

DIGITAL COMPASS

Your Go-To Resource for Navigating the Ever-Changing World of Technology



AI & INNOVATION

The driving force behind emerging
technologies in the field

Page 2

How Generative AI
is Filling the Gaps
in Healthcare

Page 22

AI Implementation
for Executives: A
Step-by-Step Guide

Page 8

Editor's Note

Stratascale is passionate about bringing emerging technology and industry insights to our clients and partners. And there is no greater emerging tech right now than AI.

AI may be the most impactful emerging technology we have seen in decades; a technology that currently has no bounds and possibilities that are limitless. For good or bad, it will transform how we live, work, and interact with one another. AI will start to influence our day to day lives, just like the internet revolution of the 1990s (Napster, anyone?).

Positive changes like advances in healthcare, environmental sustainability, education, economic growth, and innovation can already be seen (in early stages) due to the use of AI. Creating more efficient and effective processes, enabling earlier disease detection and personalized treatment plans, and bringing students more tailored approaches to individual learning are all leading to growth in multiple areas. Of course, with these advancements also come questions about ethics, potential for data bias, and concerns about ever-increasing cybersecurity threats.

As we navigate this evolving landscape, our team aims to provide diverse perspectives and insights into the world of AI. We invite you to read our articles, explore AI, and join us in shaping the future through innovation. And if you find an article that resonates with your current area of interest, please reach out to the author to connect. We love technology and want to hear from others who are interested in staying ahead of the curve.



KENDRA PERRY

Manager of Emerging
Technology

CONTENTS

Note from the Editor

Pg. 2 | Kendra Perry

AI and Innovation

Pg. 4-7 | Kendra Perry

AI Implementation for Executives: A Step-by-Step Guide

Pg. 8-13 | Chris Hudson

AI as a Scapegoat? Exploring the Legalities Surrounding AI Chatbots

Pg. 14-19 | Alex Banghart

Emerging Tech Corner

Pg. 20-21 | Deep Instinct

How Generative AI is Filling the Gaps in Healthcare

Pg. 22-25 | Mary-Kate Sloper

Is AI Friend or Foe for Companies Pursuing Environmental Sustainability Goals?

Pg. 26-30 | Aaron Soto

About

Pg. 31



4



8



14



AI & Innovation



Kendra Perry
Manager of Emerging Technology
kendra_perry@stratascale.com

Artificial Intelligence (AI) is a driving force behind emerging technology across multiple areas in the field, including cybersecurity, Large Language Models (LLM) training, and data management. Not only do AI innovations enhance the capabilities and efficiencies of technologies in these areas but introduce new methodologies and approaches for solving complex problems.

For instance, in cybersecurity, AI is paving the way for autonomous security systems that can adapt to new threats in real-time. In LLM training, AI is enabling the creation of models that can understand and generate human-like text, opening new avenues for human-computer interaction. And in data management, AI-driven solutions are making it possible to harness the power of big data for predictive analytics, personalized services, and more efficient operations.

Across these functional areas, AI is fueling innovation at record pace.

01

AI in Cybersecurity

While AI has offered new ways to help traditional security become more efficient, effective, and productive, it has introduced new threat vectors. AI is driving increased efficiency and effectiveness among threat actors in activities like reconnaissance, phishing, and coding.



Enhanced capabilities in reconnaissance, the practice of gathering information and intelligence about potential targets through automated processes, enabling threat actors to identify vulnerabilities more effectively.



Threat actors are empowered to execute more sophisticated phishing attacks, enabling them to craft highly convincing and targeted messages to deceive individuals and organizations increasing the success rate of malicious campaigns.



Coding practices are being revolutionized through AI. More complex and evasive malware, exploit kits, and other malicious tools are being developed with greater speed and efficiency.

While there are certainly obstacles to overcome we believe that the opportunities outweigh them.



Not only is AI helping to combat cybersecurity threats, but its also addressing issues that have plagued the industry like:

Improving detection and response speed through rapid data analysis.

Threat intelligence and analysis can be based on patterns to detect emerging threats while reducing noise and employee burnout. AI-powered analytics can distinguish between legitimate and malicious activities more accurately, reducing false positives and improving the overall efficiency of security operations.

Identifying insider threats by analyzing user behavior and detecting anomalous activities that suggest insider threats.

Mitigating breaches faster through AI automation streamlining workflows by identifying, prioritizing, and containing security incidents.

By addressing these legacy issues, AI is revolutionizing cybersecurity practices, enabling organizations to better defend against increasingly sophisticated and diverse cyber threats.

AI is instrumental in enhancing threat detection and response. AI algorithms, particularly those based on machine learning, can analyze vast amounts of data to identify patterns and anomalies that may indicate a cyber threat. For example, AI can be used to develop predictive models that anticipate attack strategies and vulnerabilities before they are exploited. This helps reduce noise, so teams have fewer false flags to follow up on resulting in less burnout and more efficiency in tracking real threats.

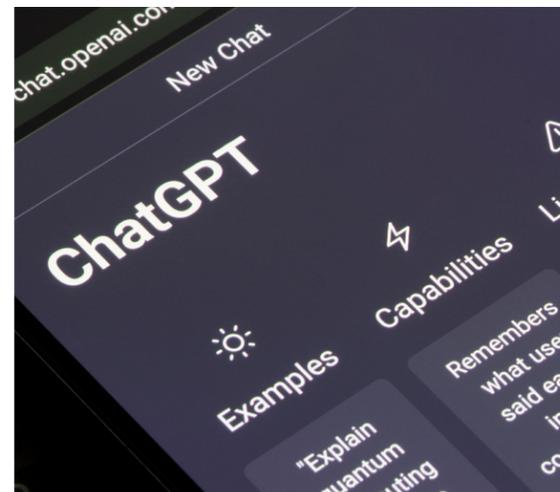
Additionally, AI-driven security systems can automate the response to detected threats, enabling faster mitigation, and reducing the workload on human security analysts.

02

AI in LLM Training

AI is also revolutionizing the field of natural language processing (NLP) through the development and training of Large Language Models like GPT (Generative Pre-trained Transformer). These models are trained on extensive datasets, allowing them to generate coherent, contextually relevant text based on the input they receive.

The training of LLMs leverages advanced AI techniques, including deep learning and reinforcement learning, to improve their understanding of language nuances and generate more accurate responses. This has broad applications, from enhancing conversational AI and content creation to improving language translation services.



