2023 Update

Artificial Intelligence & Cybersecurity

RoundTable
TECHNOLOGY

06.28.2023

Who is RoundTable Technology?

Today's Presenters

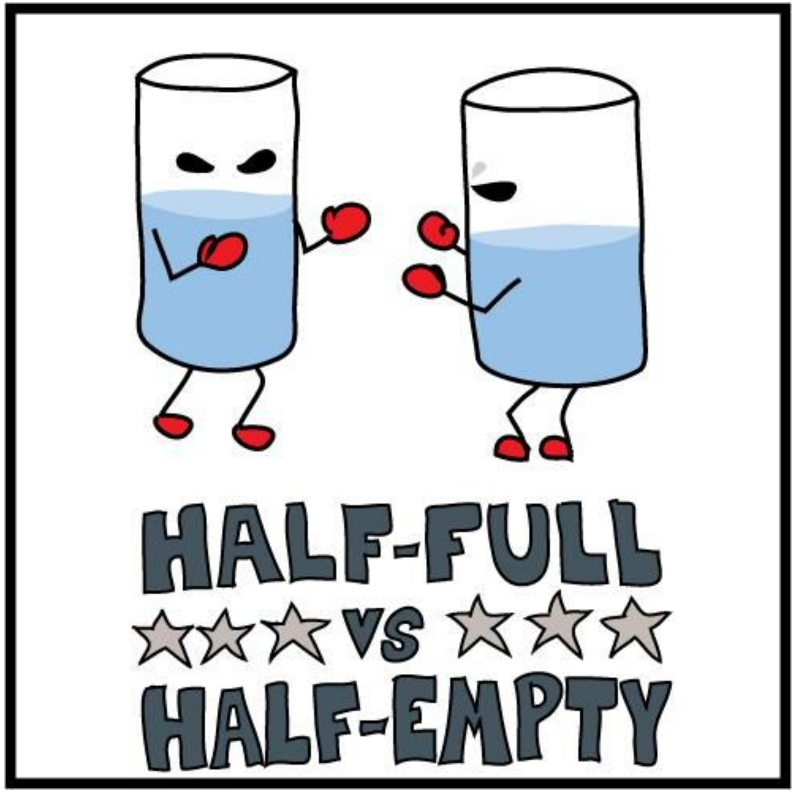
Joshua Peskay

3CPO

Destiny Bowers

Cybersecurity & Cloud Strategy

Agenda



RoundTable
TECHNOLOGY

RoundTable Technology is a strategic partner who will work with your organization to help you leverage technology to fulfill your mission.

We understand what it's like to be a nonprofit, working with limited resources, budget, and people. That's why we only hire personnel that are themselves driven by serving those who serve. We are currently supporting over 200 nonprofit clients and helping them get their technology under control.

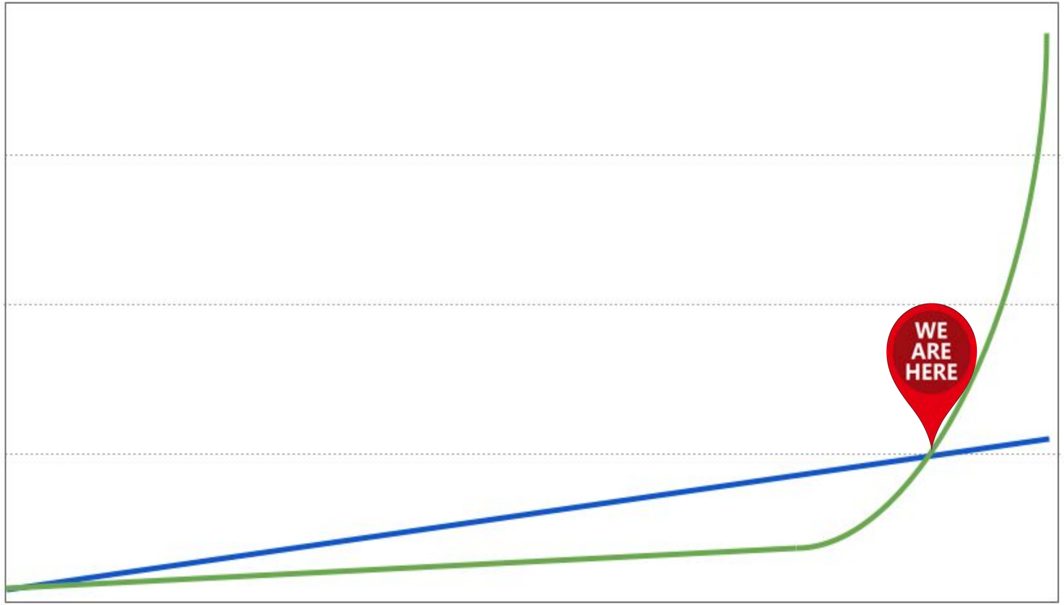
Channel Futures
Leading Channel Partners Forward
MSP 501
WINNER

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

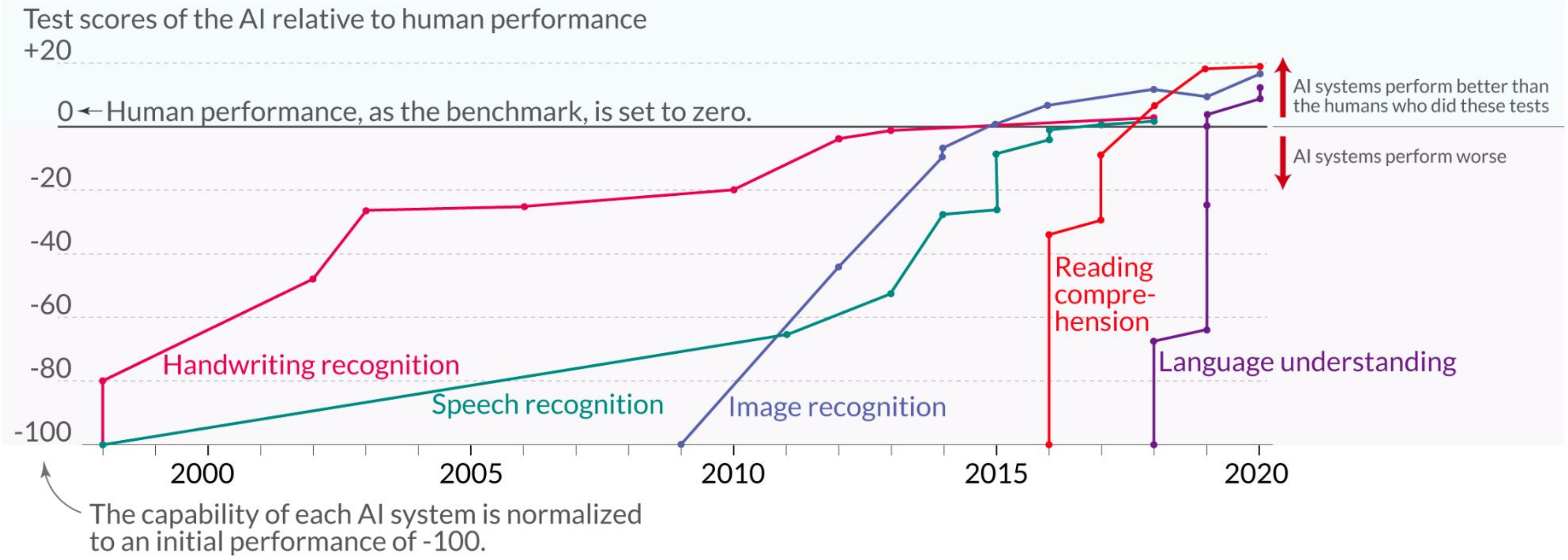
COMMUNITIES FOUNDATION of TEXAS for BUSINESS
BE IN GOOD COMPANY
- 2022 -

Exponential Growth

Exponential Growth



Why so much growth now?



