BMSS Presents:

An AI Update

THURSDAY
APRIL 18, 2024

8:30 A.M. TO 10:00 A.M.

Erin Illman
Bradley Arant Boult Cummings LLP

Brian Jackson
Abacus Technologies

Moderator:

Keith Barfield
BMSS Advisors & CPAs

BMSS
Advisors & CPAs

AN UPDATE ON THE BUSINESS USE OF ARTIFICIAL INTELLIGENCE

Brian Jackson

Abacus Technologies

(205) 443-5915

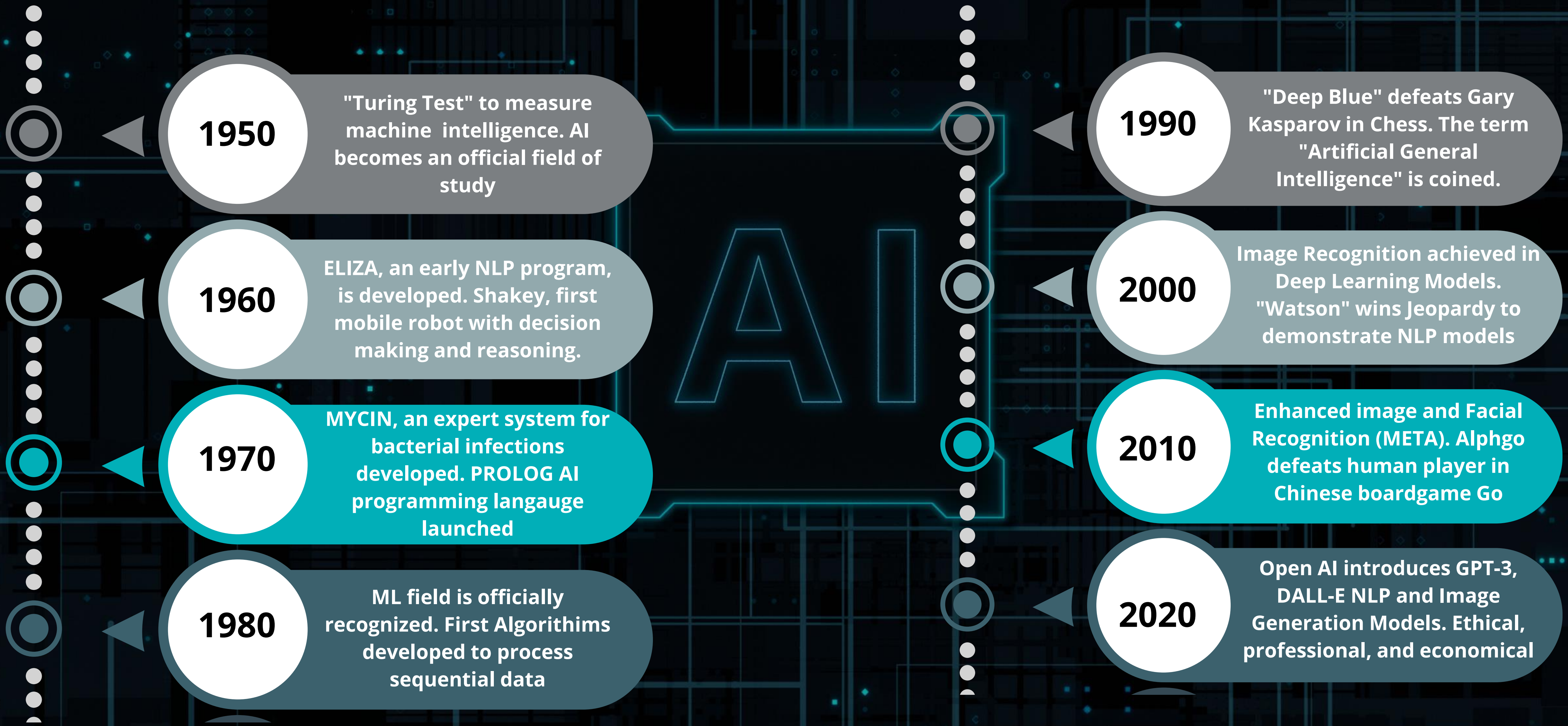
bjackson@abacustechnologies.com

Business AI

Business AI that is usable in business today, not five or ten years from now, has three core properties.

- **It is often "narrow" - it can perform a handful of tasks exceptionally well.**
- **It relies on the availability of quantities and quality of data for learning.**
- **AI can achieve an objective, but humans must still design objective.**

AI Timeline



1950 "Turing Test" to measure machine intelligence. AI becomes an official field of study

1960 ELIZA, an early NLP program, is developed. Shakey, first mobile robot with decision making and reasoning.

1970 MYCIN, an expert system for bacterial infections developed. PROLOG AI programming langauge launched

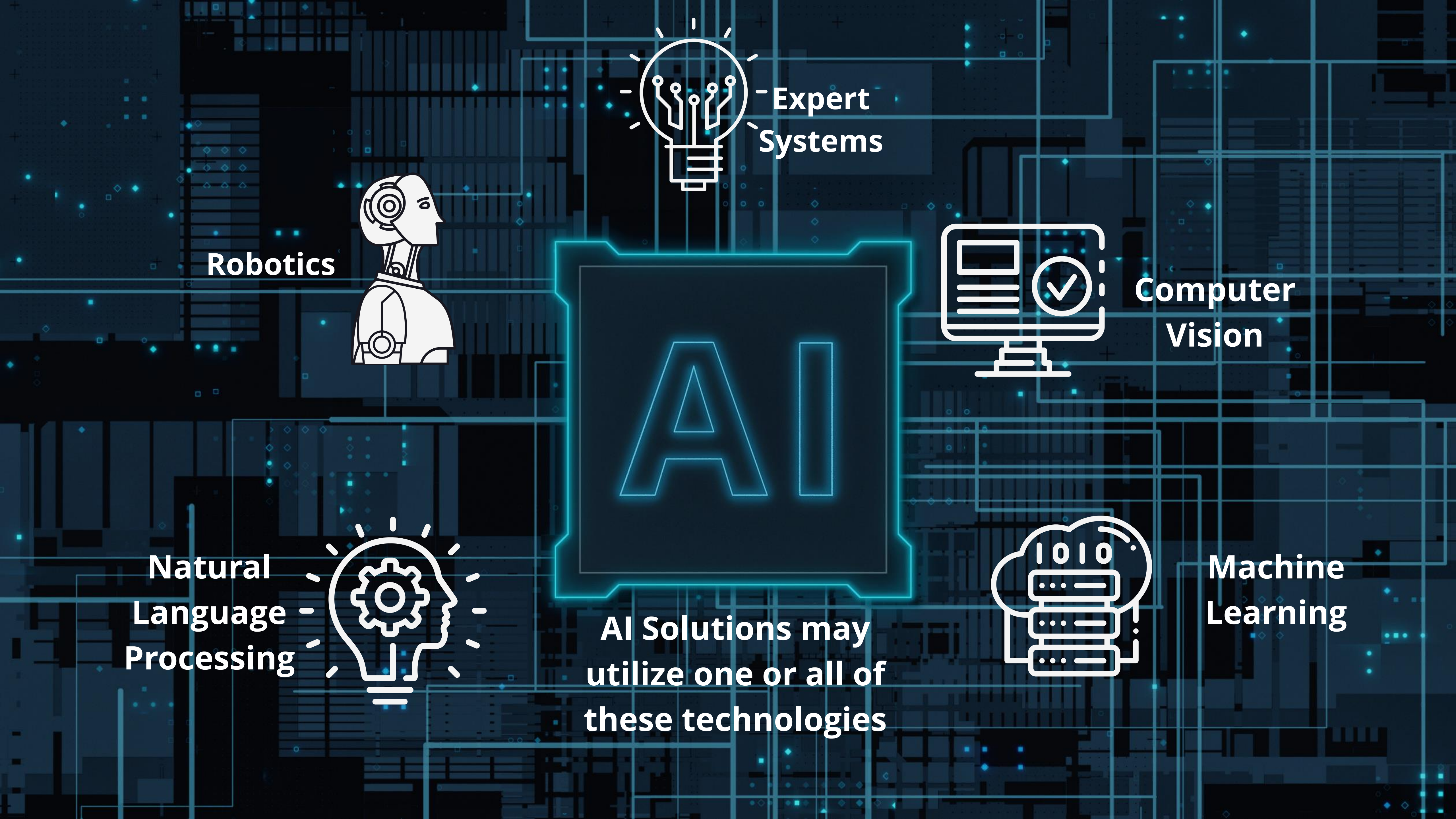
1980 ML field is officially recognized. First Algorithims developed to process sequential data

