "at-risk" and¶ closing down or limiting their opportunities to access information and resources.166¶ Moreover, school data systems are vulnerable to breaches, hacks, ransomware, and denial-of-service attacks.167 A data breach at the student-tracking ed tech company Illuminate,¶ for example, compromised the educational data of at least a million public school students¶ and prompted New York City's Department of Education to ask schools to stop using Illuminate's products.168 School data systems feature highly detailed and intimate student¶ information, including personal and demographic data, grades, attendance, behavioral information, and other confidential information. Increasing AI capacity in ed tech products¶ may exacerbate these vulnerabilities, as student data are collected at even greater scale by a¶ wide range of companies—including AI companies—that offer only vague data privacy protections.169 Reduced Transparency and Accountability¶ Finally, enabling AI to play a role in school administration will reduce the transparency and¶ accountability of decision-making.170 Many digital products already used in schools are neither transparent nor accountable because current law and regulation allows companies to¶ shield the inner working of their products behind proprietary protections.171¶ AI is even more opaque than other digital programs.172 Black box machine learning and AI¶ models are so complicated that their outputs are often impossible to explain or interpret.173¶ Although in many cases simpler and more accessible statistical models can produce equally accurate results, companies benefit from selling access to proprietary models that require¶ customers to trust the systems and simply accept being unable to verify results.174 If the¶ system makes a mistake, it might never be identified or redressed and the public suffers the¶ consequences. For example, the facial identification systems used for remote testing often¶ fail to accurately identify individuals or mistakenly flag student behaviors as suspicious, but¶ they are very hard for students to challenge.175¶ In high-stakes decision-making in a sector like education, allowing such impenetrable models to assume responsibility for key administrative procedures necessarily means the creation of schools in which school leaders and teachers will be unable to exercise judgment,¶ provide a rationale, or take responsibility for classroom and institutional decisions.176¶ Considerations for the Future¶ Is AI Development Responsible?

The rapid creation of AI applications for schools raises the urgency of prioritizing ethics,¶ student rights, and social responsibility in their development.177 Responsible AI development would ensure that products are safe and trustworthy, designed to benefit people, communities, and society, and mitigate harms.178 As yet, there is little indication that such values are adequately addressed in education applications.179 Unfortunately, academic AIED¶ researchers have tended to ignore them or delegate addressing them to the educational tech¶ industry and policy centers.180 This complacency—along with the money and power held by commercial actors—enables commercial rather than educational imperatives to guide the development of AI and furthers political interests promoting relentless testing and school¶ surveillance.181¶ Responsible governance would require the companies developing AI to commit to transparent and responsible product design, and also to monitoring, understanding, and mitigating¶ the continuous impacts of AI in various contexts. Of particular concern is the automation¶ of decisions with "irreversible and severe consequences."182 For example, technologies to¶ identify emotions are currently being developed to assess if a person is lying and cheating.183¶ These technologies are inherently inaccurate, however, and an inaccurate judgment that a¶ student has cheated or that a witness is lying could have dire consequences for their lives.¶ Responsible AI governance might lead to delaying or indefinitely pausing development of¶ such technologies.¶ Although several responsible AI initiatives have produced principles, frameworks or checklists for safe and trustworthy AI development and accountability,184 these agendas can be¶ manipulated through various forms of industry lobbying and efforts to water down their¶ scope or possibilities of enforcement.185 Expanding responsibility for product safety to include the wide ra nge of people or organizations that build and use AI—rather than leaving it to technicians and business alone—would mitigate such dangers.186 Among the many obstacles to the implementation of responsible policies governing AI is their cost. The goal of profit-seeking business is to shift to the public as many costs as possible while garnering the highest possible private rate of return on investments. Public oversight of AI necessarily entails either public ownership or a comprehensive regulatory regime adequately financed to achieve its mission. The question is, where will the money come from? Moreover, the required regulation flies in the face of 50 years of policy devoted to deregulation and