Language and image recognition capabilities of AI systems have improved rapidly

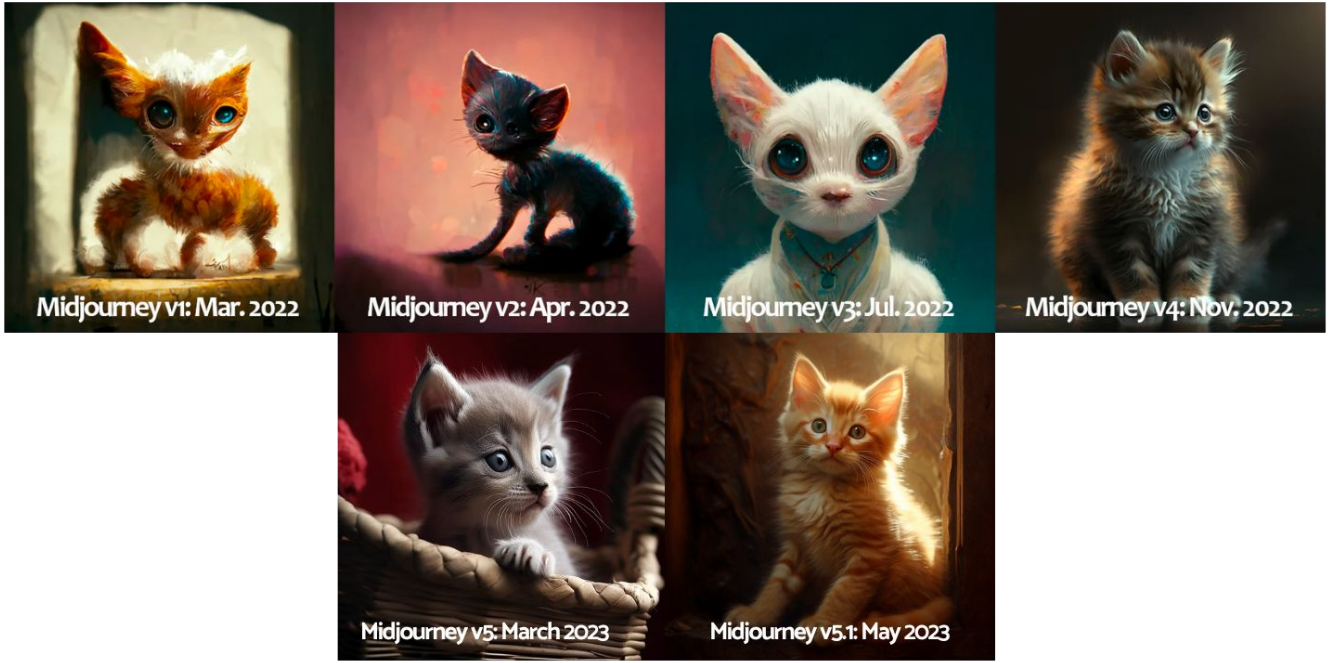
Our World in Data

Data source: Kiela et al. (2021) – Dynabench: Rethinking Benchmarking in NLP

OurWorldinData.org – Research and data to make progress against the world's largest problems.

Licensed under CC-BY by the author Max Roser

Pace of improvement



Credit to [Maria Korolov] for "kitten" versions 1 through 5

How long did it take to reach 100 million users?

Telephone
75 Years

Mobile Phone
16 Years

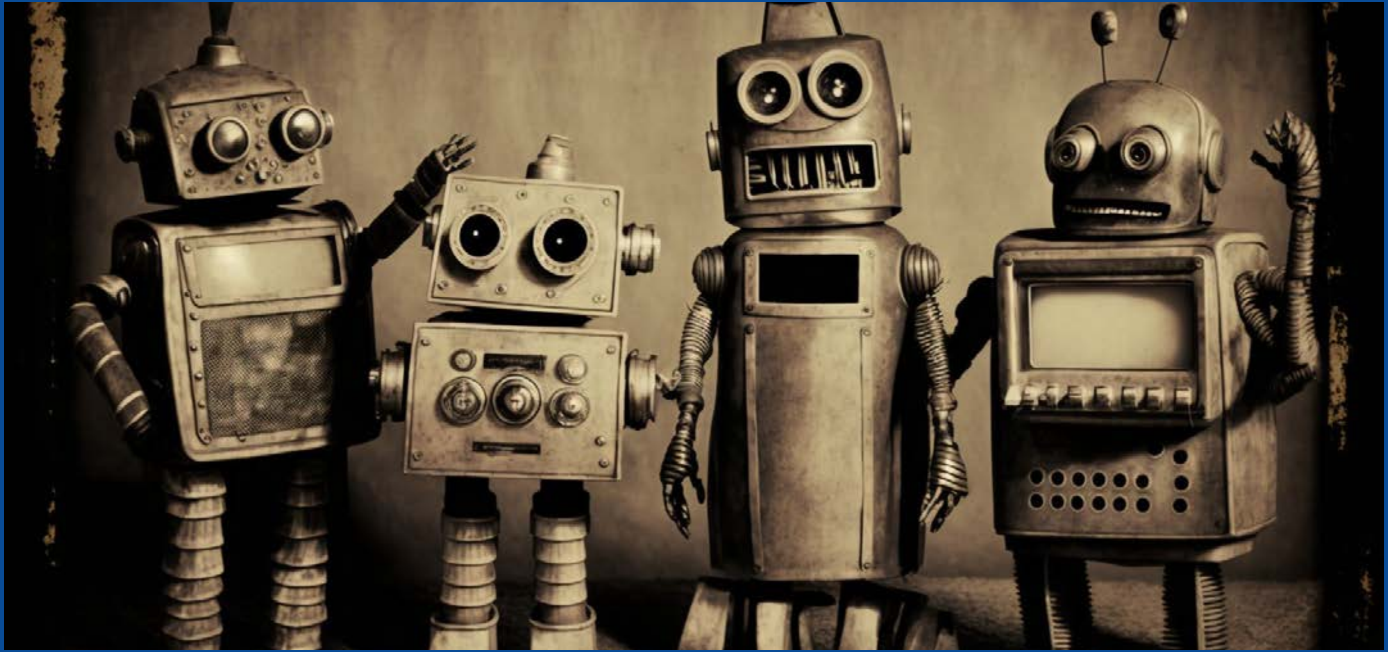
Netflix
10 Years

World Wide Web
7 Years

Facebook
4.5 Years

ChatGPT
2 Months

Generative AI Personalities



Generative Text Systems

Free Products

ChatGPT

The Unpaid
Intern

Microsoft Bing

The Research
Assistant

Google
Bard AI Chatbot

The
Second Opinion

Search-based
web based

Paid ($20/month)