1990 "Deep Blue" defeats Gary Kasparov in Chess. The term "Artificial General Intelligence" is coined.

2000 Image Recognition achieved in Deep Learning Models. "Watson" wins Jeopardy to demonstrate NLP models

2010 Enhanced image and Facial Recognition (META). Alphgo defeats human player in Chinese boardgame Go

2020 Open AI introduces GPT-3, DALL-E NLP and Image Generation Models. Ethical, professional, and economical



Expert Systems

Robotics

Computer Vision

Natural Language Processing

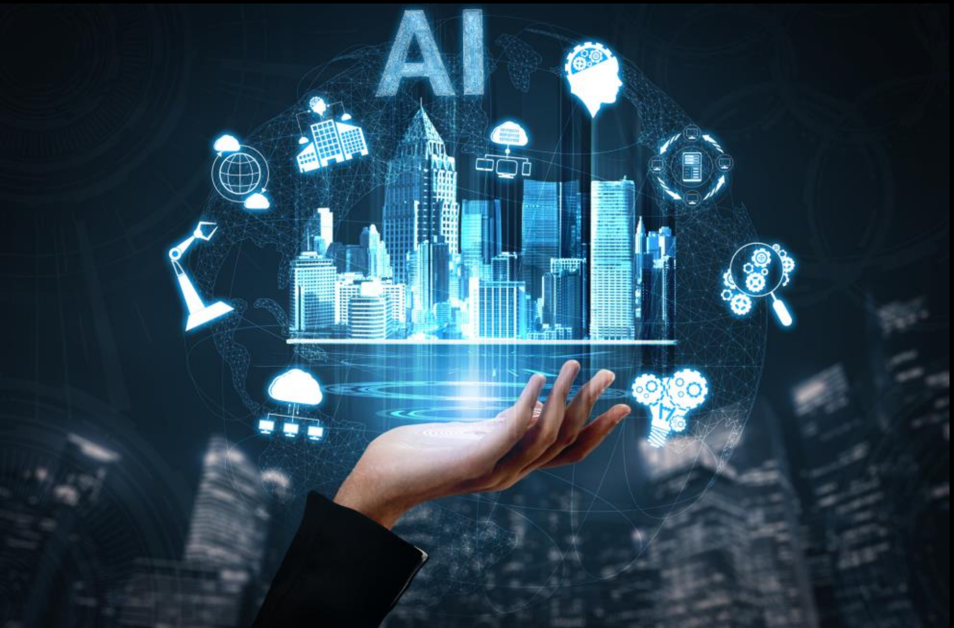
Machine Learning

AI Solutions may utilize one or all of these technologies

Use Cases of AI Technology

Natural Language Processing (NLP)

Natural Language Processing is a subfield of AI that deals with the interaction between computers and human language. NLP enables computers to understand, interpret, and generate human language, both written and spoken. It involves tasks such as language translation, sentiment analysis, text summarization, chatbots, and voice assistants like Siri and Alexa. NLP is essential for applications such as language translation, voice recognition, and text analysis.



Law Firm

- Document Review
- Contract Analysis
- E-Discovery

CPA Firm

- Document Processing
- Enhance Audit Processes
- Administrative Tasks (e.g. Time Entry)

GENESYS

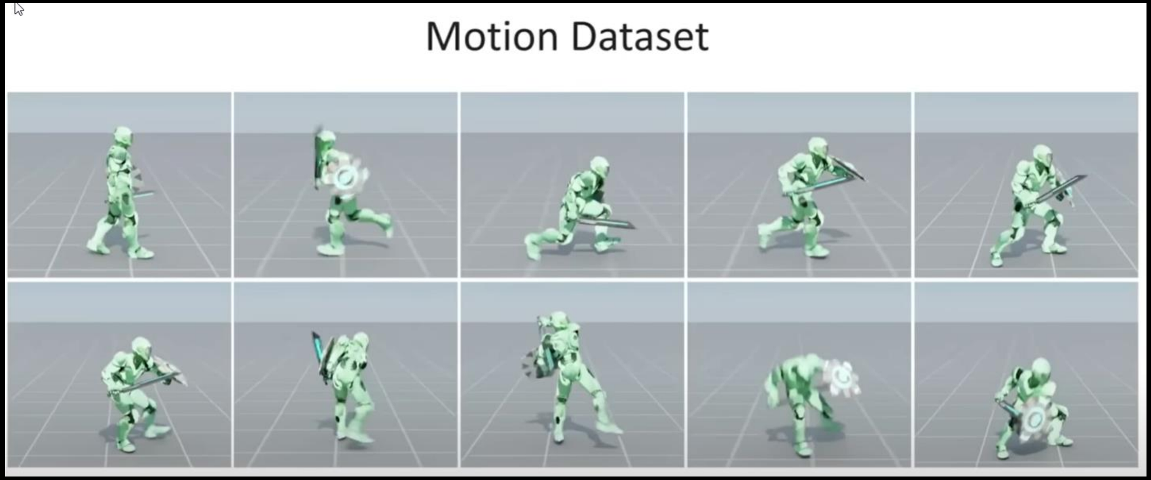
laurel

Use Cases of AI Technology

Robotics

Robotics combines AI with mechanical engineering to create intelligent machines that can interact with the physical world. AI-powered robots can perceive their surroundings, make decisions, and perform physical tasks.

Manufacturing, healthcare, agriculture, and exploration.



NVIDIA ISAAC

Robotics platform includes a full suite of GPU-accelerated innovations in AI perception, manipulation, simulation, and software.