privatization. It would demand a fundamental rethinking of the government's relationship to commercial interests. Such rethinking would, without a doubt, be attacked by self-interested parties as not only too costly but also as stifling innovation and promoting inefficiency. While these arguments may be relevant in individual circumstances, they are neither generally nor self-evidently true. From the perspective of education, responsible governance of AI therefore entails significantly more commitment than the simple principles of responsible development issued by industry. It also requires costly and ongoing monitoring of the effects of AI in classroom contexts. It may also require delays and indefinite pauses in development where warranted—such as, for example, in cases where commercial AI providers seek to introduce products into schools with insufficient evidence that they produce beneficial outcomes, or when those products automate professional judgement with potentially negative consequences, or when they inadequately address questions of AI ethics directly relevant to education. Is AI Inevitable? AI products are moving into schools at dizzying speed. As we have noted, this is in part the result of the pressure on schools to "modernize" by adopting the latest products that the¶ technology industry offers. There is already a consensus of sorts that the move to AI is inevitable. The director of educational technology at Newark Public Schools made the case to the¶ New York Times when he explained why his district adopted Khanmigo: "It's important to¶ introduce our students to it, because it's not going away."187¶ The de facto requirement that students serve as a technology company's experimental subjects might be explained by the initially low entry cost for school districts. Struggling districts, especially, might be willing to gamble that a technological innovation might turn things around for their students. However, before placing that bet it would be valuable to¶ first ask some fundamental questions. Computer scientist Joseph Weizenbaum posed such¶ concerns 50 years ago, essentially arguing that no technology—including AI—should be implemented unless we know that it is both necessary and good.188

The impact is tradeoff – programs like special education will be cut first when AI saps public budgets.

Sinha 24 (Tannistha Sinha covers education, housing, and politics in Houston for the Houston Defender Network as a Report for America corps member. She graduated with a master of science in journalism from the University of Southern California in 2022, and was the recipient of the Annenberg Graduate fellowship. , "Texas school districts face $300 million federal special education funding cut", DefenderNetwork, https://defendernetwork.com/news/education/texas-special-education-funding-cuts/, 1-26-2024, DOA: 2-21-2025)

Texas public schools unexpectedly lost $300 million per year in federal special education funding amidst rising costs, the Texas Health and Human Services Commission notified school districts on Dec. 15. The cuts are to the School Health and Related Services (SHARS), a federal special education program that allows Texas local educational agencies (LEAs) and shared service arrangements (SSAs) to request reimbursement for Medicaid health-related services. School districts are eligible for partial reimbursements when they directly offer medical services to students with special needs, instead of relying on a doctor or nurse. The loss in annual funding relates to Medicaid reimbursements for special education students. It followed a court ruling in a billing disagreement between school districts and the federal government, dating back to 2017.

Contention 2 : Exploitation

Gen harms - exploited workers prove

Rowe 2023

Rowe, Niamh. 2023. "'It's Destroyed Me Completely': Kenyan Moderators Decry Toll of Training of AI Models." The Guardian, August 2, 2023, sec. Technology. https://www.theguardian.com/technology/2023/aug/02/ai-chatbot-training-human-toll-content-moderator-meta-openai.

'It's destroyed me completely': Kenyan moderators decry toll of training of AI models

Okinyi, a former content moderator for Open AI's ChatGPT in Nairobi, Kenya, is one of four people in that role who have filed a petition to the Kenyan government calling for an investigation into what they describe as exploitative conditions for contractors reviewing the content that powers artificial intelligence programs.

"It has really damaged my mental health," said **Okinyi.**

The 27-year-old said he would would view up to 700 text passages a day, many depicting graphic sexual violence. He recalls he started avoiding people after having read texts about rapists and found himself projecting paranoid narratives on to people around him. Then last year, his wife told him he was a changed man, and left. She was pregnant at the time. "I lost my family," he said.

The petition filed by the moderators relates to a contract between OpenAI and Sama – a data annotation services company headquartered in California that employs content moderators around the world. While employed by Sama in 2021 and 2022 in Nairobi to review content for OpenAI, the content moderators allege, they suffered psychological trauma, low pay and abrupt dismissal.