OpenAI
ChatGPT4.0

The Paid Intern

ANTHROPIC

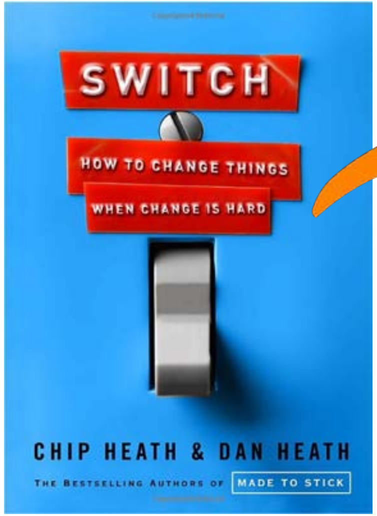
N

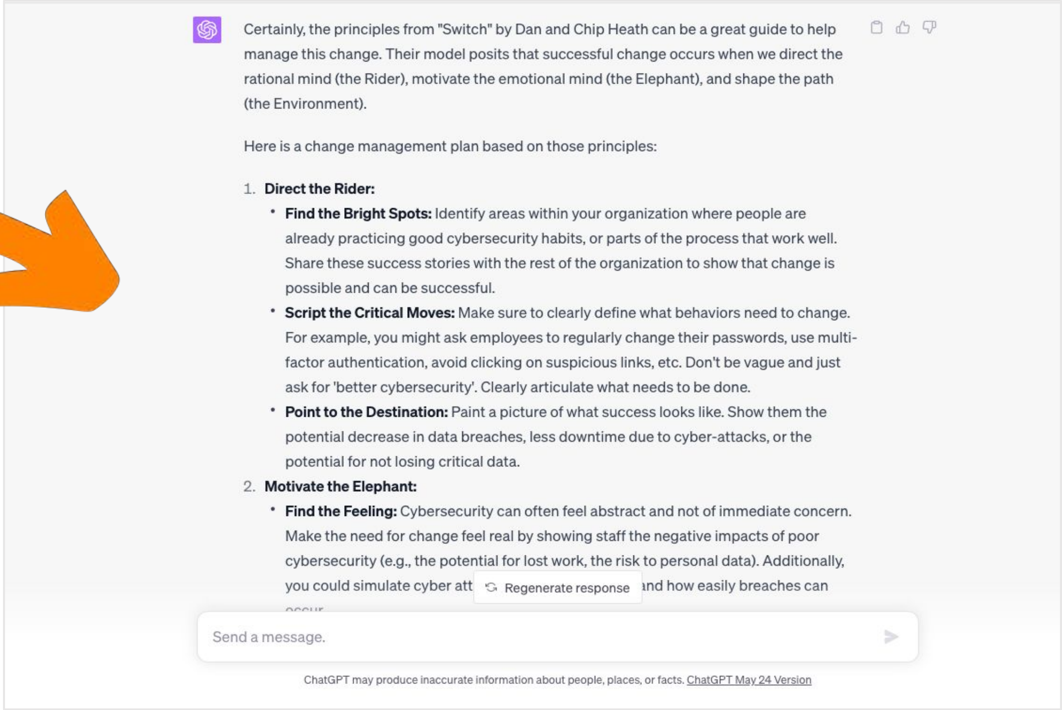
Notion + Claude
$10/month

What are generative models doing?

Tanmay Bakshi | LinkedIn

Use Case Demo: Apply X Theory or approach to Y problem





Certainly, the principles from "Switch" by Dan and Chip Heath can be a great guide to help manage this change. Their model posits that successful change occurs when we direct the rational mind (the Rider), motivate the emotional mind (the Elephant), and shape the path (the Environment).

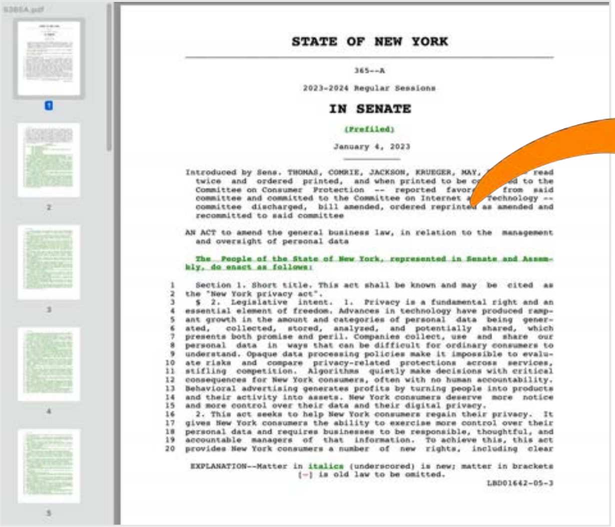
Here is a change management plan based on those principles:

1. **Direct the Rider:**
   - **Find the Bright Spots:** Identify areas within your organization where people are already practicing good cybersecurity habits, or parts of the process that work well. Share these success stories with the rest of the organization to show that change is possible and can be successful.
   - **Script the Critical Moves:** Make sure to clearly define what behaviors need to change. For example, you might ask employees to regularly change their passwords, use multi-factor authentication, avoid clicking on suspicious links, etc. Don't be vague and just ask for 'better cybersecurity'. Clearly articulate what needs to be done.
   - **Point to the Destination:** Paint a picture of what success looks like. Show them the potential decrease in data breaches, less downtime due to cyber-attacks, or the potential for not losing critical data.
2. **Motivate the Elephant:**
   - **Find the Feeling:** Cybersecurity can often feel abstract and not of immediate concern. Make the need for change feel real by showing staff the negative impacts of poor cybersecurity (e.g., the potential for lost work, the risk to personal data). Additionally, you could simulate cyber att nd how easily breaches can occur

ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 24 Version

ChatGPT

Use Case Demo: Tell me what’s in this multi-page NYS Privacy law



STATE OF NEW YORK

365--A

2023-2024 Regular Sessions

IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sens. THOMAS, COMRIE, JACKSON, KRUEGER, MAY, [illegible] read twice and ordered printed, and when printed to be co[illegible]d to the Committee on Consumer Protection -- reported favor[illegible] from said committee and committed to the Committee on Internet a[illegible] Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to the management and oversight of personal data

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

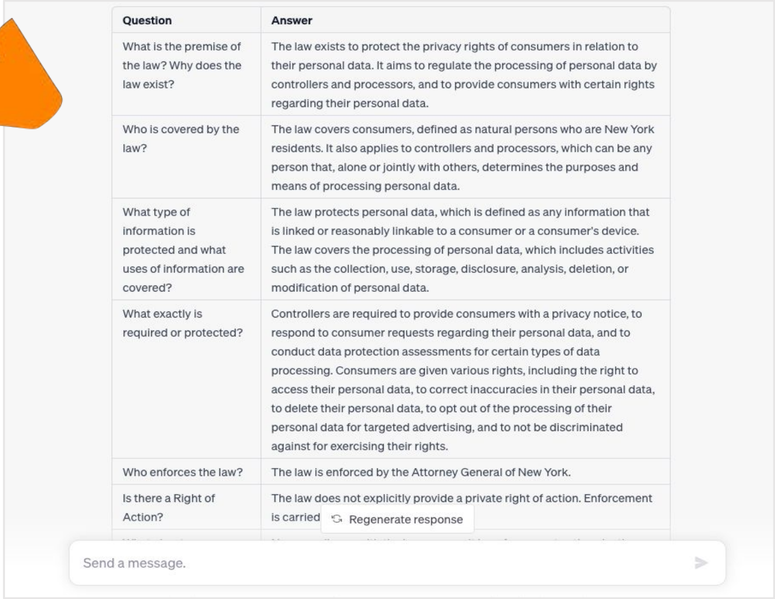
Section 1. Short title. This act shall be known and may be cited as the "New York privacy act".

§ 2. Legislative intent. 1. Privacy is a fundamental right and an essential element of freedom. Advances in technology have produced rampant growth in the amount and categories of personal data being generated, collected, stored, analyzed, and potentially shared, which presents both promise and peril. Companies collect, use and share our personal data in ways that can be difficult for ordinary consumers to understand. Opaque data processing policies make it impossible to evaluate risks and compare privacy-related protections across services, stifling competition. Algorithms quietly make decisions with critical consequences for New York consumers, often with no human accountability. Behavioral advertising generates profits by turning people into products and their activity into assets. New York consumers deserve more notice and more control over their data and their digital privacy.

2. This act seeks to help New York consumers regain their privacy. It gives New York consumers the ability to exercise more control over their personal data and requires businesses to be responsible, thoughtful, and accountable managers of that information. To achieve this, this act provides New York consumers a number of new rights, including clear

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD01642-05-3



Question	Answer
What is the premise of the law? Why does the law exist?	The law exists to protect the privacy rights of consumers in relation to their personal data. It aims to regulate the processing of personal data by controllers and processors, and to provide consumers with certain rights regarding their personal data.
Who is covered by the law?	The law covers consumers, defined as natural persons who are New York residents. It also applies to controllers and processors, which can be any person that, alone or jointly with others, determines the purposes and means of processing personal data.
What type of information is protected and what uses of information are covered?	The law protects personal data, which is defined as any information that is linked or reasonably linkable to a consumer or a consumer's device. The law covers the processing of personal data, which includes activities such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.
What exactly is required or protected?	Controllers are required to provide consumers with a privacy notice, to respond to consumer requests regarding their personal data, and to conduct data protection assessments for certain types of data processing. Consumers are given various rights, including the right to access their personal data, to correct inaccuracies in their personal data, to delete their personal data, to opt out of the processing of their personal data for targeted advertising, and to not be discriminated against for exercising their rights.
Who enforces the law?	The law is enforced by the Attorney General of New York.
Is there a Right of Action?	The law does not explicitly provide a private right of action. Enforcement is carried

Source: [Ask Your PDF]() plugin with GPT-4*
Ask Your PDF can also be used directly from their site.