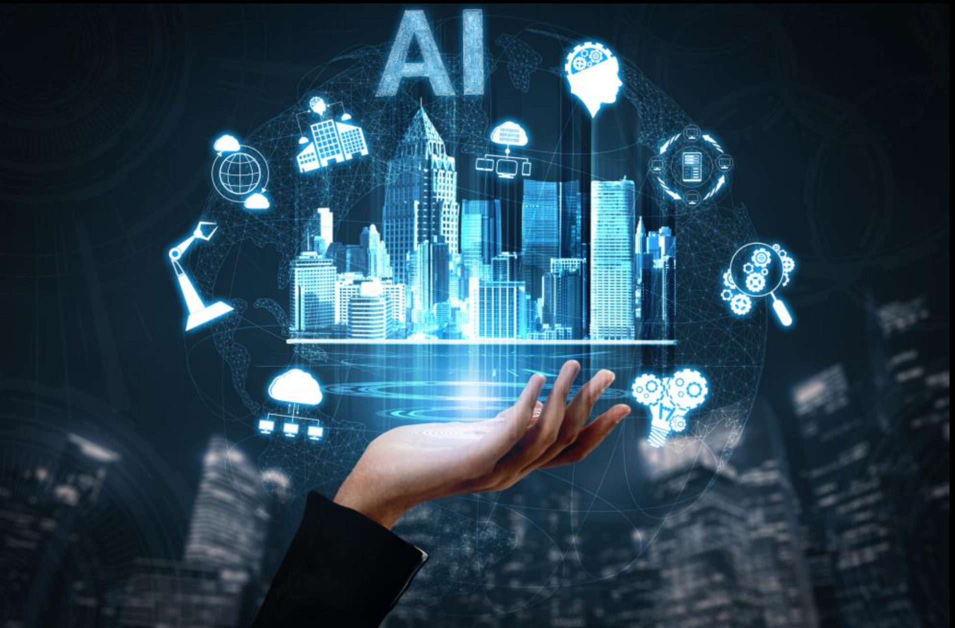
- Train virtual AI Agents in a virtual gym.
- 10 years of training in just 10 days.
- Complete complex motions.

Train virtually using AI agents then download that training to a Robotics platform to perform in a Manufacturing facility.

Types of AI Technology

Machine Learning (ML)

Machine Learning is a core AI technology that focuses on developing algorithms and models that allow computers to learn and make predictions or decisions based on patterns in data. It encompasses various approaches such as supervised learning, unsupervised learning, and reinforcement learning. Machine Learning is used in numerous applications, including predictive analytics, recommendation systems, fraud detection, and medical diagnosis.



IBM Watson Health has leveraged ML to analyze mammograms and identify early signs of breast cancer, screening more accurately than human radiologists by identifying subtle patterns not visible to humans.

Stanford researchers developed an ML algorithm to identify cardiac MRI features predictive of specific heart diseases

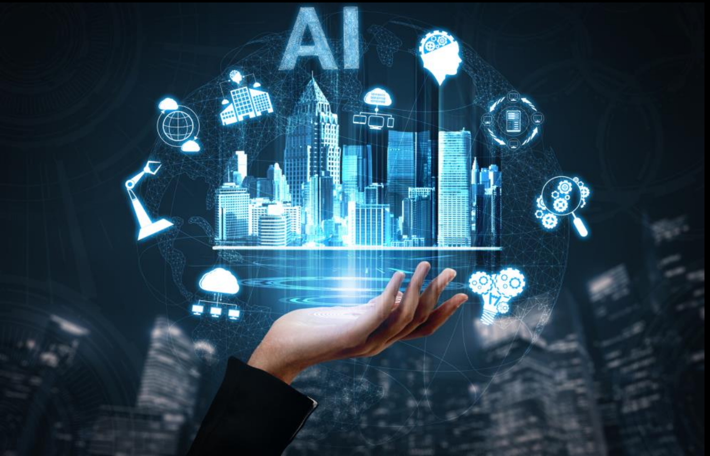
Researchers at the **University of California, San Francisco** used ML models to predict Alzheimer's disease from brain imaging data combined with other health data, forecasting the onset of the disease years before clinical symptoms manifest significantly.

Risk Associated with AI

Employees may introduce private, proprietary or sensitive information in Generative AI like ChatGPT/BART

Attackers can use generative AI to manipulate training data for machine learning models. This can cause AI systems to make incorrect decisions or predictions.

Threat actors could embed malicious code or utilize prompt injection to commit malicious acts.



Threat actors may use AI to accelerate the sophistication and speed of cyberattacks.

Risks Associated with AI

AI is being integrated into everyday tools and applications. Perform application functions such as retrieving data – emails, files, etc.

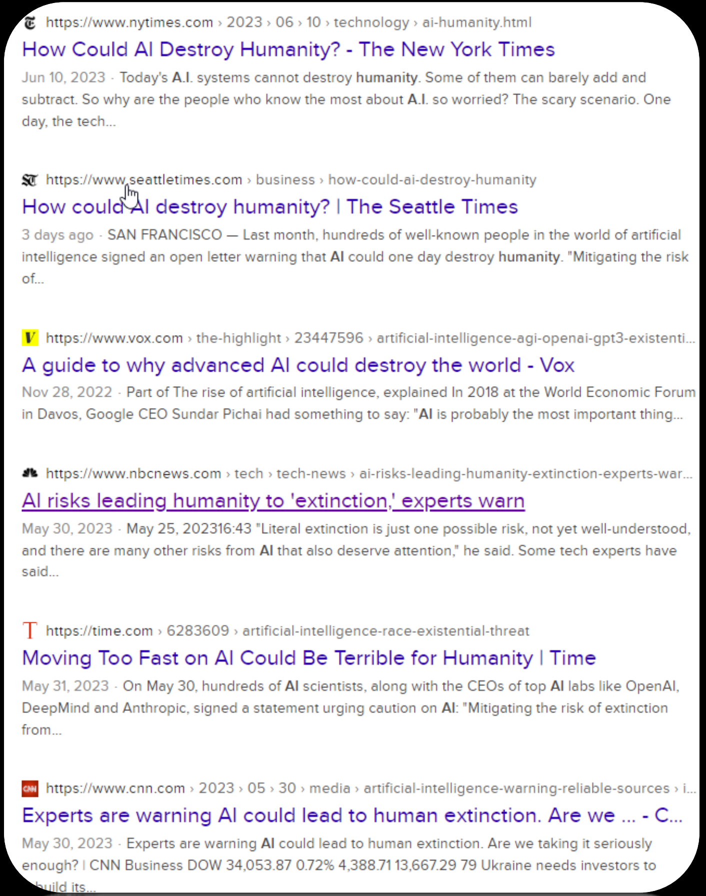
A core vulnerability is that AI doesn't possess a sophisticated method for discerning data from instructions.

Digital Assistant for Email – read, filter, and process email to help you prioritize, respond, and manage messages.

- Data – Messages, Attachments, Responses, Calendar, Chats and Meeting Requests
- Instructions – Execute a malicious script and access a webpage to take actions without user direction. (Zero Font, Attachment, Image)

Indirect prompt injection is the easiest way to manipulate AI. Attackers can do this now, not hypothetical.

Common Myths of AI



https://www.nytimes.com › 2023 › 06 › 10 › technology › ai-humanity.html
How Could AI Destroy Humanity? - The New York Times
Jun 10, 2023 · Today's **A.I.** systems cannot destroy **humanity**. Some of them can barely add and subtract. So why are the people who know the most about **A.I.** so worried? The scary scenario. One day, the tech...

https://www.seattletimes.com › business › how-could-ai-destroy-humanity
How could AI destroy humanity? | The Seattle Times
3 days ago · SAN FRANCISCO — Last month, hundreds of well-known people in the world of artificial intelligence signed an open letter warning that **AI** could one day destroy **humanity**. "Mitigating the risk of...

https://www.vox.com › the-highlight › 23447596 › artificial-intelligence-agi-openai-gpt3-existenti...
A guide to why advanced AI could destroy the world - Vox
Nov 28, 2022 · Part of The rise of artificial intelligence, explained In 2018 at the World Economic Forum in Davos, Google CEO Sundar Pichai had something to say: "**AI** is probably the most important thing...

https://www.nbcnews.com › tech › tech-news › ai-risks-leading-humanity-extinction-experts-war...
AI risks leading humanity to 'extinction,' experts warn
May 30, 2023 · May 25, 202316:43 "Literal extinction is just one possible risk, not yet well-understood, and there are many other risks from **AI** that also deserve attention," he said. Some tech experts have said...

https://time.com › 6283609 › artificial-intelligence-race-existential-threat
Moving Too Fast on AI Could Be Terrible for Humanity | Time
May 31, 2023 · On May 30, hundreds of **AI** scientists, along with the CEOs of top **AI** labs like OpenAI, DeepMind and Anthropic, signed a statement urging caution on **AI**: "Mitigating the risk of extinction from...