Bots like ChatGPT are examples of large language models, a type of AI algorithm that teaches computers to learn by example. To teach Bard, Bing or ChatGPT to recognize prompts that would generate harmful materials, algorithms must be fed examples of hate speech, violence and sexual abuse. The work of feeding the algorithms examples is a growing business, and the data collection and labeling industry is expected to grow to over $14bn by 2030, according to GlobalData, a data analytics and consultancy firm.

Much of that labeling work is performed thousands of miles from Silicon Valley, in east Africa, India, the Philippines, and even refugees living in Kenya's Dadaab and Lebanon's Shatila – camps with a large pool of multilingual workers who are willing to do the work for a fraction of the cost, said Srravya Chandhiramowuli, a researcher of data annotation at the University of London.

Global Ai is growing and so is exploitation

Graham 24
We, AI. 2024. "Newsreel Asia." Newsreel Asia. July 13, 2024.
https://www.newsreel.asia/articles/the-exploited-workers-behind-the-ai-we-use.

The global AI market, projected to grow from $200 billion in 2023 to nearly $2 trillion by 2030, is drawing millions of workers into its rapidly expanding sector. This surge in artificial intelligence affects industries like logistics, manufacturing, and healthcare but masks a harsh reality: **the widespread exploitation of labour that powers these advanced systems**

Thish supercedes human rights

Arun 2024 "Transnational AI and Corporate Imperialism." 2024. Carnegie Endowment for International Peace. 2024.
https://carnegieendowment.org/research/2024/10/transnational-ai-and-corporate-imperialism?lang=en

.

Global informational capitalism and corporate imperialism drive companies to take advantage of the uneven geographical conditions of capital accumulation, which explains why AI's business models inevitably harm vulnerable people that cannot access state protection.[50] If one state legislates to protect data annotators, companies can move to a different state that permits their exploitative practices. If one state bans an AI product, companies can sell it in a more permissive market. Companies are driven to compete to maximize profits, and they seek access to new markets as they reach the limits of their initial markets. They engage in exploitation of resources to increase their profit margins.

Given the distribution of capital, it is unsurprising that a significant proportion of the demand for digital labor comes from the so-called Global North, while the supply of labor tends to come from what was once called the Global South.[5] More than one scholar focusing on global capitalism has noted that the exploited workforces tend to be concentrated in the Global South.[51] After painstaking empirical work on the people who annotate and verify data for three major platforms operating in Latin America, Julian Posada concluded that American technology companies, often through intermediaries, use poorly paid workers in countries in crisis as a source of cheap labor.[53] The platformization of labor breaks down traditional organizing structures: workers are unable to bargain with the companies since they see themselves as being in competition, not in solidarity, with each other.[54] There are no institutional or structural solutions to protect them. Kalindi Vora argued that there are "**structural inequalities that result from histories of colonial, racial, and gender dispossession that map directly onto new technological platforms."**[55]

The lucrative business of data annotation, through which companies hire Kenyan workers for less than $2 an hour, is an example of how the exploitation of cognitive labor is a part of the creation of global AI systems.[56] While the exploitation of physical labor—whether that of the miners and assembly line workers or those who clean the waste that these systems generate— is also a part of AI's value chain, informational capitalism has inherited this set of practices from industrial capitalism. The exploitation of cognitive labor is characteristic of informational capitalism but derives from, and is co-extensive with, industrial capitalism's systems for labor exploitation. Industrial capitalism also exploited immaterial labor such as affective and biological labor.[57] Informational capitalism has created new practices to do so. These new practices can be more easily understood in terms of their connection to capitalism.[58]

Uneven legal protections in states around the world leave some populations vulnerable to exploitation and other harms resulting from the companies' practices. The history of capitalism is full of such examples. Consider product liability laws in the United States, which emerged from mass torts or from regulators: products like banned pesticides that cannot be sold or used in the United States are exported to other markets.[59] Apart from the harm that this causes to people in states without regulatory safeguards, the risk can boomerang to the United States through products further down the value chain.[60] When the United States imports produce grown using banned pesticides, its population is also affected. While international coordinated action is taken from time to time, like in the case of the insecticide DDT, capitalism's legal order permits risky products to find markets that are unable to offer resistance.[61] Informational capitalism is currently governed by a similarly permissive legal order—if the United States and EU regulate to protect their populations, harmful AI products will continue to be developed and inflicted on the people of other states. Powerful states' legislators and regulators might wish to consider, right from the start, how to identify and restrict the algorithmic equivalent of DDT.