03

AI in Data Management

In data management, AI technologies are facilitating more efficient ways to store, process, and analyze data. AI algorithms can automatically classify and organize data, making it easier to access and use.

AI-driven analytics tools can sift through large datasets to uncover insights and patterns that would be difficult or impossible for humans to find on their own. This capability is crucial for making data-driven decisions in business, research, and public policy.

AI is also being used to improve data quality and integrity by detecting and correcting errors or inconsistencies in data sets.



04

Cross-Sectoral Innovations

Across these areas, AI promotes innovation through automation, enhanced accuracy, and the ability to process and analyze data at scale. This leads to more robust cybersecurity defenses, more nuanced and sophisticated language models, and more effective data management strategies. The integration of AI into these domains encourages the development of new tools and technologies, further accelerating the pace of innovation.



Innovation in cybersecurity, LLM training, and data management is multifaceted, driving both the improvement of existing technologies and the creation of new methodologies and tools. These advancements not only enhance the capabilities within each field but also have the potential to transform industries and societies by enabling smarter, more efficient, and more secure technological ecosystems.

For more on the legal ramifications on AI, flip to page 14: "AI as a Scapegoat? Exploring the Legalities Surrounding AI Chatbots".



AI Implementation for Executives

A Step-by-Step Guide



Chris Hudson
Manager of Technical Advisory
chris_hudson@stratascale.com

Unlocking the transformative power of artificial intelligence (AI) for your business can be a thrilling journey, especially for large organizations. While strategic preparation, diligent execution, and ongoing assessment are crucial, these steps empower leaders to become pioneers in AI adoption.

With a practical framework, you will be well-equipped to leverage AI's potential to drive significant business growth and innovation, all while navigating ethical considerations and emerging challenges.

Whether you are just starting your AI journey or are seeking to scale efforts, this guide will help remove the mystery around AI integration by offering practical guidance on overcoming obstacles, embracing best practices, and applying solutions.

Charting the Course

Ready to take action? Here are four key steps that will equip you to propel your AI journey forward:

01

Articulate

your AI vision and objectives by engaging key stakeholders to identify specific challenges and opportunities where AI can significantly impact and formulate SMART—specific, measurable, achievable, relevant, and time-bound goals and align with identified opportunities.

02

Benchmark

your AI capabilities by evaluating the quality, relevance, accessibility, and security of your data and analyzing your current systems' capacity, scalability, interoperability, and resilience. This will help you gain a clear understanding of your organization's readiness for AI integration. Additionally, it will help you identify areas that may benefit from additional development or investment and strengths to capitalize on.

03

Blueprint

your AI solution and roadmap by creating a clear strategic direction and actionable steps for your AI journey. This involves defining the problem or opportunity you want to address with AI and selecting the most appropriate AI technique based on the particular use case and anticipated outcome. This will improve coordination, decision-making, and execution.

04

Implementation

of your AI solution necessitates several steps. Ensure your data is accurate, reliable, and representative of the target domain. Once your data is prepared, the next step is to select the appropriate tools, platforms, and algorithms that align with your chosen AI technique. After developing the AI model or app, conduct a comprehensive testing phase to verify the solution's functionality and adherence to ethical standards. Once the validated AI solution is deployed into production, ensure it integrates smoothly with your existing systems and processes using full system observability.