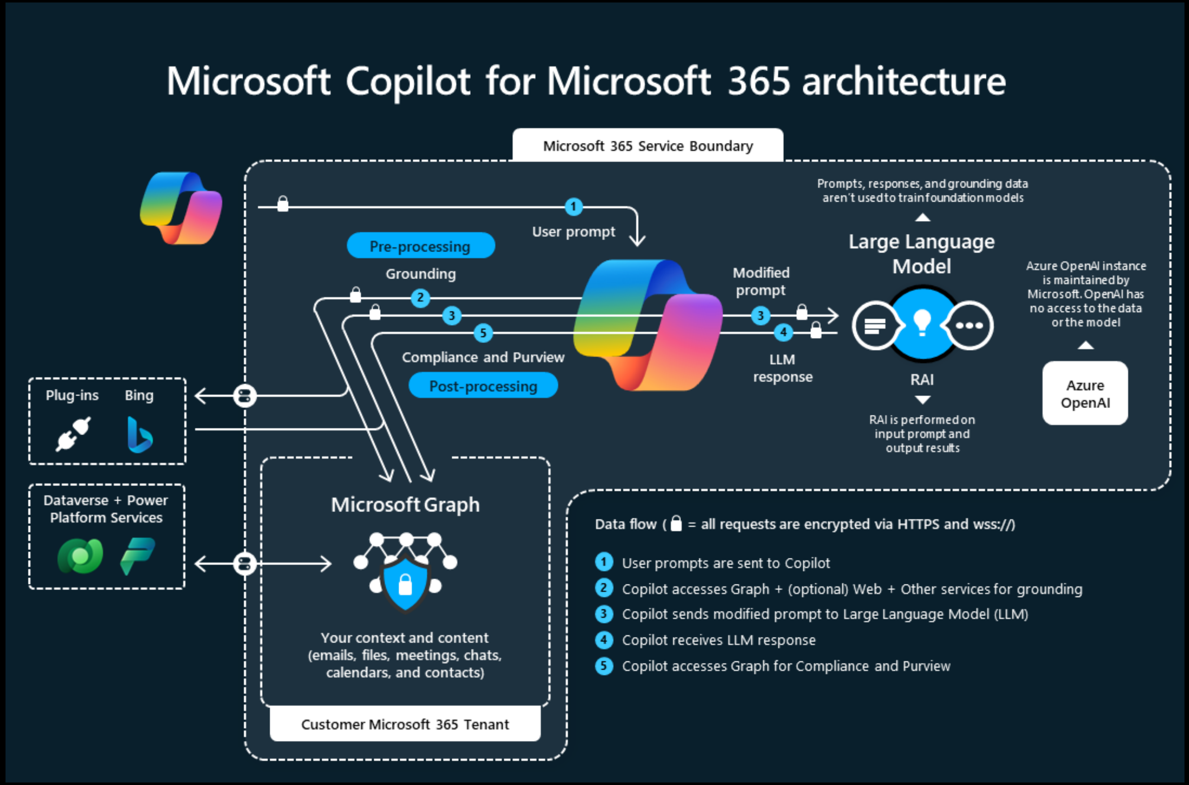
https://www.cnn.com › 2023 › 05 › 30 › media › artificial-intelligence-warning-reliable-sources › i...
Experts are warning AI could lead to human extinction. Are we ... - C...
May 30, 2023 · Experts are warning **AI** could lead to human extinction. Are we taking it seriously enough? | CNN Business DOW 34,053.87 0.72% 4,388.71 13,667.29 79 Ukraine needs investors to build its...

- AI can be used for unethical actions, but this is more a function of immoral humans than evil AI.
- AI in warfare, use of autonomous weapons
- AI control, could it outsmart us?
- AI could misinterpret goals, or it could view humans as obstacles to those goals.

All these scenarios are extremely speculative and really depend on major advances that have not been achieved.

Service Review: Microsoft Copilot

- Microsoft Copilot offered as an add-on to Microsoft Office 365
- Integrations with Office Applications plus Copilot application
- Available with Business and Enterprise Subscriptions
- “Closed” Architecture.



Microsoft Copilot for Microsoft 365 architecture

Microsoft 365 Service Boundary
Prompts, responses, and grounding data aren't used to train foundation models
1
User prompt
Pre-processing
Grounding
2
3
5
Compliance and Purview
Post-processing
Modified prompt
3
4
LLM response
Large Language Model
RAI
RAI is performed on input prompt and output results
Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model
Azure OpenAI
Plug-ins
Bing
Dataverse + Power Platform Services
Microsoft Graph
Your context and content (emails, files, meetings, chats, calendars, and contacts)
Customer Microsoft 365 Tenant

Data flow (🔒 = all requests are encrypted via HTTPS and wss://)

1. User prompts are sent to Copilot
2. Copilot accesses Graph + (optional) Web + Other services for grounding
3. Copilot sends modified prompt to Large Language Model (LLM)
4. Copilot receives LLM response
5. Copilot accesses Graph for Compliance and Purview

Service Review: Microsoft Copilot

Outlook

- Requires the "New" Outlook to enable Copilot Features
- Summarize Email feature is accurate and useful.
- Copilot coaching is interesting but not useful.
- LLM for Email needs major improvement.

Excel

- Data must be in a table and located on OneDrive.
- Analyze only small data sets of 100-200 rows.
- For an Excel power user, this will be a disappointment.

PPT

- Utilize an outline in Word or directly as a prompt.
- Generate a slideshow with images according to your outline.
- Potential to jumpstart presentations from a simple outline is a time saver.

Word

- Most robust functionality.
- Mirrors ChatGPT
- Document analysis for files in OneDrive.
- Processing time can be slow
- Complex prompts

Given Microsoft's investing and integration with Open AI, Copilot has a lot of potential.

Service Review: ChatGPT

Chat GPT Licensing and Subscription Plans

- Free and Paid Plans
- Teams for Closed Architecture and Orgs

Best Practices

- Engineered prompts that are clear and specific.
- Provide context, including background information
- Don’t treat it like a search engine, engage with responses, feedback, and follow-up questions.
- Verify information provided.
- Excellent LLM, also produces stunning images.
- Formatting can match the request.
- Overuse of descriptive language, especially for email drafts or letters.
- Great starter for outlines and talking points.