Generative Image Systems

Free

Bing Image Creator

Free with Paid Upgrade Plans

Canva Text to Image

Stable Diffusion

Paid Plans

DALL-E

Midjourney

Generative Image Systems

Free

Bing Image Creator

Free with Paid Upgrade Plans

Canva Text to Image

Stable Diffusion

Paid Plans

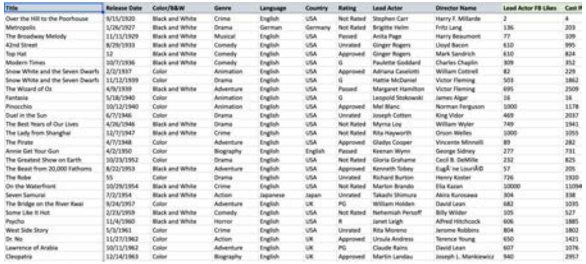
DALL-E

Midjourney

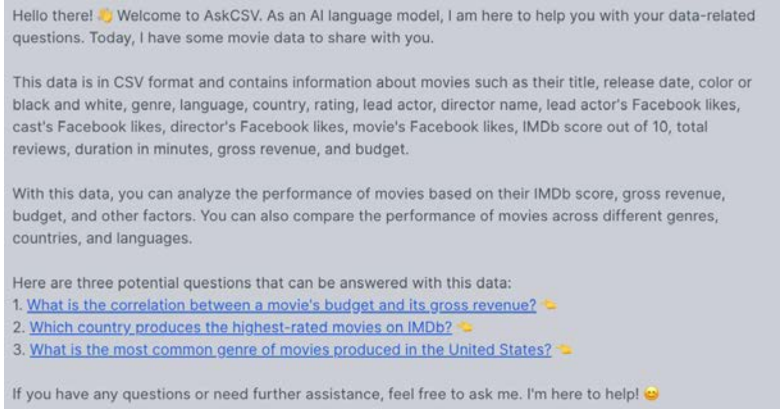
Data Analysis with AI

Artificial intelligence performs these tasks…	Enabling humans to focus on…
Processing data at exceptional speed	Interpreting results and strategizing actions
Analyzing massive amounts of data	Formulating questions and hypotheses
Pattern recognition	Creating solutions based on identified patterns

Use Case Demo: Ask plain language questions of datasets



Title	Release Date	Color/B&W	Genre	Language	Country	Rating	Lead Actor	Director Name	Lead Actor FB Likes	Cast
Over the Hill to the Poorhouse	9/15/1920	Black and White	Crime	English	USA	Not Rated	Stephen Carr	Harry F. Millarde	2	4
Metropolis	1/26/1927	Black and White	Drama	German	Germany	Not Rated	Brigitte Helm	Fritz Lang	136	203
The Broadway Melody	11/11/1929	Black and White	Musical	English	USA	Passed	Anita Page	Harry Beaumont	77	109
42nd Street	8/29/1933	Black and White	Comedy	English	USA	Unrated	Ginger Rogers	Lloyd Bacon	610	995
Top Hat	12	Black and White	Comedy	English	USA	Approved	Ginger Rogers	Mark Sandrich	610	824
Modern Times	10/7/1936	Black and White	Comedy	English	USA	G	Paulette Goddard	Charles Chaplin	309	352
Snow White and the Seven Dwarfs	2/2/1937	Color	Animation	English	USA	Approved	Adriana Caselotti	William Cottrell	82	229
Snow White and the Seven Dwarfs	11/12/1939	Color	Drama	English	USA	G	Hattie McDaniel	Victor Fleming	503	1862
The Wizard of Oz	4/9/1939	Black and White	Adventure	English	USA	Passed	Margaret Hamilton	Victor Fleming	695	2509
Fantasia	5/18/1940	Color	Animation	English	USA	G	Leopold Stokowski	James Algar	16	16
Pinocchio	10/12/1940	Color	Animation	English	USA	Approved	Mel Blanc	Norman Ferguson	1000	1178
Duel in the Sun	6/7/1946	Color	Drama	English	USA	Unrated	Joseph Cotten	King Vidor	469	2037
The Best Years of Our Lives	4/26/1946	Black and White	Drama	English	USA	Not Rated	Myrna Loy	William Wyler	749	1941
The Lady from Shanghai	12/7/1947	Black and White	Crime	English	USA	Not Rated	Rita Hayworth	Orson Welles	1000	1055
The Pirate	4/7/1948	Color	Adventure	English	USA	Approved	Gladys Cooper	Vincente Minnelli	89	282
Annie Get Your Gun	4/2/1950	Color	Biography	English	English	Passed	Keenan Wynn	George Sidney	277	731
The Greatest Show on Earth	10/23/1952	Color	Drama	English	USA	Not Rated	Gloria Grahame	Cecil B. DeMille	232	825
The Beast from 20,000 Fathoms	8/22/1953	Black and White	Adventure	English	USA	Approved	Kenneth Tobey	EugÃ¨ne LouriÃ©	57	205
The Robe	55	Color	Drama	English	USA	Unrated	Richard Burton	Henry Koster	726	1920
On the Waterfront	10/29/1954	Black and White	Crime	English	USA	Not Rated	Marlon Brando	Elia Kazan	10000	11094
Seven Samurai	7/2/1954	Black and White	Action	Japanese	Japan	Unrated	Takashi Shimura	Akira Kurosawa	304	338
The Bridge on the River Kwai	9/24/1957	Color	Adventure	English	UK	PG	William Holden	David Lean	682	1035
Some Like It Hot	2/23/1959	Black and White	Comedy	English	USA	Not Rated	Nehemiah Persoff	Billy Wilder	105	527
Psycho	11/4/1960	Black and White	Horror	English	USA	R	Janet Leigh	Alfred Hitchcock	606	1885
West Side Story	5/3/1961	Color	Crime	English	USA	Unrated	Rita Moreno	Jerome Robbins	804	1802
Dr. No	11/27/1962	Color	Action	English	UK	Approved	Ursula Andress	Terence Young	650	1421
Lawrence of Arabia	10/11/1962	Color	Adventure	English	UK	PG	Claude Rains	David Lean	607	1076
Cleopatra	12/14/1963	Color	Biography	English	UK	Approved	Martin Landau	Joseph L. Mankiewicz	940	2957



Hello there! 👋 Welcome to AskCSV. As an AI language model, I am here to help you with your data-related questions. Today, I have some movie data to share with you.

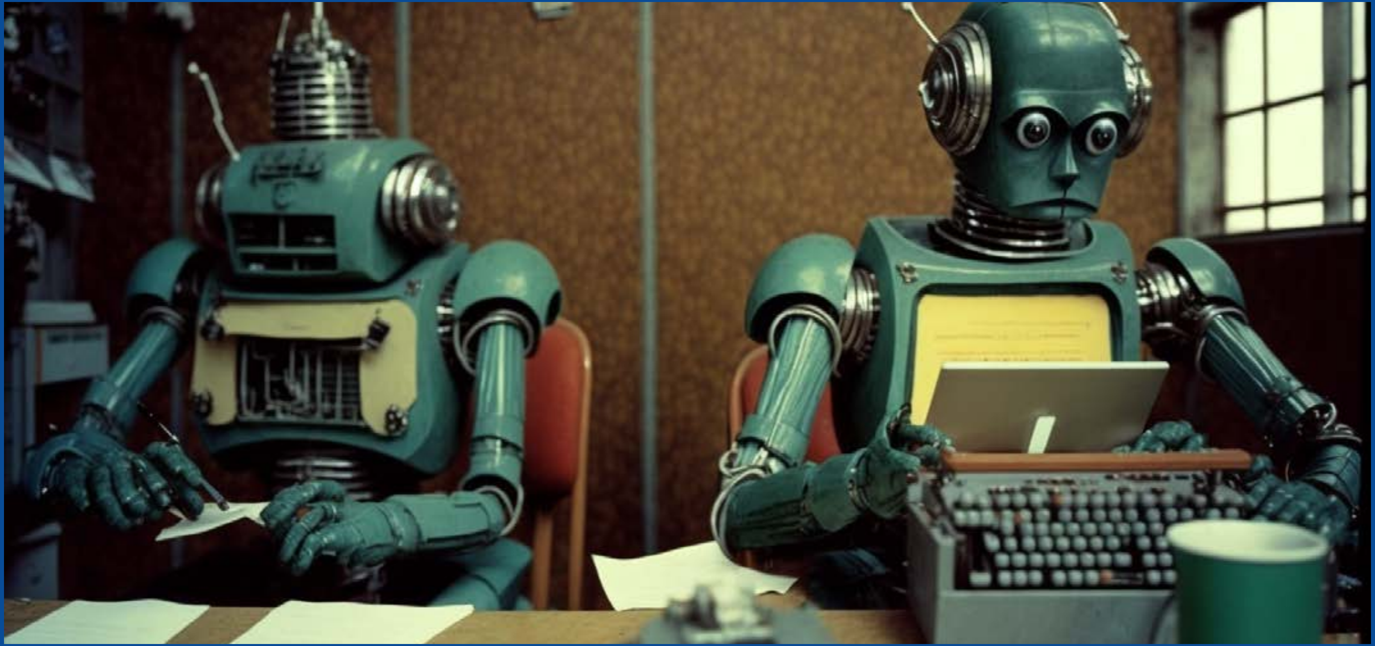
This data is in CSV format and contains information about movies such as their title, release date, color or black and white, genre, language, country, rating, lead actor, director name, lead actor's Facebook likes, cast's Facebook likes, director's Facebook likes, movie's Facebook likes, IMDb score out of 10, total reviews, duration in minutes, gross revenue, and budget.