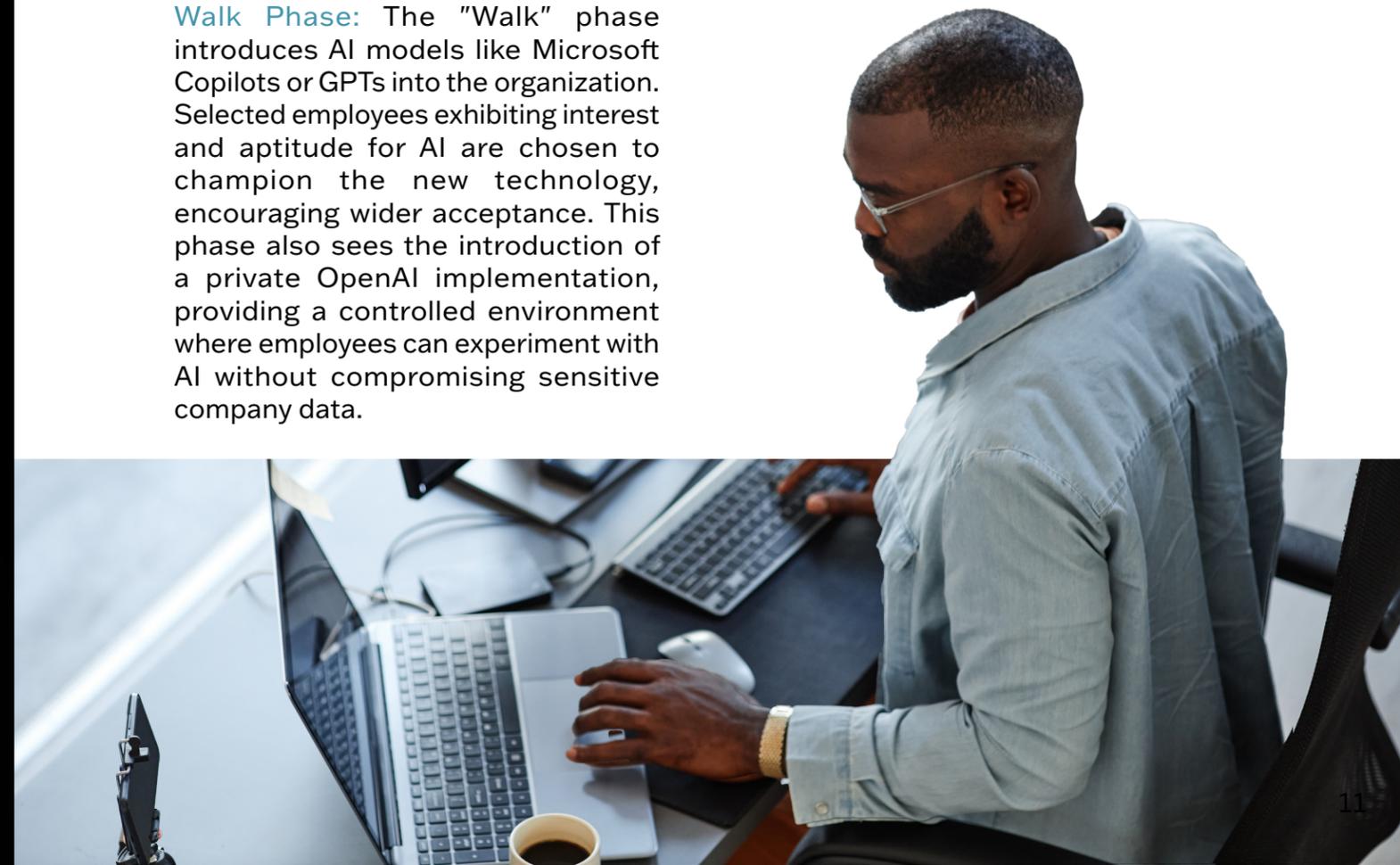
Implementing for Success

The journey to AI success takes time to happen. Many organizations benefit from a phased approach called "Crawl, Walk, Run". This structured framework allows companies to build a strong foundation, gain experience, and gradually scale their AI initiatives. Let us delve into each stage and see how it contributes to a thriving AI ecosystem within your organization.

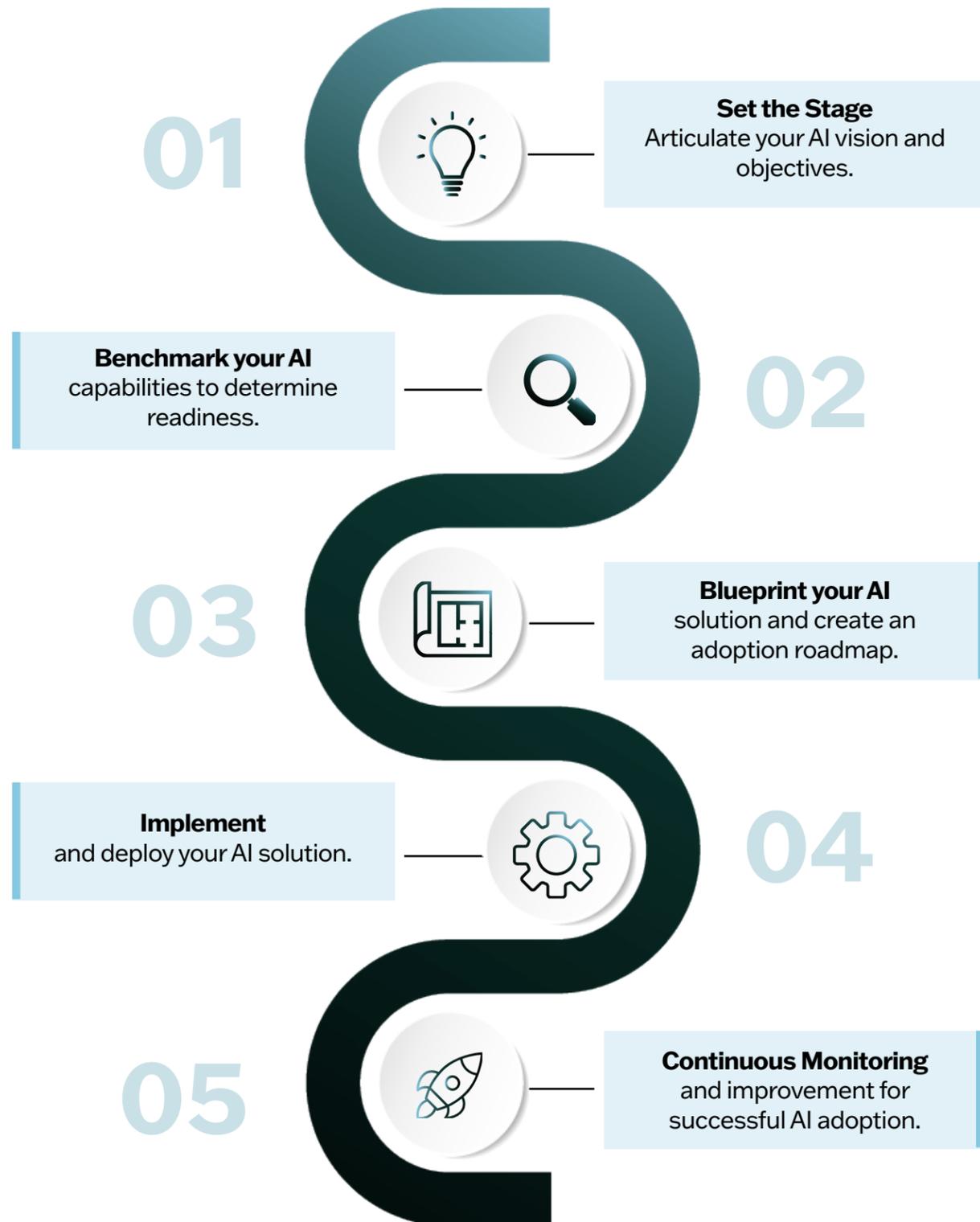
Crawl Phase: The initial phase, known as the "Crawl" phase, focuses on knowledge acquisition and employee upskilling. Enterprises build a common language around AI during this stage to ensure a smooth transition. The use of prompts helps teach AI and understand its capabilities. Central to this phase is establishing an AI Center of Excellence (CoE), which serves as a hub for understanding AI, strategizing its implementation, setting security measures, and ensuring data privacy best practices.

Run Phase: The "Run" phase is the maturity stage of AI implementation, where AI becomes integrated into tools, platforms, and processes. Enterprises must consider when to expose their data to the public while understanding and countering new security threats that arise with AI. This phase also demands attention to privacy and bias concerns, necessitating strategies to address these issues and reassure stakeholders about AI's benefits and safety measures.

Walk Phase: The "Walk" phase introduces AI models like Microsoft Copilots or GPTs into the organization. Selected employees exhibiting interest and aptitude for AI are chosen to champion the new technology, encouraging wider acceptance. This phase also sees the introduction of a private OpenAI implementation, providing a controlled environment where employees can experiment with AI without compromising sensitive company data.



Five Steps to Implementing AI



FAQs

What should be considered when formulating my organization's AI vision and objectives?

When formulating the AI vision and objectives, it is important to engage key stakeholders to identify specific challenges and opportunities where AI can have a significant impact. The objectives should be SMART - Specific, Measurable, Achievable, Relevant, and Time-bound - and align with these identified opportunities.

How can I assess my organization's readiness for AI integration, and what steps can be taken to improve this readiness?