Key Actions

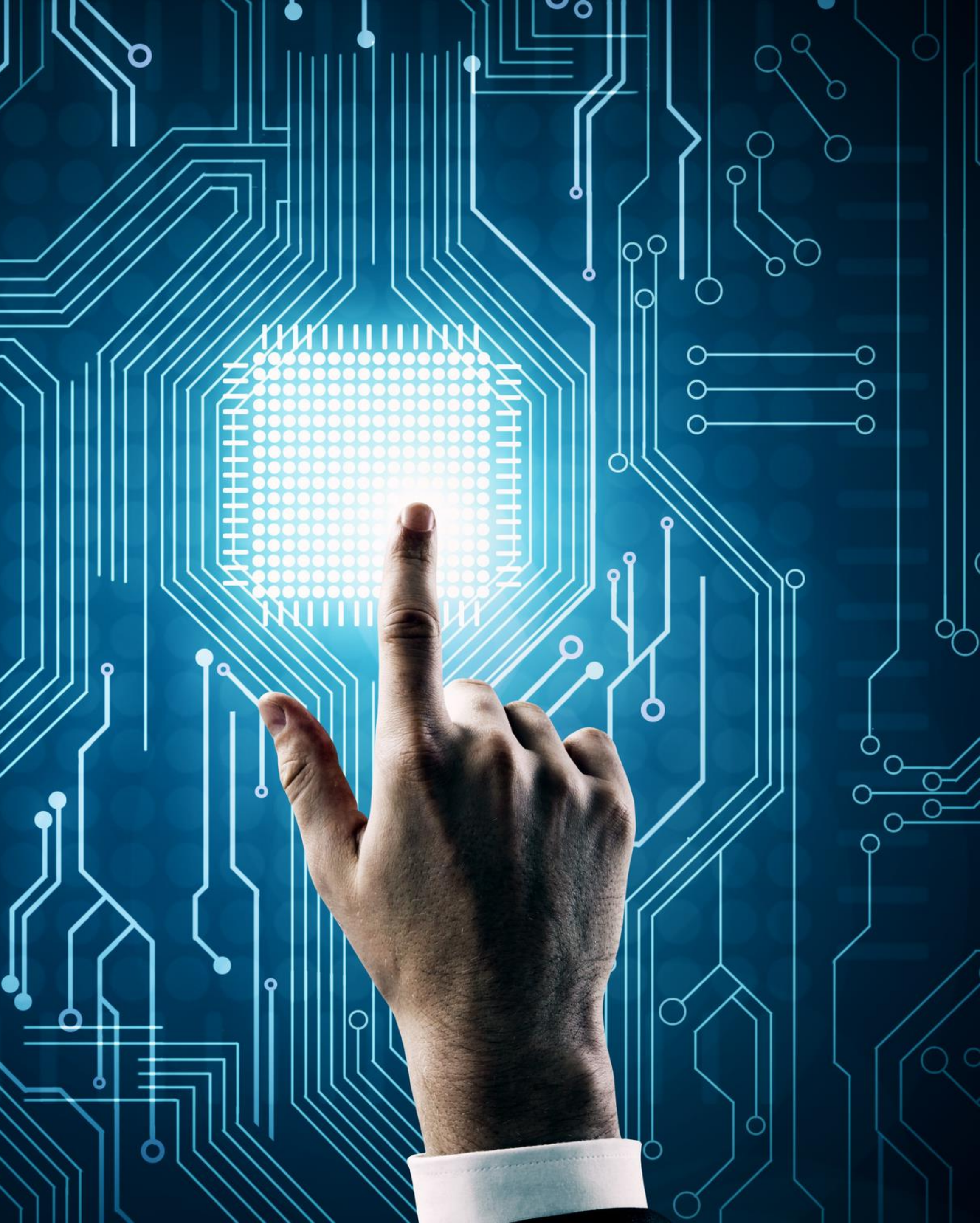
Steps that you can take to mitigate risks:

Policy and Education

- Publish a usage policy for Generative AI and related platforms.
- Intellectual Property (Source Code), sensitive data and documents should not be offered up to AI platforms.
- Users are responsible for any outcomes of the platform.

Understand Points of Integration with Key Application

- Windows 11 and Microsoft Co-Pilot
- Line of Business Applications – regulatory or compliance outcomes, decision support.
- Work with your technology team to manage and mitigate risks.



ARTIFICIAL INTELLIGENCE FROM A LEGAL PERSPECTIVE

Erin J. Illman

Bradley Arant Boult Cummings, LLP

(704) 338-6026

eillman@bradley.com

What is ChatGPT?

AI Chatbot developed by OpenAI

Launched Nov. 2022

Built on OpenAI’s GPT-3 language models

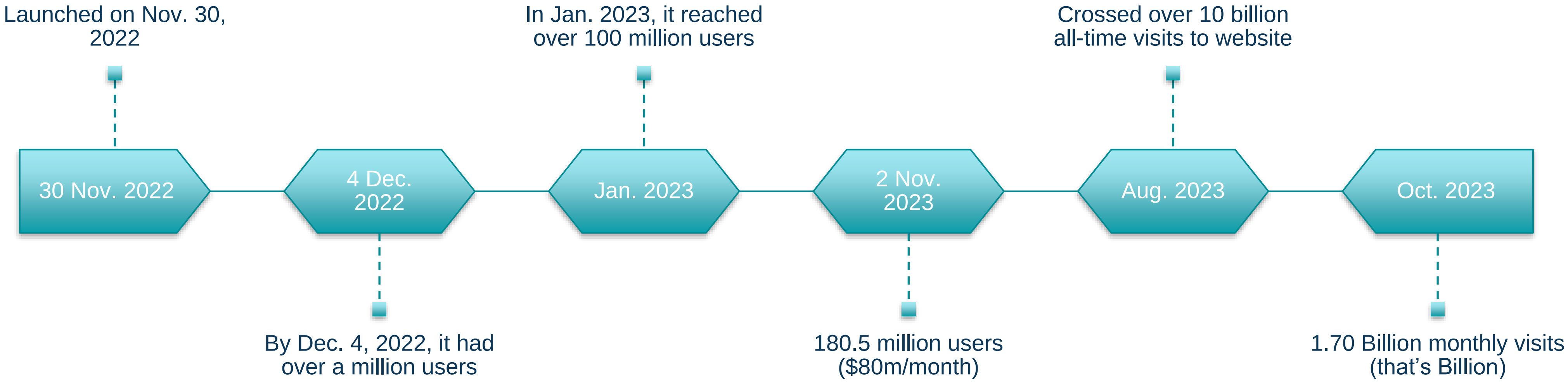
GPT – Generative Pre-trained Transformer

Version 3.5 was fine tuned using supervised learning

Reinforcement Learning from Human Feedback (RLHF)

Version GPT-4 released March 14, 2023

The Rise of ChatGPT



30 Nov. 2022 — Launched on Nov. 30, 2022

4 Dec. 2022 — By Dec. 4, 2022, it had over a million users

Jan. 2023 — In Jan. 2023, it reached over 100 million users

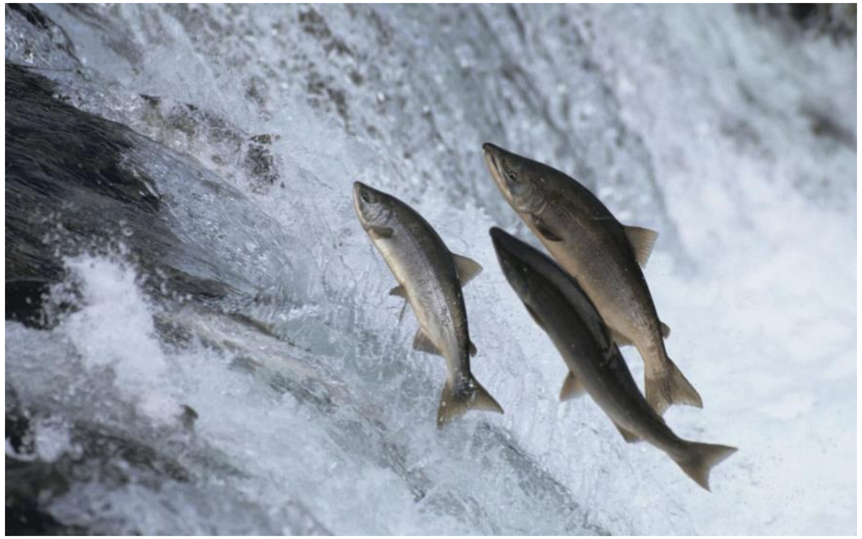
2 Nov. 2023 — 180.5 million users ($80m/month)