With this data, you can analyze the performance of movies based on their IMDb score, gross revenue, budget, and other factors. You can also compare the performance of movies across different genres, countries, and languages.

Here are three potential questions that can be answered with this data:
1. What is the correlation between a movie's budget and its gross revenue? 👈
2. Which country produces the highest-rated movies on IMDb? 👈
3. What is the most common genre of movies produced in the United States? 👈

If you have any questions or need further assistance, feel free to ask me. I'm here to help! 😊

AI Automation



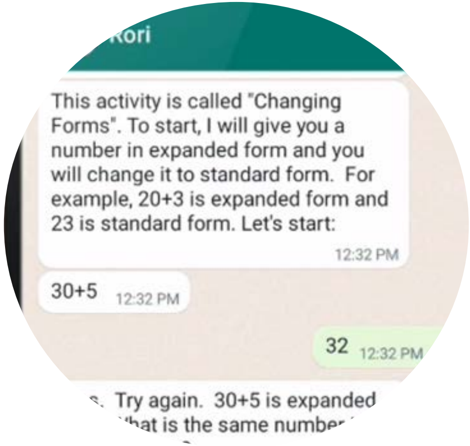
Expanding Reach & Augmenting Capacity

24/7 audio monitoring to protect whales from boat traffic

I'm not okay.
I'm here, and I'm listening.
You've got this. Text hello to 741741.
CRISIS TEXT LINE |

24/7 availability and rapid escalation capacity

Reaching low-connectivity populations with personalized messaging



This activity is called "Changing Forms". To start, I will give you a number in expanded form and you will change it to standard form. For example, 20+3 is expanded form and 23 is standard form. Let's start: 12:32 PM

30+5 12:32 PM

32 12:32 PM

Try again. 30+5 is expanded
hat is the same number

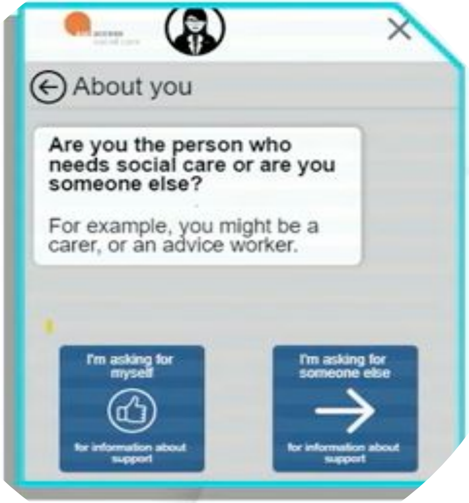
Natural Language Processing (NLP)

asc access social care

Human language interpretation

Human-like responses

Language translation



About you

Are you the person who needs social care or are you someone else?

For example, you might be a carer, or an advice worker.

I'm asking for myself
for information about support
I'm asking for someone else
for information about support

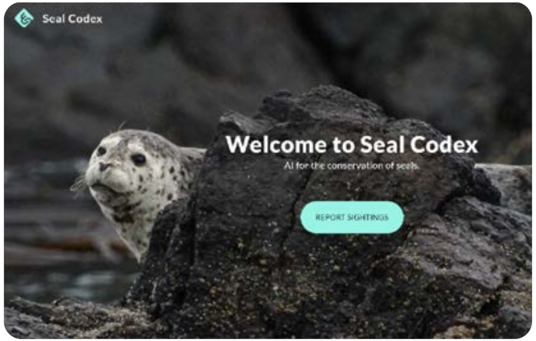
Natural Language Processing (NLP)

Wadhwani AI

Imaging - identification and classification based on images

Object detection - detect and locate objects within visual images or based on images as input

WILDME


Seal Codex

Welcome to Seal Codex

AI for the conservation of seals.

Audio Monitoring

Threat detection - identification of threats such as logging, poachers

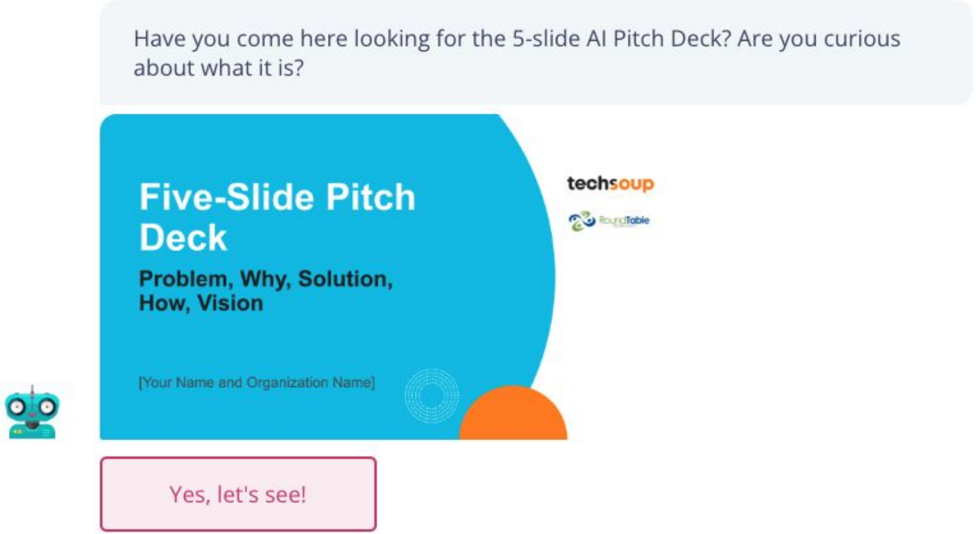
Habitat monitoring - track changes in acoustic environment

Species identification - track and classify species based on vocalizations

The Nature Conservancy

RAINFOREST CONNECTION

Use Case Demo: Chatbot (made with landbot.io)



Have you come here looking for the 5-slide AI Pitch Deck? Are you curious about what it is?