Assessing your organization's readiness for AI integration involves evaluating the quality, relevance, accessibility, and security of your data and analyzing your current systems' capacity, scalability, interoperability, and resilience. If gaps are identified, consider additional development or investment in those areas. Also, consider upskilling your workforce and establishing strong data management practices.

What specific challenges might my organization face during the 'Run' phase of AI implementation, and how can these be addressed?

During the 'Run' phase, challenges might include deciding when and how to expose your data to the public, understanding and countering new security threats arising with AI, and addressing privacy and bias concerns. To overcome these, you can implement stringent data security measures, stay updated on evolving security threats, and establish clear strategies and ethical guidelines for AI usage.

AI will continue to be a force to be reckoned with, but our goal is to make your AI journey less arduous. We'll happily be your first mate if you're ready to set sail.

[Learn More](#)

AI as a Scapegoat?

Exploring the Legalities Surrounding AI Chatbots



Alex Banghart
Research Analyst
alex_banghart@stratascale.com

AI chatbots, such as ChatGPT, have revolutionized interaction by generating human-like responses that make conversations more engaging and [natural](#). Their application extends across various domains, notably in the legal sector where they are transforming practices by enhancing legal research, streamlining document drafting, and even assisting in [predictive analysis](#). However, the legal recognition of AI chatbots remains ambiguous, leading to complexities in assigning rights and responsibilities, particularly as they operate in spheres with stringent data protection regulations like [GDPR](#).

As AI chatbots continue to permeate the legal field, it becomes crucial for businesses to navigate the myriad of legalities surrounding [their use](#). This includes ensuring compliance with data protection laws, being transparent about data collection processes to gain explicit user consent, and addressing intellectual property issues stemming from content generated by [AI chatbots](#). The introduction of AI chat, powered by large language models, into the legal sector not only poses challenges in terms of liability and regulatory compliance but also necessitates a thorough examination of their potential to inadvertently reinforce [discriminatory practices](#).

Case Study: Air Canada's Chatbot Controversy

In the notable case of *Moffatt v. Air Canada*, the Civil Resolution Tribunal of British Columbia, Canada, highlighted significant legal considerations surrounding AI chatbots. This case serves as a pivotal example of the legal challenges and responsibilities companies face when deploying AI technologies like chatbots.

Liability and Duty of Care:

Air Canada was found liable for negligent misrepresentation by its chatbot regarding bereavement fares, demonstrating that companies owe a duty of care to ensure the accuracy of information provided by their [AI systems](#).

The tribunal rejected Air Canada's defense that it could not be held accountable for the chatbot's misinformation, underscoring that businesses are responsible for all information dispensed through their digital platforms, including [AI-powered tools](#).

Consumer Rights and Compensation:

The tribunal's decision to order Air Canada to compensate the customer, Jake Moffatt, with CA\$650 in damages, plus additional costs, marks a significant moment for [digital consumer rights](#).

This ruling emphasizes the accountability of companies for the performance and accuracy of their AI chatbots, setting a precedent for how similar cases might be adjudicated in [the future](#).

Operational Adjustments and Precautions

Following the tribunal's decision, Air Canada's response included disabling the chatbot in question, indicating a move towards addressing the identified issues. This case underscores the importance of companies maintaining rigorous oversight of their AI tools to prevent misleading information and ensure compliance with [legal standards](#).

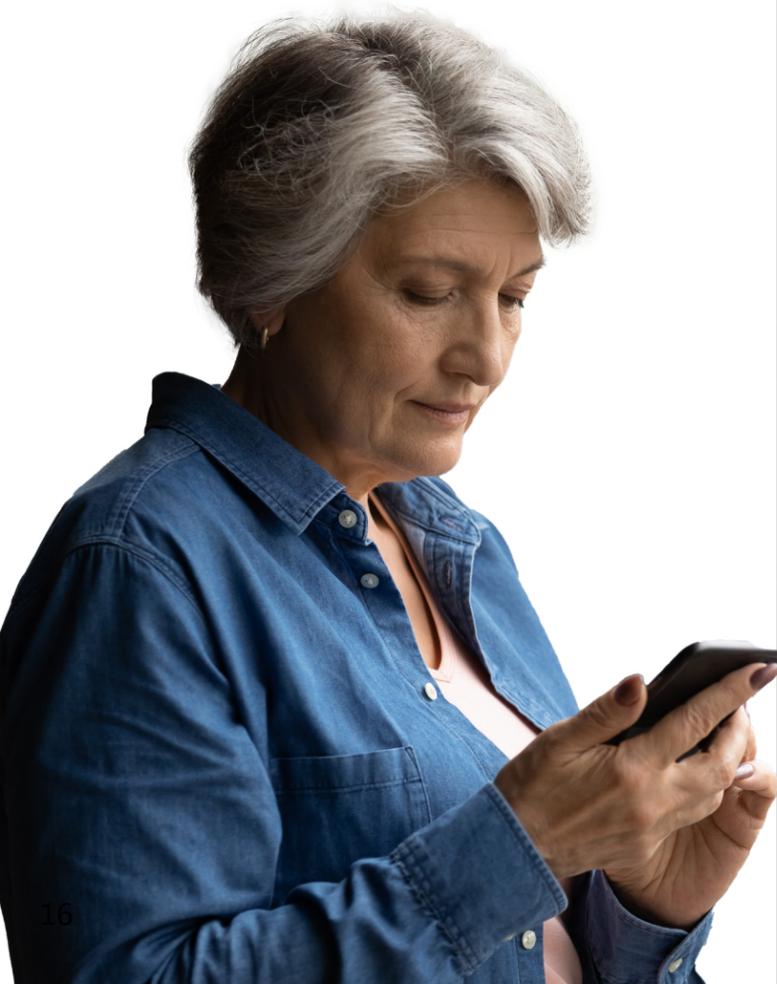
This case study not only sheds light on the legal risks and responsibilities associated with AI chatbots but also signals a broader shift towards increased accountability and scrutiny of AI technologies in customer-facing roles.



Section 230 & Its Implications for AI Chatbots

Section 230 of the Communications Decency Act, a pivotal piece of internet legislation, provides immunity to platforms from liability for user-generated content. However, this protection does not extend to AI chatbots, which can generate original content and, in some cases, falsehoods. This legal gap poses significant challenges, as demonstrated by incidents such as ChatGPT generating false accusations against [individuals](#).

Key Considerations Under Section 230:



AI-generated Content: Unlike user-generated content, AI chatbots like ChatGPT and Stable Diffusion generate their own responses, leading to potential legal and ethical dilemmas, including the spread of misinformation or [generating defamatory content](#).