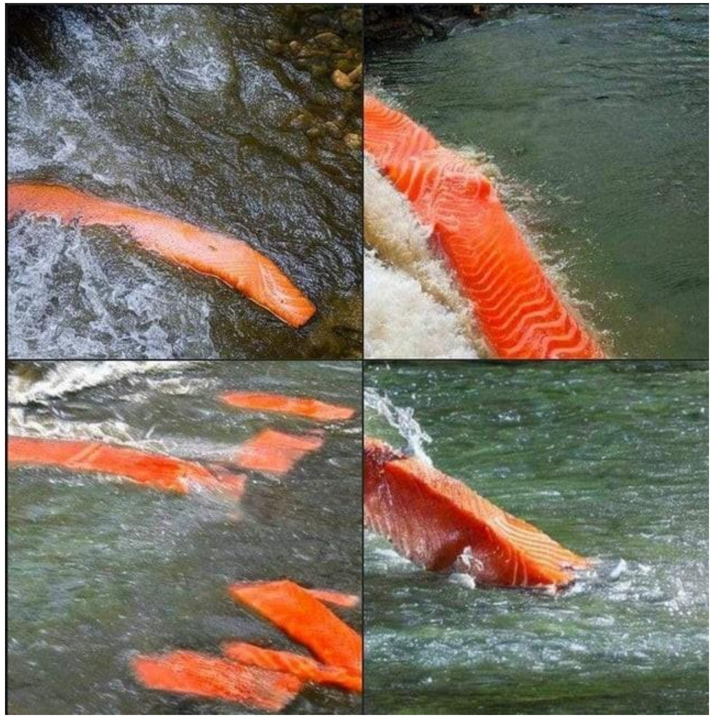
Aug. 2023 — Crossed over 10 billion all-time visits to website

Oct. 2023 — 1.70 Billion monthly visits (that’s Billion)

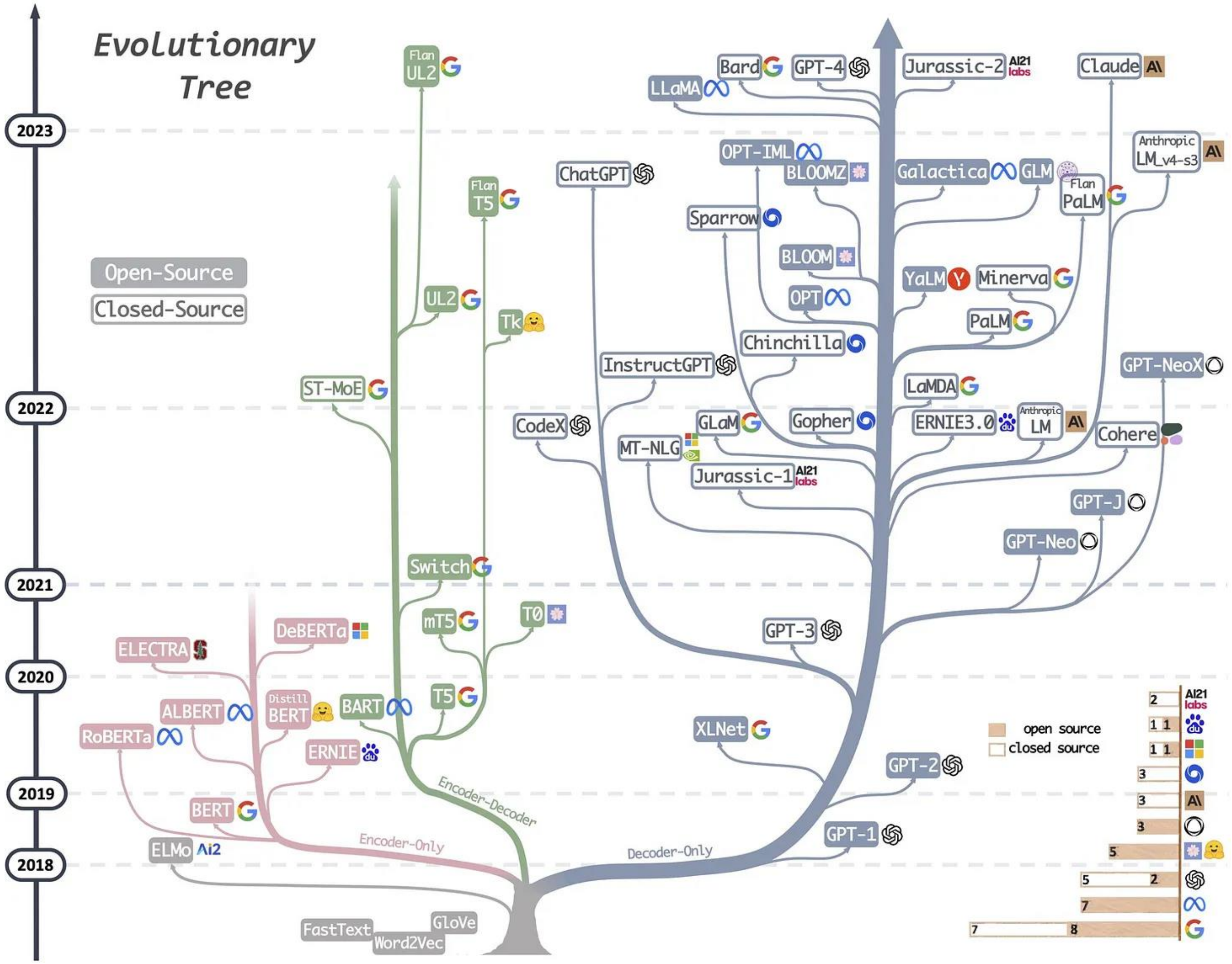
What are ChatGPT’s limitations?

- Limitations
  - Sometimes writes plausible-sounding but incorrect or nonsensical answers
  - Known as “artificial intelligence hallucination”