Even those who are not concerned about people at a distance should be concerned about the proliferation of harmful algorithmic systems and datasets that cause downstream problems.[62] An AI system encoded with outdated and discriminatory information perpetuates harm. Take, for example, the databases that have designated certain freedom fighters and opposition leaders around the world as terrorists. Imagine how this could affect someone such as former South African President Nelson Mandela, who was once designated as a terrorist and later underwent a change of status.[63] AI systems trained on old datasets may not encode this change of status and similar changes of the corresponding statuses of people connected with such figures, meaning that such systems may still flag all these people as potential terrorists on the basis of outdated information. Even seemingly safe and stable states go through phases of discrimination and persecution and will probably eventually be affected by harmful AI products that are created and available because they are marketable.[64] Even if the products are never used in the United States or the EU, persecution, oppression, and violence elsewhere in the world will be visible at the borders of more privileged countries in the form of asylum-seekers, and an increase in global crime and terrorism.

The use of Gen AI props up exploitation in countries in the global south

C3: Don’t trust AI

Generative AI is inherently unverifiable and creates false information. This means that even if students use it, they aren’t learning anything new.

Because the training data is private, we can’t verify the accuracy of generative AI tools.

Lalli, John. “The Problem with ChatGPT Writing Your Essay.” Seven Pillars Institute. October 19, 2023, https://sevenpillarsinstitute.org/the-problem-with-chatgpt- writing-your-essay/. Accessed February 15, 2025.

The second factor is **ChatGPT operates with private training data**. There is often no way to know exactly the source of the information. When asking ChatGPT to provide sources for information included in the essay it responds, “As an AI language model, I don’t have direct access to my training data or know where it came from.” [12] Since the AI and **thus** the plagiarizing individual **do not know the exact source of the information**, they are not even afforded the opportunity of skimming through these sources for bits of information. In short, using ChatGPT allows for even less effort and time to be put into the assignment and thus for even less educational benefit to be reaped.

More than 50% of the answers given by generative AI, regarding current affairs topics, are inaccurate.

Weaver, Matthew. “AI chatbots distort and mislead when asked about current affairs, BBC finds.” The Guardian, February 10, 2025, https://www.theguardian.com/technology/2025/feb/11/ai-chatbots-distort-and-mislead-when-asked-about-current-affairs-bbc-finds. Accessed February 15, 2025.

Leading artificial intelligence assistants create distortions, factual inaccuracies and misleading content in response to questions about news and current affairs, research has found. **More than half of the AI-generated answers provided by ChatGPT, Copilot, Gemini and Perplexity** were judged to **have “significant issues”,** according to the study by the BBC. The errors included stating that Rishi Sunak was still the prime minister and that Nicola Sturgeon was still Scotland’s first minister; misrepresenting NHS advice about vaping; and mistaking opinions and archive material for up-to-date facts. The researchers asked the four generative AI tools to answer 100 questions using BBC articles as a source. The answers were then rated by BBC journalists who specialise in the relevant subject areas. About a fifth of the answers introduced factual errors on numbers, dates or statements; 13% of quotes sourced to the BBC were either altered or did not exist in the articles cited.

Because of its frequent errors, generative AI threatens to weaken public trust in facts and media.

Weaver, Matthew. "AI chatbots distort and mislead when asked about current affairs, BBC finds." The Guardian, February 10, 20**25**, https://www.theguardian.com/technology/2025/feb/11/ai-chatbots-distort-and-mislead-when-asked-about-current-affairs-bbc-finds. Accessed February 15, 2025.