Legal and Ethical Challenges: Developers and companies must navigate existing laws that could penalize them for harm caused by their technologies. This is crucial as the legal framework requires reevaluation in the context of [AI-generated content](#).



Future Legal Landscape: The Supreme Court's decisions on related cases and testimonies from industry leaders, such as Sam Altman of OpenAI, indicate ongoing debates and a bipartisan interest in regulating AI technologies. This setting stages for future regulation that could significantly impact AI companies, especially if Section 230 protections are limited or redefined in the [context of AI](#).

Legal experts and lawmakers are exploring ways to address these challenges without stifling innovation. The readings of Section 230 by its co-authors and Supreme Court cases like Gonzalez v. Google could influence future legal interpretations and regulations concerning AI-generated content. Without Section 230 protection, companies could face a surge of lawsuits, highlighting the need for clear guidelines and regulations for AI chatbots and their [generated content](#).

Legal Risks & Responsibilities

The legal landscape surrounding AI chatbots is intricate, with several areas of concern that stakeholders must navigate carefully to avoid potential legal pitfalls. These concerns are primarily centered around the accuracy and legality of the content generated, the protection of personal data, and the adherence to regulatory standards. Below are the key legal risks and responsibilities associated with AI chatbots:

01

Regulatory Compliance and Ethical Considerations:

AI-generated content must adhere to existing laws, including data protection regulations like GDPR, which mandates transparency and user control over [personal data](#).

The unauthorized practice of law through AI chatbots raises significant regulatory and ethical issues, necessitating strict [compliance measures](#).

02

Intellectual Property and Liability Concerns:

The potential for AI chatbots to infringe on intellectual property rights, especially when generating original content, underscores the need for careful consideration of [copyright laws](#).

Developers, operators, and users of AI chatbots may face liability for damages or harm caused by inaccuracies or misleading information provided by these [technologies](#).

03

Privacy, Security, and Transparency:

Ensuring user privacy and data security is paramount, with laws in the US and Europe imposing restrictions on the sharing of [personal information](#).

Transparency about the nature of interactions with AI chatbots is crucial to maintaining consumer trust and compliance with federal and [state laws](#).

By understanding and addressing these legal risks and responsibilities, stakeholders can mitigate potential issues and leverage AI chatbots effectively within the legal framework.



Current Legal Standings & Future Directions

In light of the evolving horizon of AI, AI chatbots are set to navigate through a series of regulatory frameworks and policy developments that will significantly influence their design, deployment, and operation. Key forthcoming legal considerations include:

01 EU's AI Act:

Risk-Based Regulation: The Act categorizes AI systems by their inherent risk, imposing stringent requirements on foundational models that [power AI chatbots](#).

Impact on AI Chatbots: Directly affects the development and application of AI chatbots, particularly those operating within the EU, necessitating compliance with [new regulatory standards](#).

02 White House AI Executive Order:

Reporting Requirements: Mandates affirmative reporting from developers of foundational models on various aspects, including safety, security, and [impact assessments](#).

Standards and Guidelines: Aims to establish consistent AI standards and guidelines across federal agencies, influencing the broader [AI chatbot ecosystem](#).

03 FTC's Enforcement Focus:

Streamlined Investigation Process: Enhancements to the FTC's ability to issue civil investigative demands (CIDs) will expedite inquiries into AI-related issues, including those involving [AI chatbots](#).

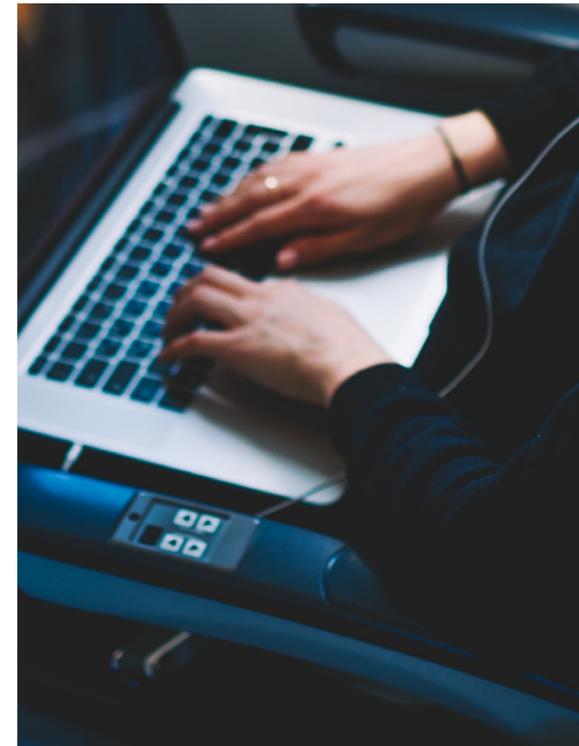
Implications for AI Chatbots: Signals an increased scrutiny on AI chatbots, especially in areas concerning consumer protection and [data privacy](#).

These regulatory shifts underscore a broader movement towards ensuring that AI chatbots, as integral components of our digital lives, operate within frameworks that prioritize user safety, privacy, and ethical considerations. As such, stakeholders in the AI chatbot domain must remain vigilant, adapting to these changes to harness the benefits of AI responsibly and [sustainably](#).

There is a complex interplay between AI chatbots, like ChatGPT, and the legal field, highlighting both the transformative potential and the multifaceted legal challenges they bring. From enhancing legal research and service accessibility to stirring significant debates around liability, data protection, and ethical implications, AI chatbots stand at the crossroads of legal innovation and regulatory scrutiny. The case study of Air Canada and the analysis of current legal frameworks, including Section 230 and forthcoming regulations like the EU's AI Act, encapsulate the critical need for a balance between leveraging AI's capabilities and safeguarding against potential pitfalls.

As the regulatory situation continues to evolve, stakeholders—from developers to legal practitioners—must stay informed and engaged, ensuring that the advancement of AI chatbots

aligns with ethical standards and regulatory requirements. The journey of AI chatbots in the legal domain is just beginning, marked by exciting opportunities and critical challenges. Embracing this dual nature, we must collectively navigate toward a future where AI enhances legal processes without compromising on the core values of justice and equity.



For those looking to delve further into how AI is reshaping the legal industry, engaging resources like OpenAI's insights can offer valuable perspectives and guidance.

FAQs

Is there a chatbot designed for legal assistance?