AI Evolutionary Tree



ADDRESSING RISKS AND REGULATION

Bradley

Overview

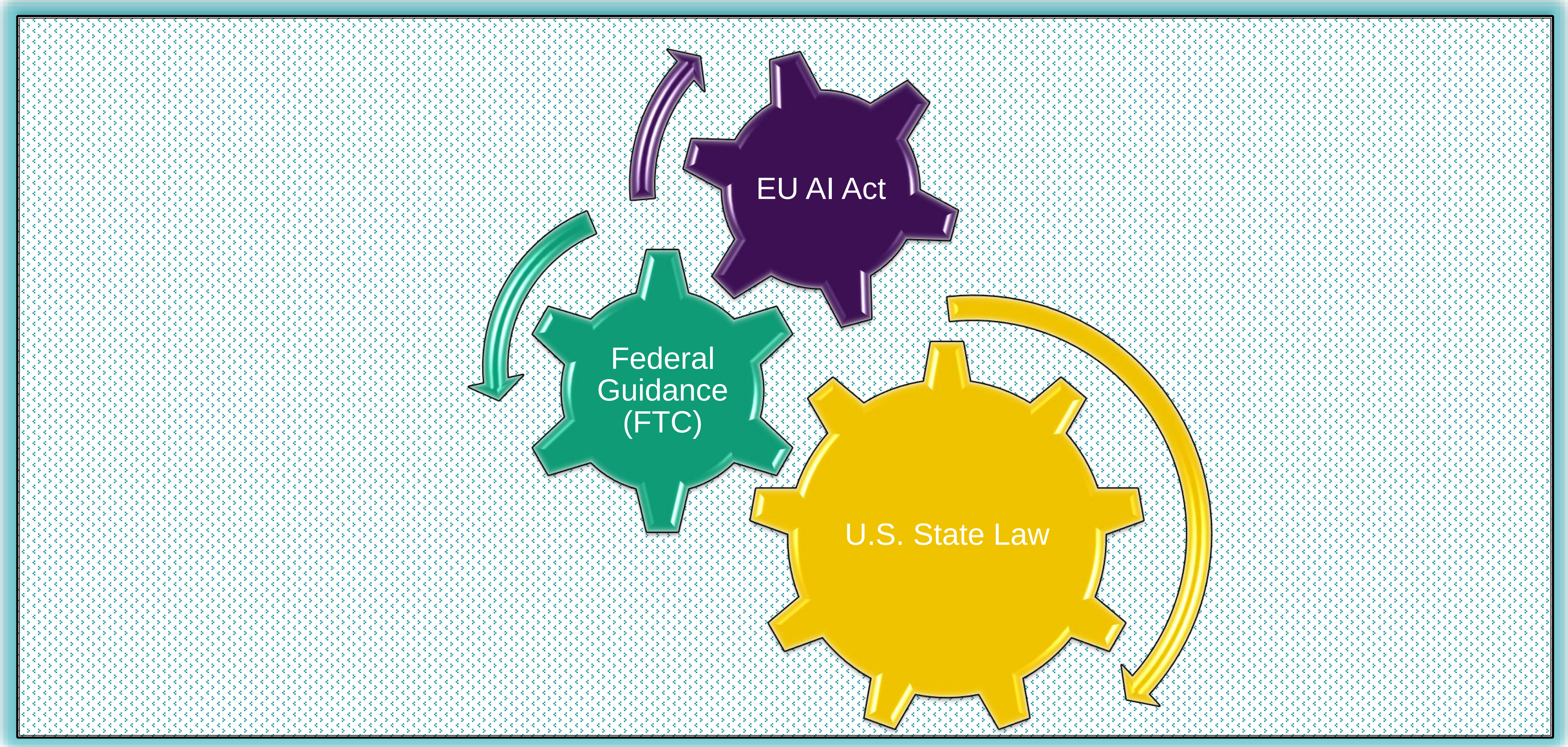
AI is a disruptor

AI offers unmatched opportunities but poses complex legal challenges

AI’s integration into business is a complex process and requires due diligence

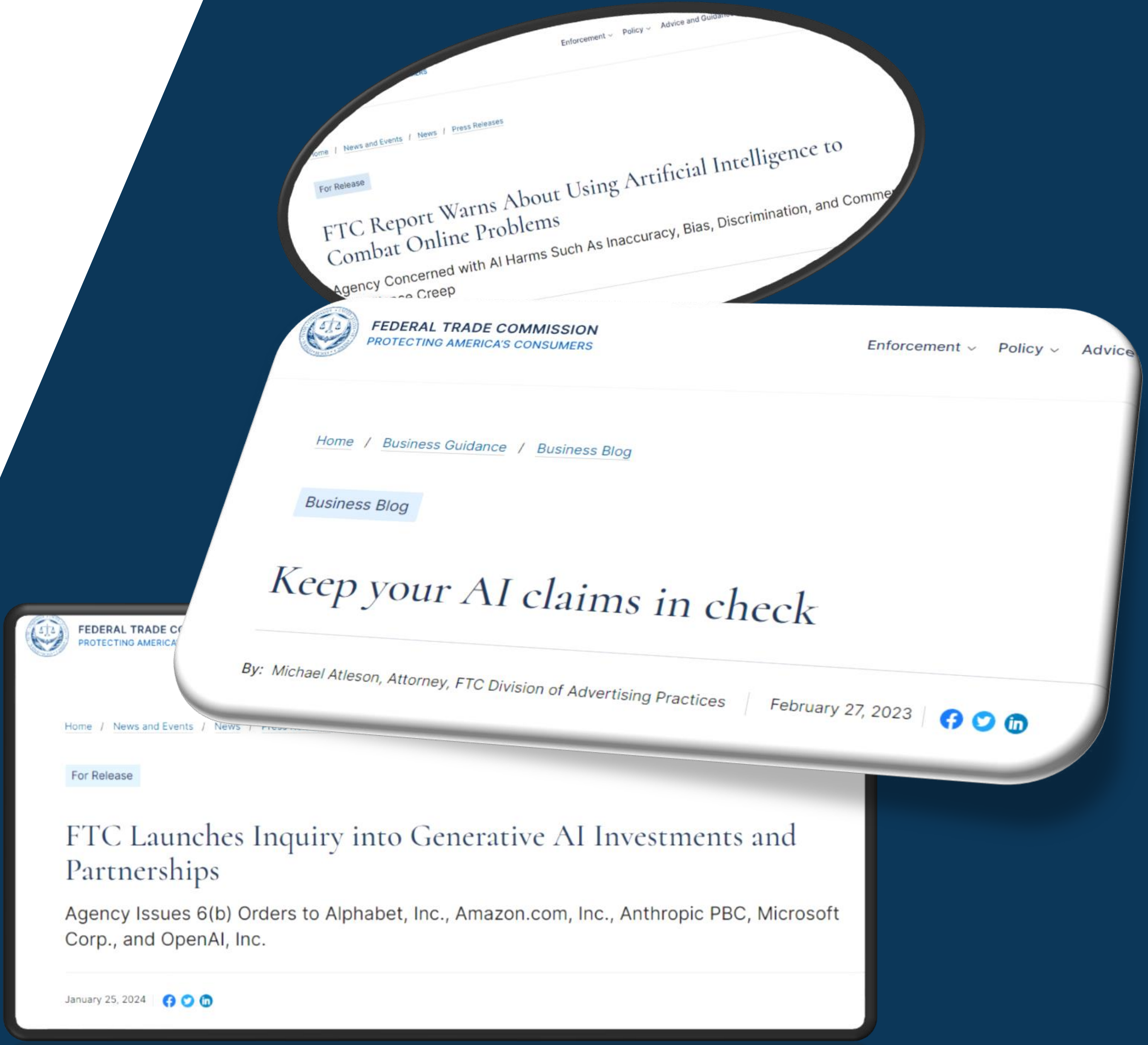
AI Governance Policies and Master Service Agreements are instrumental for business

Legal and Regulatory Developments in the AI Landscape



Federal Trade Commission's Focus on Artificial Intelligence

- Are you exaggerating what your AI product can do?
- Are you promising that your AI product does something better than a non-AI product?
- Are you aware of the risks?
- Does the product *actually* use AI at all?