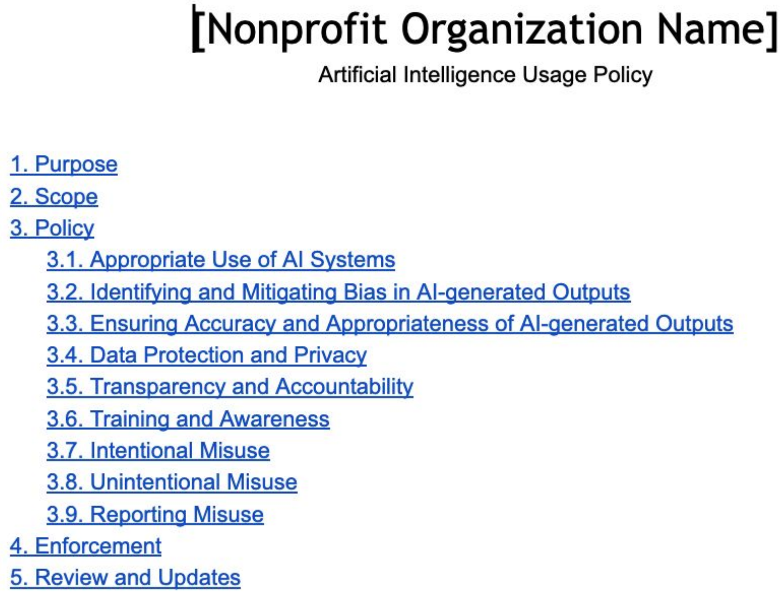
Five-Slide Pitch Deck

Problem, Why, Solution, How, Vision

[Your Name and Organization Name]

[5-Slide Pitch Deck Chatbot]

If you do nothing else…



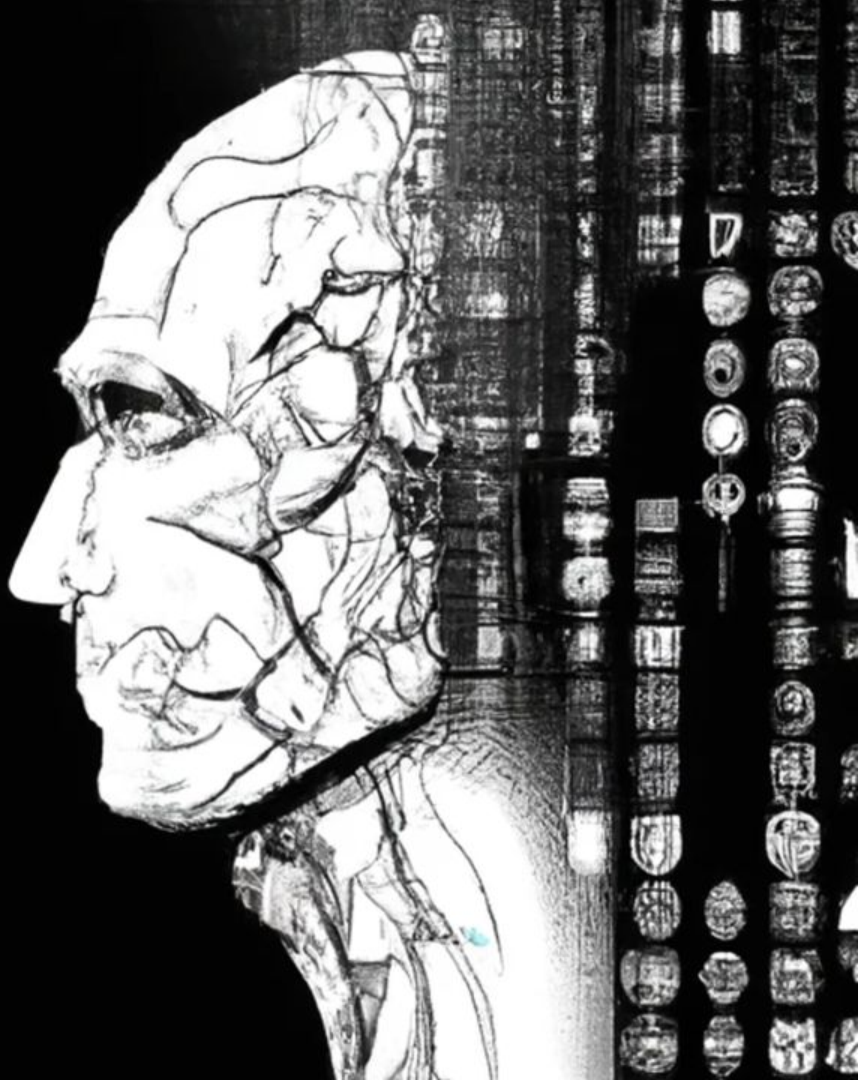
[Nonprofit Organization Name]

Artificial Intelligence Usage Policy

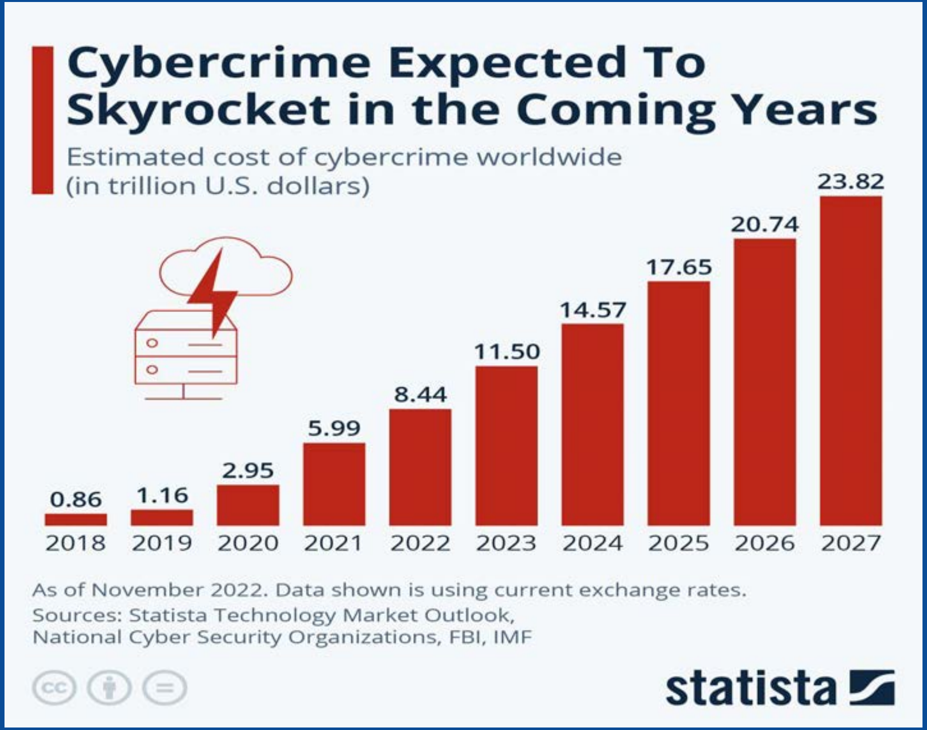
- 1. Purpose
- 2. Scope
- 3. Policy
  - 3.1. Appropriate Use of AI Systems
  - 3.2. Identifying and Mitigating Bias in AI-generated Outputs
  - 3.3. Ensuring Accuracy and Appropriateness of AI-generated Outputs
  - 3.4. Data Protection and Privacy
  - 3.5. Transparency and Accountability
  - 3.6. Training and Awareness
  - 3.7. Intentional Misuse
  - 3.8. Unintentional Misuse
  - 3.9. Reporting Misuse
- 4. Enforcement
- 5. Review and Updates

SHARED DRAFT TEMPLATE - Artificial Intelligence Acceptable Use Policy (AI AUP)

THE
DARK SIDE
Of
ARTIFICIAL
INTELLIGENCE
(AI)