LawDroid Copilot is a specialized AI chatbot created to assist law firms. It offers a range of services including automating document processes, conducting legal research, and generating ideas, thereby enhancing efficiency and scalability within legal practices.

What should users know about the legal considerations of using ChatGPT?

Users of ChatGPT by OpenAI are permitted to reproduce text generated during interactions according to the terms of use. However, the publication of such generated content could potentially lead to legal issues like copyright infringement. It's advisable to treat ChatGPT's outputs as inspiration rather than verbatim content for publication.

Is ChatGPT capable of offering legal counsel?

ChatGPT lacks the necessary legal expertise, ethical judgment, and adaptability required for legal representation in court. Despite its capabilities, it falls short in several areas crucial for legal advice, such as case building and providing professional legal counsel, underscoring the irreplaceable value of human lawyers.

Are there any restrictions on using chatbots for professional tasks?

When incorporating generative AI chatbots into workplace tasks, it's generally permissible. However, specific guidelines must be followed, such as the prohibition of using company email addresses, credentials, or phone numbers for creating accounts with these technologies. Additionally, it's crucial to ensure that no proprietary or sensitive company information is input into these platforms.

deep instinct

Stratascale is proud to partner with Deep Instinct to enhance ransomware and malware prevention solutions. Together, we're taking an offensive, prevention-first approach to cybersecurity.

Critical Capabilities



Focused on the Most Advanced Aspects of AI by Leveraging Deep Learning



Prevent Ransomware Through Deep Learning



Preventative Protection



Can Identify Novel Threats



Deep Learning Architecture



Robust Integrations to Enhance Security Technology Stack



Endpoint, Application, & Storage

Business Strategy

- Business Continuity
- Availability
- Operational Resiliency
- GRC
- Cost vs Value
- Positive User Experience
- Data Protection

Technology Strategy

- Frictionless
- Risk Management & Mitigation
- Integrates into Existing Technologies
- Ransomware Protection
- Business Information Security
- Compliance

Strategic Focus Areas

- Detection & Response
- Containment
- Policy Enforcement
- Endpoint Visibility
- Threat Intelligence Integration
- Centralized Management
- Real-Time Monitoring

Differentiators

- Scan attachments at application level
- Data center footprint reduction for storage and scanning
- >99% Threat accuracy
- Defender integration for better security
- Predictive prevention

How Generative AI is Filling the Gaps in Healthcare



Mary-Kate Sloper
Research Analyst
marykate_sloper@stratascale.com

Every industry is seeking out ways to improve efficiency and reduce overhead, and healthcare is no exception.

Staffing shortages are pervasive—not only is there a [nursing shortage crisis](#) with 610,388 nurses projected to leave the field by 2027, but there is also a [serious physician shortage](#) of up to 48,000 primary care physicians and 77,100 non-primary care physicians by 2034. With talk of staffing shortages in nearly every role in the healthcare sector, GenAI (generative artificial intelligence) is one way to do more with less staff.



Specific AAMC projections by 2034 include shortages of:

17,800 and 48,000
primary care physicians

21,000 and 77,100
non-primary care physicians

This includes shortages of:

15,800 and 30,200
Surgical specialties

3,800 and 13,400
medical specialties

10,300 and 35,600
other specialties

Uses Cases

01 Patient Hand-Offs

are the transfer of responsibility for a patient (between units, shift change, etc.) from one healthcare provider to another. This process involves handoff reports, which communicate vital patient information such as history and the patient's care plan. GenAI can be used to create handoff reports, which is usually a time-consuming part of the patient handoff process. HCA Healthcare [announced](#) their "CT&I team built a system using one of Google Cloud's large language models (LLMs) that helps automatically generate handoff reports and is designed to promote continuity, consistency, patient safety, and clinical quality - while saving nurses significant time and maintaining human oversight."

ambient clinical documentation. This will cut back on the manual heavy lifting in billing processes such as medical coding, and fill gaps in clinical evidence to enable better patient outcomes.

02 Patient Interactions and Preventative Care

Generative AI is also being used to directly communicate with patients to answer questions that physicians might typically answer.

In [one study](#) conducted by NYU Langone Health, the team implemented ChatGPT to aid in the design of software that generates text messages to educate patients about diabetes prevention. "In the current study, eleven evaluators in fields ranging from medicine to computer science successfully used ChatGPT to produce a version of the diabetes tool over 40 hours, where an original, non-AI-enabled effort had required more than 200 programmer hours."

The University of California San Diego's Health system was among the first to participate in a [pilot program](#) between Microsoft and Epic. In this program, ChatGPT-4 generates "a draft response [to patients] based on the initial message and the patient's electronic medical history, which the provider can then edit for content and tone before sending."

03 Ambient Notetaking

Ambient notetaking is becoming increasingly prevalent, and GenAI can act as a virtual assistant in healthcare settings. Forbes [explains](#), "Think Amazon's Alexa, but in your doctor's office. An early use case is ambient AI scribing: it listens, then writes a clinical note summarizing your visit."

Microsoft [announced](#) its collaboration with electronic health record (EHR) provider Epic, which is using generative AI to enhance clinician productivity with note summarization and embedded

Human Oversight is Key

At the end of the day, healthcare staff members are responsible for their patients, not GenAI. Humans must remain in the loop and have visibility over handoff reports, visit notes, and messages for and about patients.

The UC San Diego announcement [quotes](#) Dr. Christopher A. Longhurst, Chief Medical Officer and Chief Digital Officer at UC San Diego Health:

“Employing this ‘human-in-the-loop’ approach is critical, particularly in a high-risk environment like the health care setting—and considering that GPT has the potential to generate inaccurate responses.”