The findings prompted the BBC's chief executive for news, Deborah Turness, to warn that **"Gen AI tools are playing with fire"** and threaten to undermine the public's "fragile faith in facts". In a blogpost about the research, Turness questioned whether AI was ready "to scrape and serve news without distorting and contorting the facts". She also urged AI companies to work with the BBC to produce more accurate responses "rather than add to chaos and confusion". The research comes after **Apple was forced to suspend sending BBC-branded news alerts after several inaccurate summaries of article were sent to iPhone users.** Apple's errors included falsely telling users that Luigi Mangione – who is accused of killing Brian Thompson, the chief executive of UnitedHealthcare's insurance arm – had shot himself.

accounts on gen AI websites get Hacked and stolen

Graham 23

CLULEY, Graham. 2023. "100,000 Hacked ChatGPT Accounts up for Sale on the Dark Web." Hot for Security. 2023. https://www.bitdefender.com/en-us/blog/hotforsecurity/100-000-hacked-chatgpt-accounts-up-for-sale-on-the-dark-web.

In the 12 months running up to May 2023, **the login credentials of over 100,000 hacked ChatGPT accounts found their way onto dark web marketplaces.** That's the finding of researchers at Group-IB, who discovered the usernames and passwords within the information-stealing malware sold via underground cybercrime forums.The distribution of the AI-powered chatbot account credentials is concerning for a number of reason.Firstly, the rising use of **OpenAI's ChatGPT in the workplace** **raises the risk that confidential and sensitive information will fall into unauthorised hands** as a result of account passwords being distributed.

Furthermore, there is the very real danger that workers will have reused the same password for their ChatGPT account as other online accounts, raising the prospect that **hackers** may be able to use the compromised **detail**s to access other online accounts and potentially **steal other corporate data.** According to the researchers, the logs indicated that most of the breached ChatGPT credentials were scooped up by the Raccoon information-stealing malware.The notorious Raccoon information-stealing malware is used by cybercriminals to steal sensitive data from victim's browsers and cryptocurrency wallets, scooping up saved credit card details, saved login details, and extracting information from cookies.For as little as US $200-per month malicious hackers and fraudsters could purchase access to Raccoon's capabilities. The development of the Raccoon malware was disrupted after Ukrainian national Mark Sokolovsky, its alleged developer, was arrested in the Netherlands at the request of the FBI.The news of the arrest put to the malware-as-a-service group's earlier claim that their key developer had been killed in the early days of Russia's invasion of Ukraine.Although at the time of Sokolovsky's arrest the infrastructure for Raccoon was also dismantled, new versions of Raccoon have been released since - at an increased price of US $275 per month.It is estimated that **approximately one million people had fallen victim** to Raccoon by the end of 2022, with users most commonly attacked via boobytrapped emails.

And this is leading to the rise of phishing

Jacob Fox, Jacob. "Top 40 AI Cybersecurity Statistics | Cobalt." Cobalt.io, Cobalt, 10 Oct. 20**24**, www.cobalt.io/blog/top-40-ai-cybersecurity-statistics.

The latest AI cybersecurity statistics show an **increase in artificial intelligence to power phishing, ransomware attacks,** crypto-related crime, and other forms of attack. Organizations are already feeling the impact of AI-generated attacks and anticipate the increased prevalence of low-level vulns becoming more common targets for amateur attackers empowered by LLM technology. In response, security teams are turning to AI-powered tools to fight AI with AI. Here's a roundup of some top AI cybersecurity statistics that illustrate current trends and likely future trajectories.

Cost and Frequency of AI Cyberattacks

Security stakeholders rank the highest AI-powered cybersecurity threat categories as malware distribution, vulnerability exploits, sensitive data exposure from generative AI, social engineering, net unknown and zero day threats, and reconnaissance for attack preparation (Darktrace).

74% of IT security professionals report their organizations **are suffering** significant impact from AI-powered threats (Darktrace).75% of cybersecurity professionals had to modify their strategies last year to address AI-generated incidents (Deep Instinct),**97%** of cybersecurity professionals **fear** their organizations will face **AI-generated security incidents** (Deep Instinct)

.**93% of businesses expect to face daily AI attacks** over the next year (Netacea).