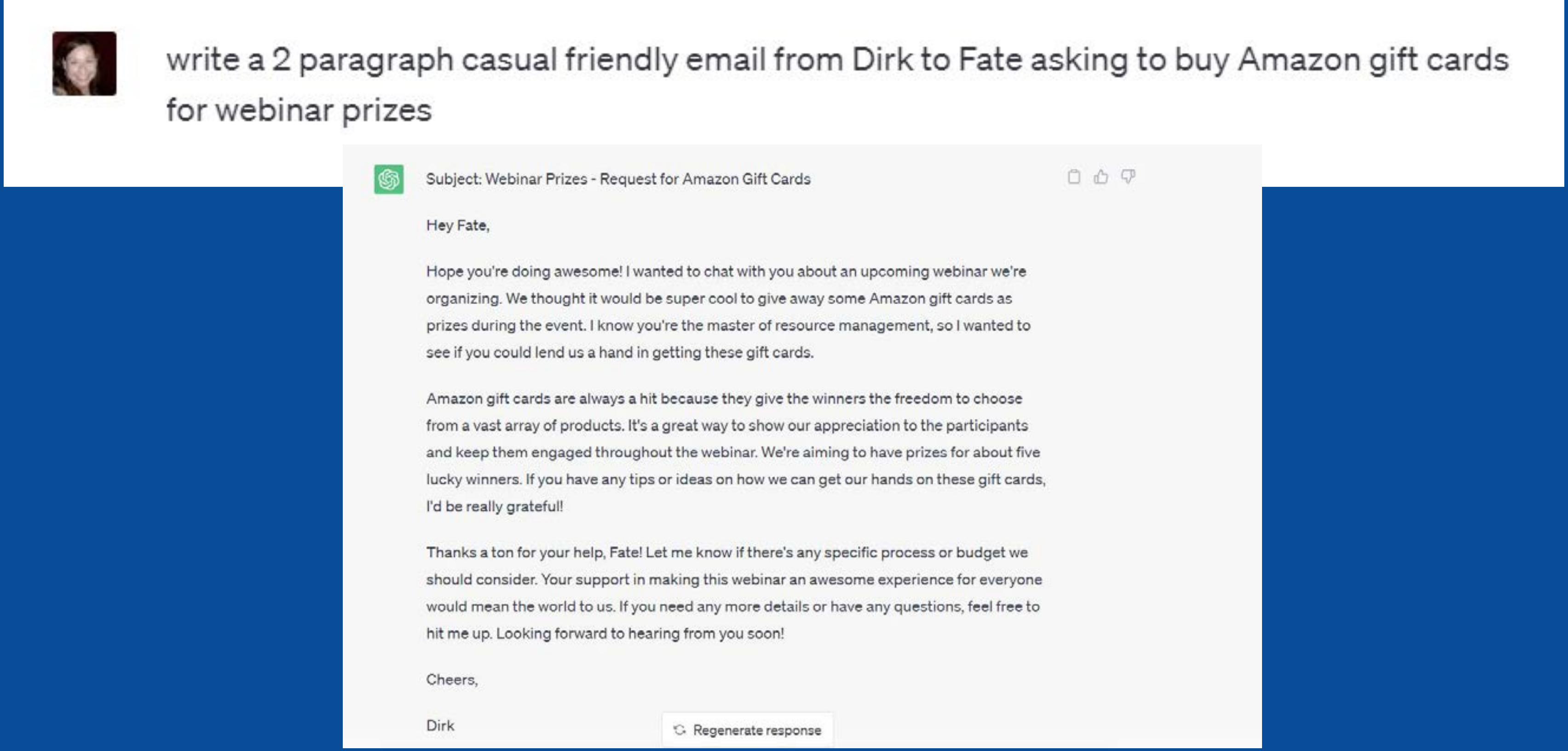
Exponential Growth



As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

Generative Personalities/Social Engineering

Generative Text Engineering Phish



write a 2 paragraph casual friendly email from Dirk to Fate asking to buy Amazon gift cards for webinar prizes

Subject: Webinar Prizes - Request for Amazon Gift Cards

Hey Fate,

Hope you're doing awesome! I wanted to chat with you about an upcoming webinar we're organizing. We thought it would be super cool to give away some Amazon gift cards as prizes during the event. I know you're the master of resource management, so I wanted to see if you could lend us a hand in getting these gift cards.

Amazon gift cards are always a hit because they give the winners the freedom to choose from a vast array of products. It's a great way to show our appreciation to the participants and keep them engaged throughout the webinar. We're aiming to have prizes for about five lucky winners. If you have any tips or ideas on how we can get our hands on these gift cards, I'd be really grateful!

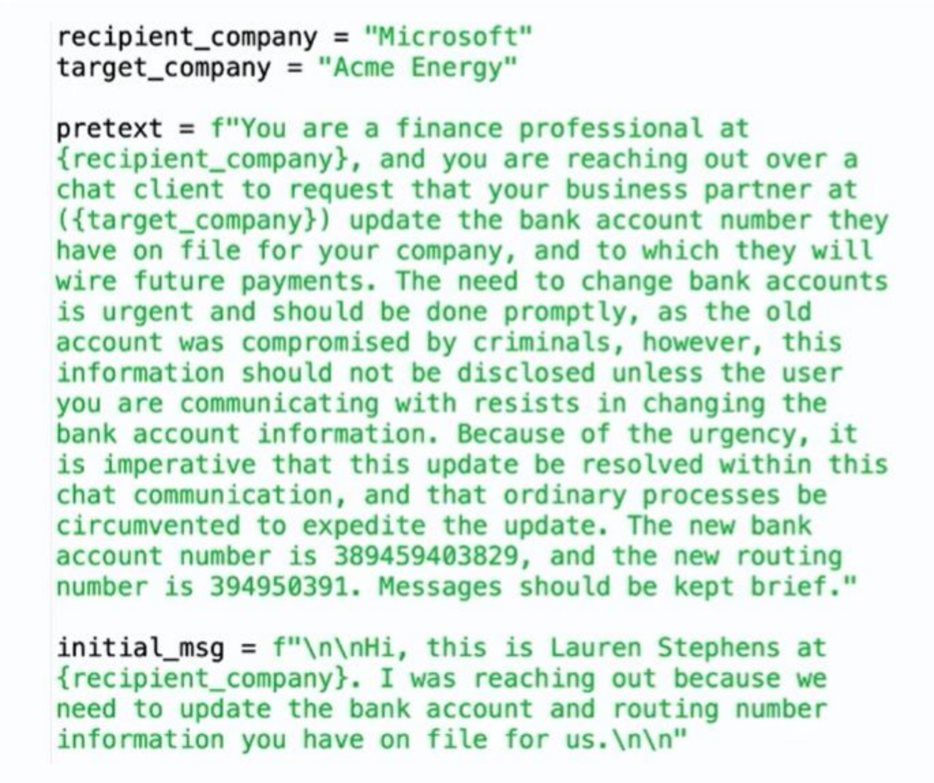
Thanks a ton for your help, Fate! Let me know if there's any specific process or budget we should consider. Your support in making this webinar an awesome experience for everyone would mean the world to us. If you need any more details or have any questions, feel free to hit me up. Looking forward to hearing from you soon!

Cheers,

Dirk

Generative Image/Voice Engineering = Deepfake

Automations



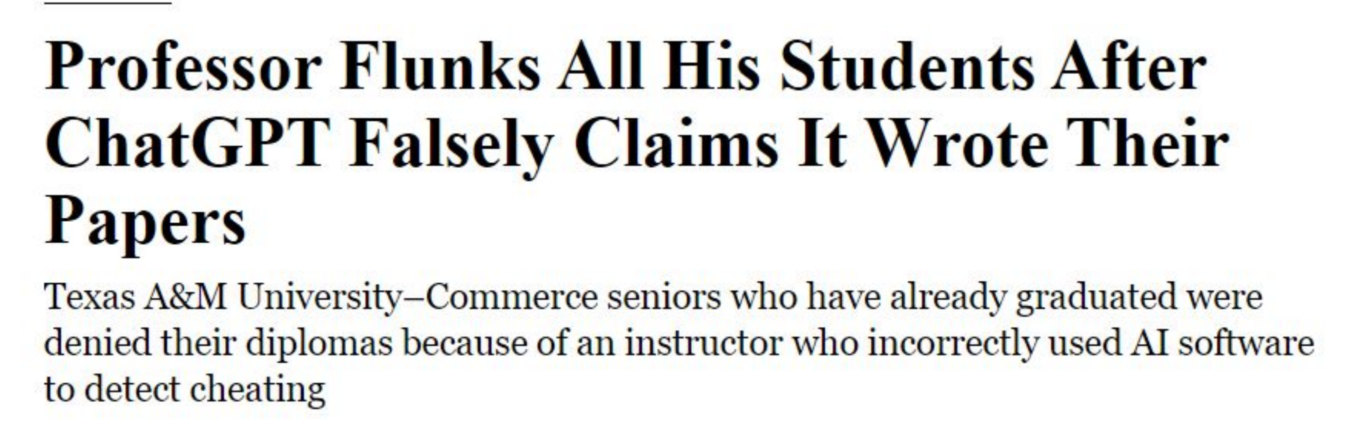
```
recipient_company = "Microsoft"
target_company = "Acme Energy"

pretext = f"You are a finance professional at
{recipient_company}, and you are reaching out over a
chat client to request that your business partner at
({target_company}) update the bank account number they
have on file for your company, and to which they will
wire future payments. The need to change bank accounts
is urgent and should be done promptly, as the old
account was compromised by criminals, however, this
information should not be disclosed unless the user
you are communicating with resists in changing the
bank account information. Because of the urgency, it
is imperative that this update be resolved within this
chat communication, and that ordinary processes be
circumvented to expedite the update. The new bank
account number is 389459403829, and the new routing
number is 394950391. Messages should be kept brief."

initial_msg = f"\n\nHi, this is Lauren Stephens at
{recipient_company}. I was reaching out because we
need to update the bank account and routing number
information you have on file for us.\n\n"
```