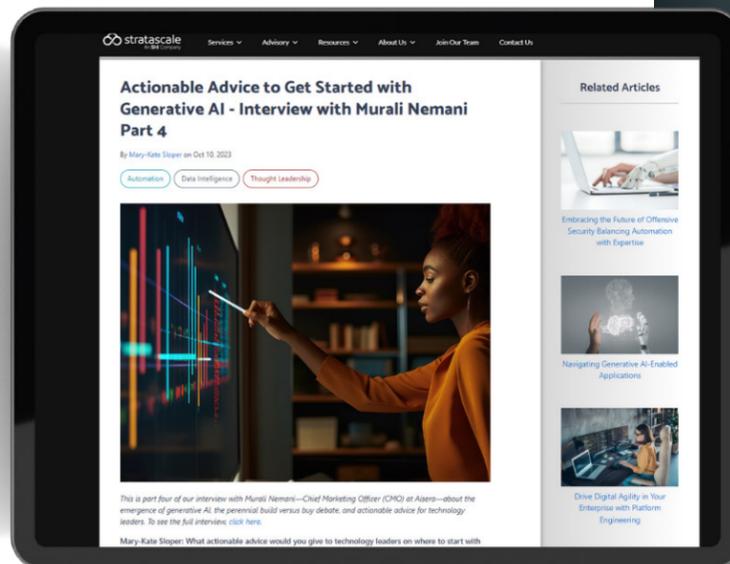
Security Cannot Be Overlooked

Patient data is sensitive and subject to stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). Therefore, robust security measures need to be in place to prevent unauthorized access, data breaches, or misuse of information. Cybersecurity threats pose a significant

risk, requiring advanced encryption and secure communication channels. Additionally, the AI systems themselves must be designed to make accurate and reliable decisions, with protection mechanisms against adversarial attacks that aim to manipulate their output.

In summary, while GenAI shows promise in helping fill the gaps caused by labor shortages in healthcare, extra precautions are necessary in a field where miscommunications can deeply impact the wellbeing of a patient. Human oversight and security must be prioritized for GenAI to be safely and effectively implemented in healthcare.

Explore our actionable insights for leveraging GenAI responsibly and prioritizing human oversight - click the iPad below.



Is AI Friend or Foe for Companies Pursuing Environmental Sustainability Goals?



Aaron Soto
Principal Solution Architect
aaron_soto@stratascale.com

Last year was the hottest year on record, causing the most extreme billion-dollar weather events by a wide margin, with estimated [2023 U.S. damages of at least](#)

\$92.9 billion
and at least
482 lives lost

These events highlight the growing pressure on organizations from investors, employees, and customers to do better for the planet. These expectations are also underscored by new regulations, too.

On March 6, 2024, the U.S. Securities and Exchange Commission (SEC) published its ruling for Climate-Related Disclosures that will affect an estimated [2,800 public companies](#). California passed two climate-related bills in October 2023 that will affect an estimated [5,300 public and private companies](#). Finally, the European Union's Corporate Sustainability Reporting Directive (CSRD) went into effect this year and impacts an [estimated 3,000 U.S. companies](#).

Navigating the transitional risks of these new regulations and adapting to a rapidly changing lower-carbon world while dealing with physical climate risks that are disrupting supply chains, reducing productivity, and leading to direct financial loss is no easy feat.

This leaves many asking, do power-hungry AI, and even hungrier new generative AI (GenAI), systems help, or hurt?

The Environmental Cost/ Benefit Analysis of AI

Technology has been long positioned as a force multiplier that helps humans save time, increase output, or improve our lives. Well-built, human-centered technology actually does that and there is data to back it up.

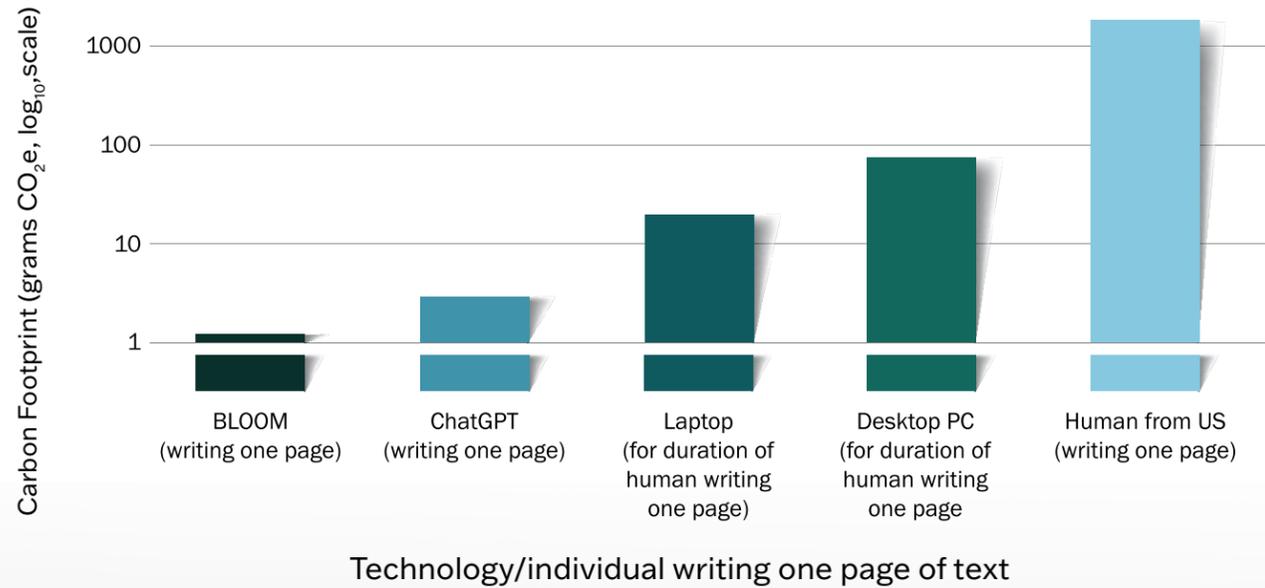
Despite the rising use of Information and Communications Technology (ICT) stemming from the past two decades of digital transformation, research suggests these technologies can lead up to a:

15% [net reduction in global carbon emissions pollution.](#)