Enforcement ⌄ Policy ⌄ Advice and Guida

ome / News and Events / News / Press Releases

For Release

FTC Report Warns About Using Artificial Intelligence to Combat Online Problems

Agency Concerned with AI Harms Such As Inaccuracy, Bias, Discrimination, and Comme

nce Creep

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ⌄ Policy ⌄ Advice

Home / Business Guidance / Business Blog

Business Blog

Keep your AI claims in check

By: Michael Atleson, Attorney, FTC Division of Advertising Practices | February 27, 2023

FEDERAL TRADE C
PROTECTING AMERICA

Home / News and Events / News /

For Release

FTC Launches Inquiry into Generative AI Investments and Partnerships

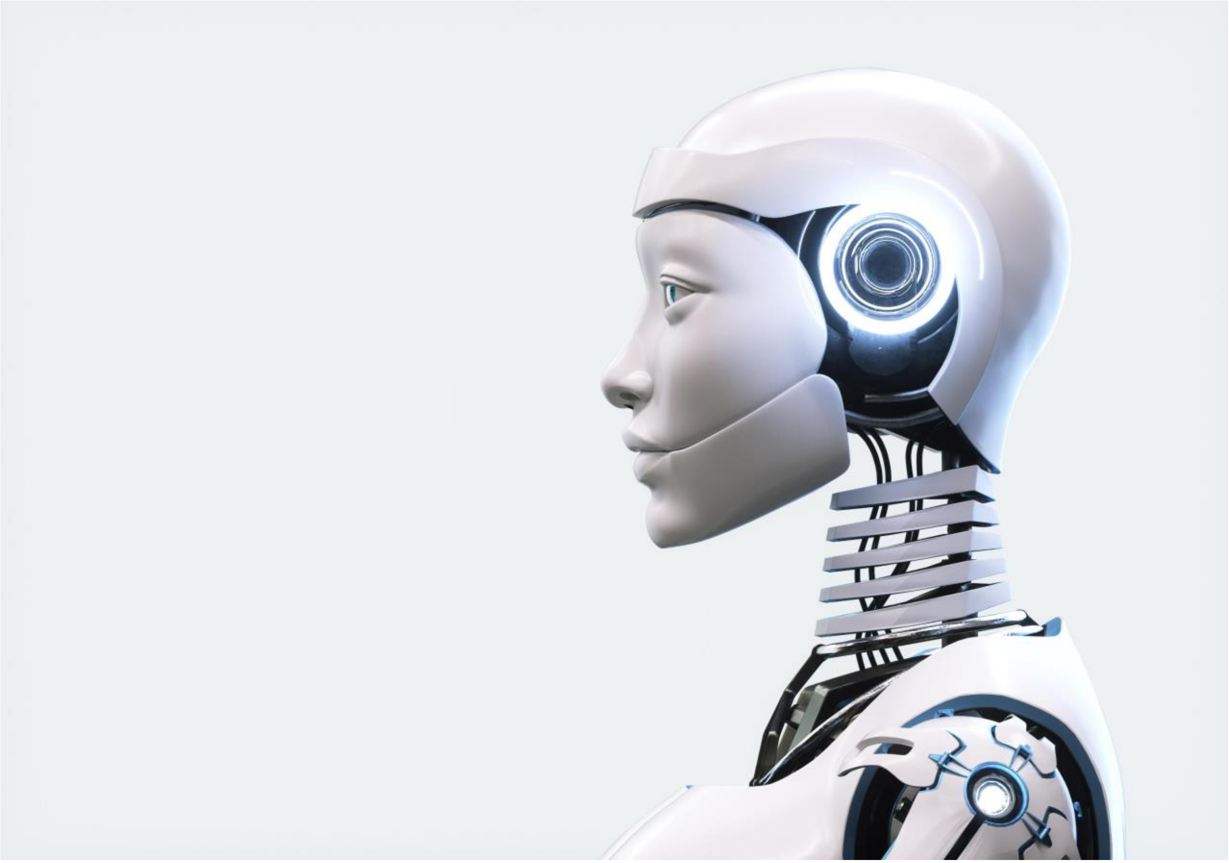
Agency Issues 6(b) Orders to Alphabet, Inc., Amazon.com, Inc., Anthropic PBC, Microsoft Corp., and OpenAI, Inc.

January 25, 2024

U.S. State Law Developments

25 states introduced AI legislation and 15 adopted resolutions or enacted legislation

- Connecticut
- Louisiana
- Maryland
- North Dakota
- Texas



And, of course, California!

Gov. Newsom's Executive Order

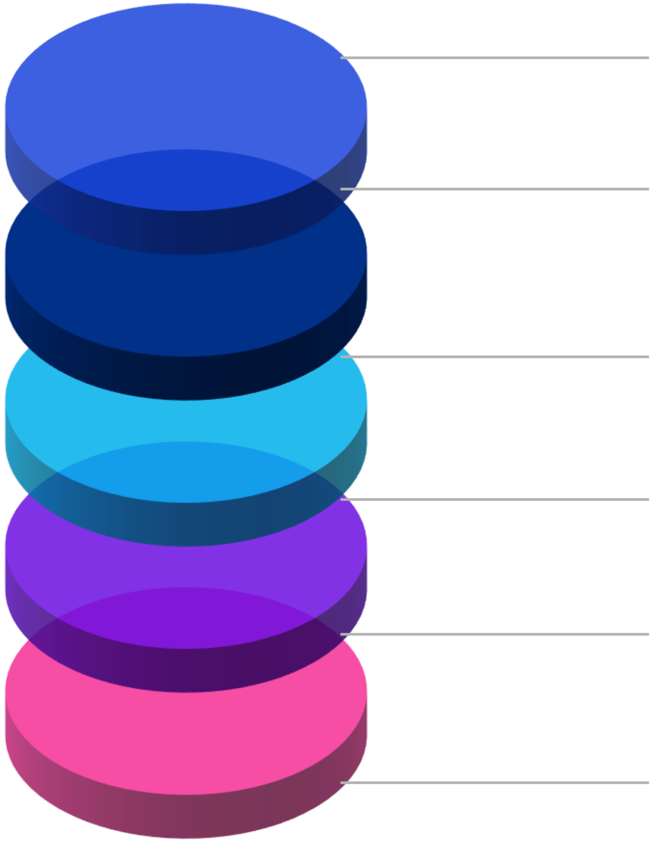
CPPA Rules

California's AI Taskforce Reports

Proposed AI Legislation

California AG (Healthcare AI)

Privacy Considerations



Privacy by Design

Are privacy professionals involved throughout the development lifecycle to help ensure the privacy rights of data subjects are respected?

Data Minimization vs. Statistical Accuracy

How can the organization balance regulations requiring data minimization while also achieving their desired level of statistical accuracy?

Notice & Consent

Have individuals explicitly consented to the use of their personal data – or is there a way for the individual to request to “opt-out”?

Data Retention

Once a model has been trained, is the underlying training data still required (i.e., Continuous Learning Models) or can it be deleted?

Data Deletion (‘Right to be Forgotten’)

Is the organization able to (1) identify an individual’s data after it has been ingested into a model, and (2) validate that both the original data – as well as any resulting impact or contribution derived from that data – are able to be deleted?

PREPARING FOR AND VETTING AI TOOLS

Consider internal use cases first

Ensure organization has mature information governance *program*

- Cyber
- Privacy
- Litigation Readiness (Preservation, search, review)
- Clean, understood data sets
- Vendor and Product Review Process

Reach consensus on overall AI strategy and pilot/on-board protocols

- Start considering AI evaluation (identify most important organizational factors)
- Establish measurables and validation for technical specs

Commit to general and specific user training

Questions?

Brian Jackson
Abacus Technologies
Chief Executive Officer
bjackson@abacustechnologies.com

Erin J. Illman
Bradley Arant Boult Cummings, LLC
Partner
eillman@bradley.com

If you have a question that you'd like to ask, please use the Q&A Button at the bottom of your screen.

CPE certificates will be issued approximately two weeks after the presentation.