87% of IT professionals anticipate AI-generated threats will continue to impact their organizations for years (Darktrace).**The global cost of data breaches averaged $4.88 million over the past year, representing a 10% increase and an all-time high (IBM).**

Organizations most frequently experience social engineering and phishing attacks (reported by 56% of IT professionals), web-based attacks (50%), and credential theft (49%) (Ponemon Institute).

AI Phishing is killing the economy

Jacob Fox 24, Jacob. "Top 40 AI Cybersecurity Statistics | Cobalt." Cobalt.io, Cobalt, 10 Oct. 2024, www.cobalt.io/blog/top-40-ai-cybersecurity-statistics.

40% of all phishing emails targeting businesses are now generated by AI (VIPRE Security Group).

60% of recipients fall victim to AI-generated phishing emails, equivalent to rates for non-AI generated emails (Harvard Business Review).

Spammers save 95% in campaign costs using large language models (LLMs) to generate phishing emails (Harvard Business Review).

Phishing attacks cost an average $4.88 million per breach (IBM).

AI Deepfakes

61% of organizations saw an increase in deepfake attacks over the past year (Deep Instinct).

Deepfake attacks are projected to increase 50% to 60% in 2024, with 140,000 to 150,000 global incidents (VPNRanks).

75% of deepfakes impersonated a CEO or other C-suite executive (Deep Instinct).

Generative AI will multiply losses from deepfakes and other attacks 32% to $40 billion annually by 2027 (Deloitte).

Impersonation scams cost $12.5 billion nationally in losses in 2023 (Federal Bureau of Investigation).

AI Ransomware

48% of security professionals believe AI will power future ransomware attacks (Netacea).

The average ransomware attack costs companies $4,450,000 (IBM).

Ransomware attacks rose 13 times over the first half of 2023 as a percentage of total malware detections (Fortinet).

AI Cryptocrimes

Deepfakes will account for 70% of cryptocrimes by 2026 (Bitget).

Cryptocrime losses totaled $5.6 billion nationally in 2023, accounting for 50% of total reported losses from financial fraud complaints(Federal Bureau of Investigation).

Cryptocurrency losses rose 53% from 2022 to 2023 (Federal Bureau of Investigation).

AI-generated Cybersecurity Risks

60% of IT professionals feel their organizations are not prepared to counter AI-generated threats (Darktrace).
While 79% of IT security executives say they've taken steps to mitigate AI-generated risks, just 54% of hands-on practitioners share their confidence (Darktrace).
41% of organizations still rely on endpoint detection and response (EDR) strategies to stop AI attacks (Deep Instinct). Previous research has found that over half of organizations say EDR solutions are ineffective against new types of threats (Ponemon Institute).
Despite the limitations of EDR, 31% or organizations plan to increase investment in EDR solutions (Deep Instinct).

Rebuttals

Amazon in 2024 [Amazon in 2024, "Amazon invests $110 million to support AI research at universities using Trainium chips", 11/12/2024, US About Amazon, https://www.aboutamazon.com/news/aws/amazon-trainium-investment-university-ai-research, Accessed 03/04/2025]