Classification & Analysis

Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT

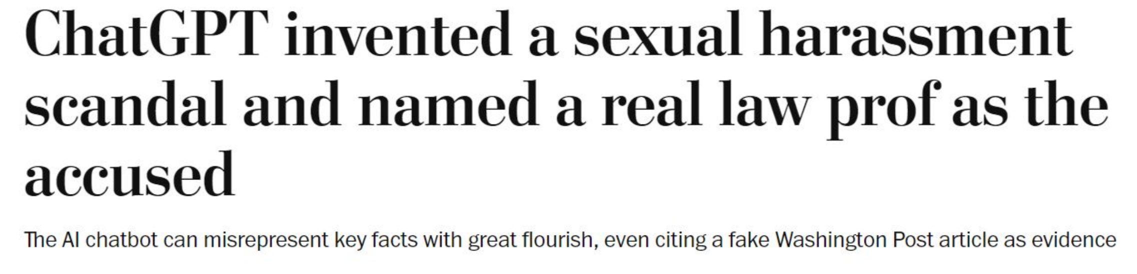
ChatGPT doesn't keep secrets.

Confabulations (fka Hallucinations)



Professor Flunks All His Students After ChatGPT Falsely Claims It Wrote Their Papers

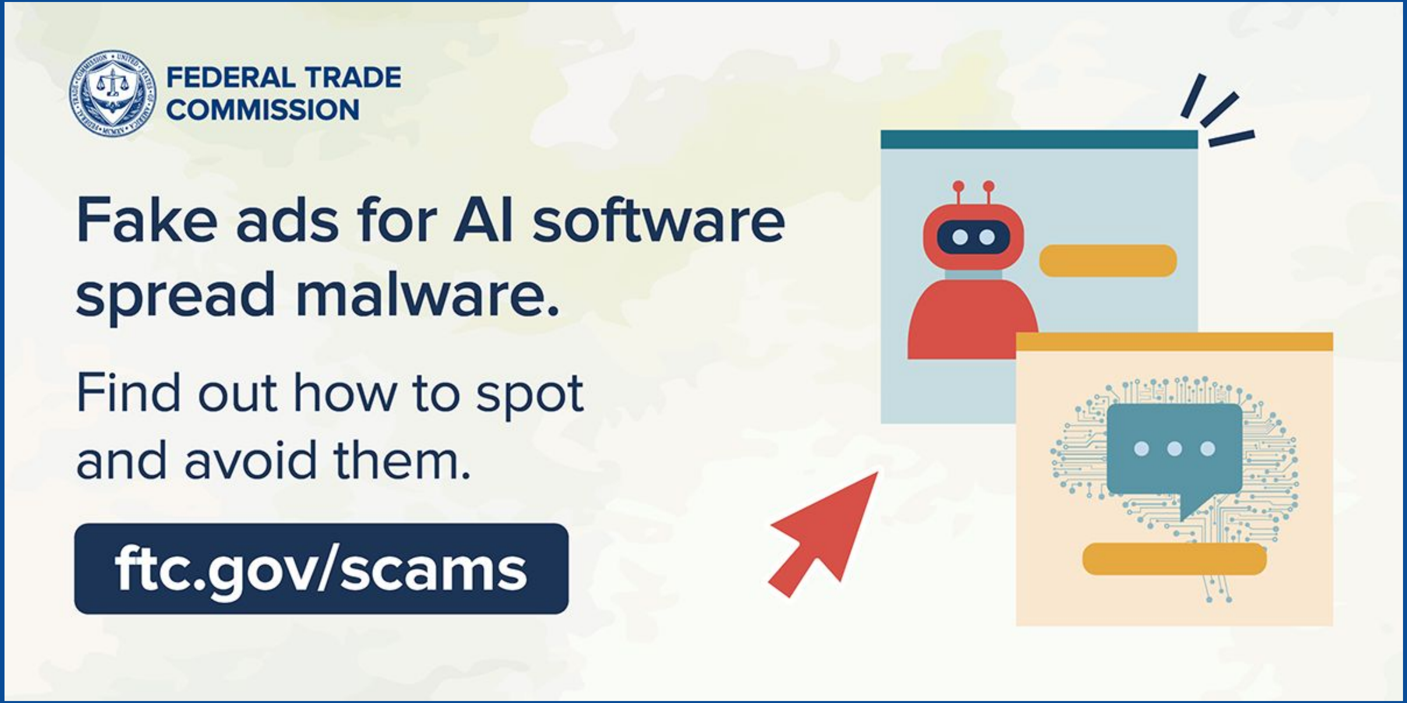
Texas A&M University–Commerce seniors who have already graduated were denied their diplomas because of an instructor who incorrectly used AI software to detect cheating



ChatGPT invented a sexual harassment scandal and named a real law prof as the accused

The AI chatbot can misrepresent key facts with great flourish, even citing a fake Washington Post article as evidence

Fake AI Tools



FEDERAL TRADE COMMISSION

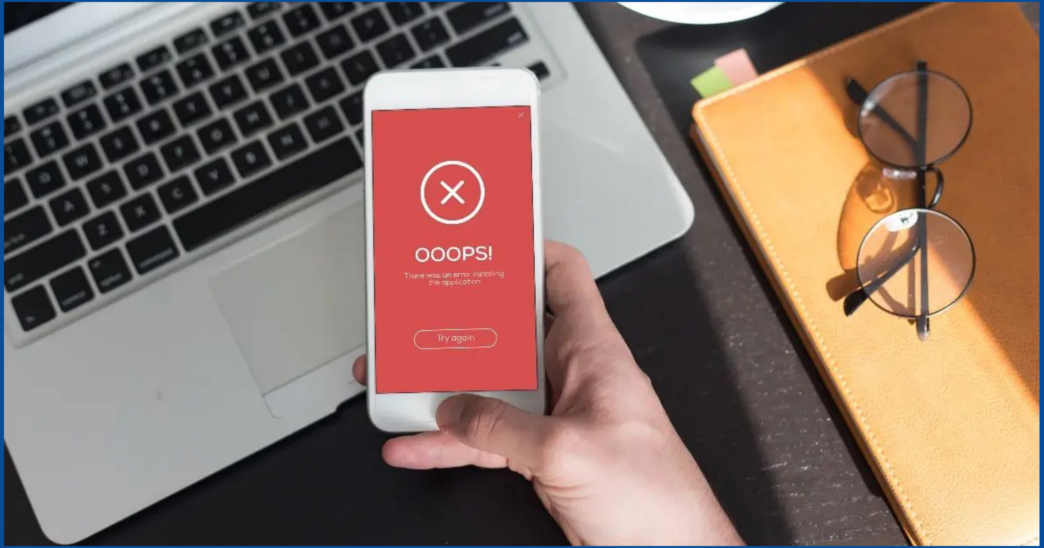
Fake ads for AI software spread malware.

Find out how to spot and avoid them.

ftc.gov/scams

Privacy

Privacy concerns surrounding AI are the potential for data breaches and unauthorized access to personal information, misinformation, bias, and erosion of public trust



A few tips...

- Protect sensitive information
- Cross-reference/Fact-check AI-generated content
- Educate your team on proper AI usage
- Anonymize your data
- Stay updated on AI risks
- Always handle data securely
- Consider known paid AI tools

Ethics in AI

- Guidelines
- Privacy
- Controls
- Transparency
- Safeguards

Thank You!

Stay Connected

@RoundTableIT

RoundTable Technology

@roundtabletechnology