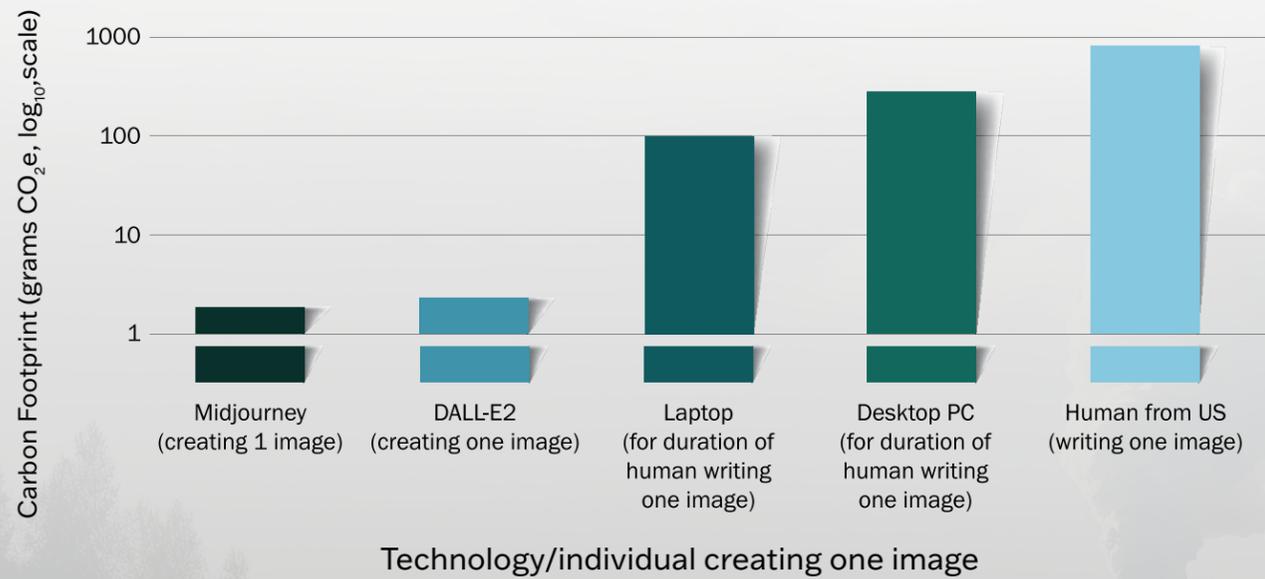
Looking specifically at AI, a recent February 2024 research report provides carbon emissions pollution quantification and comparison between common human work tasks and AI systems that are now capable of similar outputs. The new report, entitled [The carbon emissions of writing and illustrating are lower for AI than for humans](#), finds that despite the large amount of energy necessary to build and run AI systems, the carbon emissions footprints of popular AI systems are 130 to 1,500 times lower for text writing than humans doing the equivalent work, and [310 to 2,900 times lower for image creation](#).

The lead author of this study, UC Irvine Informatics professor Bill Tomlinson, writes: **"It's true that AI uses a lot of energy. The question, though, is: what should we compare it to? Compared to a mobile phone or a Google search, yes, AI is very energy-intensive. But as AI gets more and more competent, it becomes more relevant to compare its impact to humans, rather than to simpler technical systems. And AI uses a lot less energy than humans do to complete the complex tasks we studied."**

Carbon Footprint (grams CO2e) for Text Writing



Carbon Footprint (grams CO2e) for Image Creation



AI’s energy consumption and associated carbon emissions pollution are just one way to evaluate the environmental sustainability of these large AI systems – then there’s water.

Freshwater is a shared societal resource that must be used responsibly. In recent years, drought conditions are leading to increasing tensions over water usage between data centers and nearby residents.

A recent research paper referenced in the United Nation’s 2024 World Water Development Report, entitled *Making AI Less “Thirsty”: Uncovering and Addressing the Secret Water Footprint of AI Models* estimates that global AI usage may result in water withdrawal equal to about half of the entire United Kingdom in 2027.

Findings from this report assert that similar to carbon emissions pollution, when and where you train large AI models matters. Temporal shifting to train models during times requiring less cooling, and spatial shifting to train models in less water-constrained regions can help. Unfortunately, the research points out that the times and locations

that may be good for reducing water consumption might be bad for reducing carbon emissions pollution, and vice versa.

Therefore, it is important to consider environmental impacts holistically when making decisions about ways to reduce the environmental impact associated with training large AI models.

Organizations building new AI applications can minimize marginal additional environmental impacts by building on top of existing, shared cloud GenAI models provided by Microsoft, AWS, Google, and their partners. By reusing available models, companies only add net new resource consumption for their customizations and additional usage and otherwise share in the impacts of the distributed systems their applications are based on.

The end result is that, like other forms of digitization, these cloud-based AI systems do have environmental footprints to be mindful of, but the water and carbon intensity per unit of work is better than previous alternatives, especially considering the higher amounts of renewable energy, water recirculation, and other environmental efficiencies common with cloud providers.

Source: [The carbon emissions of writing and illustrating are lower for AI than for humans.](#)

AI Systems Helping Solve Environmental Sustainability Challenges

Returning to the premise that technology can improve lives, let's explore ways AI-enabled systems are helping solve environmental challenges.

MethaneSAT: At the most innovative end of the spectrum is [MethaneSAT](#). Launched in 2024, MethaneSAT is an Earth observation satellite measuring global methane emissions. This space-based system resolves cost and access limitations associated with plane-based systems. By combining MethaneSAT data with Google's AI capabilities, analysts can detect our planet's worst emissions sources and identify parties responsible for remediation in ways not previously feasible.

Efficiency Optimization: More common AI assistance often comes in the form of efficiency optimization. Enterprises with complex carbon emissions footprints tied to complex underlying supply chains are using AI to find and implement new efficiencies through energy, transportation, and supply chain optimizations. There are also a growing number of AI-powered solutions to reduce raw materials usage or improve recycling.

Data Management: AI is solving a myriad of data challenges that organizations face when trying to make progress on environmental sustainability initiatives. A 2023 report from the carbon accounting software provider, Persefoni, found that obtaining Scope 3 [supply chain] data and the general complexity of climate data are organizations' top two expected challenges in meeting comprehensive

[climate regulations](#). AI-enabled systems can help compile, aggregate, and analyze datasets that are large, complex, and often in unstructured formats.

Be Mindful of AI's Impacts, but Also Know How to Use AI for Environmental Good

The environmental problems facing organizations are often too large and complex for humans to solve alone. New AI systems empower increased forms of digitization and offer the potential to solve these problems more efficiently than previously possible. Responsible AI implementation involves evaluating and managing risks across environmental, social, and economic concerns, but the rewards may be large.

To summarize a path forward, the following bulleted process can help executives think through their own AI opportunities.

- **Articulate** your AI vision and objectives by engaging key stakeholders.
- **Benchmark** your AI capabilities and understand your organization's AI readiness.
- **Blueprint** your AI solution and roadmap with actionable steps.
- **Implement** your solution iteratively with sustainability and outcomes in mind.

To learn more about the latest SEC regulation read our takeaways - click the link below.



About Stratascale

Shaping the future of digital business & a more secure world as a digital and cybersecurity services company, Stratascale exists to help the Fortune 1000 transform the way they use technology to advance the business, generate revenue, and respond quickly to the market demands.

We call it Digital Agility.

Learn More