Amazon is announcing a $110 million investment for university-led research in generative AI. The program, known as **Build on Trainium, will provide compute hours that allow researchers the opportunity to build** new **AI architectures, machine learning (ML) libraries, and performance optimization**s for large-scale distributed AWS Trainium UltraClusters (collections of of AI accelerators that work together on complex computational tasks). AWS Trainium is the ML chip that AWS built for the purposes of deep learning training and inference. AI advances created through the Build on Trainium initiative will be open-sourced, so researchers and developers can continue to advance their innovations. 4 ways AWS is engineering infrastructure to power generative AI From networking innovations to changes in data center design, **AWS continues to optimize its**
infrastructure to support generative AI at scale. The program caters to a wide range of AI research,
from algorithmic advancements to increase AI accelerator performance, all the way up to large distributed systems research. As part of Build on Trainium, AWS created a Trainium research ltraCluster with up to 40,000 Trainium chips, which are optimally designed for the unique workloads and computational structures of AI. As part of Build on Trainium, **AWS andleading AI**
student education. In addition, Amazon will conduct multiple rounds of Amazon Research Awards calls for proposals, with selected proposals receiving AWS Trainium credits, and access to the large Trainium UltraClusters for their research. A boost to computing power Developing frontier **AI models and applications requires a**
lot of computing power, and many universities have had to slow down AI research due to budgetary constraints. A researcher might invent a new model architecture or a new performance optimization technique, but they may not be able to afford the high-performance computing resources required for a large-scale experiment. The Catalyst research group at Carnegie Mellon University (CMU) in Pittsburgh, Pennsylvania, is one of the research institutions participating in Build on Trainium. There, a large group of faculty and students are conducting research on ML systems, including developing new compiler optimizations for AI. "**AWS's Build on Trainium initiative enables our faculty and students large-scale access to modern**
accelerators, like AWS Trainium, with an open programming model. It allows us to greatly expand our research on tensor program compilation, ML parallelization, and language model serving and tuning." said Todd C. Mowry, a professor of computer science at CMU**. Funding to support AI experts of the future Since launching the AWS Inferentia chips in 2019, AWS has been a pioneer in building and scaling AI chips in the cloud.** By opening those capabilities to academics, Build on Trainium will not only help broaden the pool of ideas, but also support the training of future AI experts. What you need to know about the AWS AI chips powering Amazon's partnership with Anthropic Anthropic will use our powerful, purpose-built AI chips to

accelerate generative AI for our customers. "**Trainium is beyond programmable—not only can you run a program, you get low-level access to tune features of the hardware itself," said Christopher Fletcher, an associate professor of computer science research at the University of California at Berkeley, and a participant in Build on Trainium. "The knobs of flexibility built into the architecture at every step make it a dream platform from a research perspective**." These advancements are possible, in part, thanks to a new programming interface for AWS Trainium and Inferentia called the Neuron Kernel Interface (NKI). This interface gives direct access to the chip's instruction-set and allows researchers to build optimized compute kernels (core computational units) for new model operations, performance optimizations, and science innovations. "**AWS is really enabling unexpected innovation**," said Fletcher. "I walk across the lab and every project needs compute cluster resources for something different. The Build on Trainium resources will be immensely useful—from day-to-day work, to the deep research we do in the lab." Additional resources for grant recipients As part of the Build on Trainium program, researchers will be able to connect with others within the field to bring ideas to life. Grant recipients have access to AWS's extended technical education and enablement programs for Trainium. This is done in partnership with the growing Neuron Data Science community, a virtual organization led by Amazon's chip developer Annapurna, which bridges the AWS Technical Field Community (TFC), specialist teams, startups, AWS's Generative AI Innovation Center, and more. Your guide to free and low-cost AWS courses that can help you use generative AI More than 100 AWS trainings on AI/ML are available to everyone, with all levels of experience. AI advancements are moving quickly because developers anywhere in the world are able to access and deploy the software. **Researchers involved in Build on Trainium will publish papers on their work and will be asked to bring the code into the public sphere via open-source machine learning software libraries.** This collaborative **research will become the foundation for the next round of advancements in AI.**

Critical Thinking

Gen AI disrupts the processes that build critical thinking

Jared Cooney **Horvath**,[Jared Cooney Horvath PhD, MEd is a neuroscientist and educator with expertise in human learning, memory, and brain stimulation. Jared serves as director of the Science of Learning Group and NeuroEducation: two teams dedicated to bringing the latest in brain research to education and business.] 7-16-20**24**, "The Limits of GenAI Educators", Harvard Business Review, https://hbr.org/2024/07/the-limits-of-genai-educators

University College London Professor Rose Luckin recently argued that, since ChatGPT can access and organize all the world's knowledge, learners need no longer waste time learning "facts." Instead, they can focus on higher-order thinking skills like creative and critical thinking. Unfortunately, **much of what we term "creative" and "critical" thinking occurs via subconscious processes that rely on internalized knowledge.** When we consciously think about a problem, humans can only actively consider a very finite amount of information due to the cognitive limits of working memory. However, **once we stop consciously thinking about a problem, we enter into an incubation period whereby our brains subconsciously sort through our memory stores by seeking out relevant ideas. It's during this sorting process (known as reconsolidation) that novel connections are made and better thinking emerges**. "Even among highly skilled *human* educators, failure to cultivate an empathetic relationship inevitably hinders learning." Here's the problem: **Subconscious reconsolidation** only works with information that is stored within a person's long-term memory, which means **it cannot leverage information that is externally accessed or stored**. This explains why experts almost always demonstrate stronger problem-solving skills than novices within their field of expertise, but rarely outside of it. This also explains why semantic dementia (whereby patients lose long-term memories but maintain cognitive faculties) impairs creativity nearly twice as much as frontotemporal dementia (whereby patients lose cognitive faculties but maintain long-term memory stores). **Simply put, using AI to help learners avoid the tedious process of memorizing facts is the best way to ensure higher-order thinking skills will never emerge.** But, you may be asking, what about learners who use AI to merely assist with fact memorization? Well, consider that **textbooks have historically been written by experts—people with enough deep knowledge to aptly vet**

and organize information into a meaningfully structured curricula. Large language models (at least in their current form) have neither oversight nor vetting. This means learners who use AI are very likely to encounter wrong, oddly sequenced, or irrelevant information which—if memorized—might very well derail their path to mastery. Of course, AI models will improve and information will surely increase in accuracy. Unfortunately, this won't address the issue of vetting. Just as with Wikipedia today, users will only ever be able to work up to their current level of knowledge: Anything beyond that must be taken on faith. When **learning** relies on faith, it's imperative that faith is placed where the likelihood of success is highest; this is why having the assurance that an expert has evaluated and organized key information remains invaluable.

Studies prove the devastating effects.

Knapp in 25 shows (Alex Knapp is a Forbes senior editor covering healthcare and science since 2011., "The Prototype: Study Suggests AI Tools Decrease Critical Thinking Skills", Forbes, https://www.forbes.com/sites/alexknapp/2025/01/10/the-prototype-study-suggests-ai-tools-decrease-critical-thinking-skills/, 1-10-2025, DOA: 2-20-2025)

New AI tools are slowly becoming ubiquitous, being added to the software and hardware we use every day (sometimes whether we like it or not). But if we're using artificial intelligence to perform tasks, search for information and solve problems, what does that mean for the intelligence we're born with? To figure this out, a team of researchers conducted a study involving 666 individuals ages 17 and up, representing a diverse population. It first evaluated the extent to which each of them made use of AI tools, then tested their critical thinking skills. The results of the study, which were published in the journal Societies, found that those who used AI tools a lot showed worse critical thinking abilities than those who didn't use them often or at all. Whether someone used AI tools was a **bigger predictor** of a person's thinking skills than any other factor, including educational attainment. The reason for this is a phenomenon called "cognitive offloading" – where people's thinking and problem-solving are essentially delegated. Frequent cognitive offloading reduces a person's ability to independently think and solve problems. "This relationship underscores the dual-edged nature of AI technology," the study authors wrote. "While it enhances efficiency and convenience, it inadvertently fosters dependence, which can compromise critical thinking skills over time." These findings are consistent with other studies that have shown a similar negative impact from AI tools on critical thinking skills. The authors note, however, that other studies show AI tools can be beneficial when they complement critical thinking, rather than offloading it. "Future research should explore strategies to integrate AI tools in ways that enhance rather than hinder cognitive engagement," they wrote. "Ensuring that the next generation is equipped with the skills necessary to navigate an increasingly complex digital landscape." Stay tuned.

Here's an example

Idaho capitol sun 25

https://idahocapitalsun.com/2025/01/12/school-software-provider-is-the-latest-target-of-major-hack-of-personal-data/

The sensitive data of millions of American adults and children have been compromised after hackers targeted California-based education software company PowerSchool, the company confirmed last week.

The breach happened at the end of December, and new information confirmed by TechCrunch Thursday morning says that hackers were able to access student addresses, Social Security numbers, grades and medical information on the platform, which schools use for student records, grades, attendance and enrollment.