

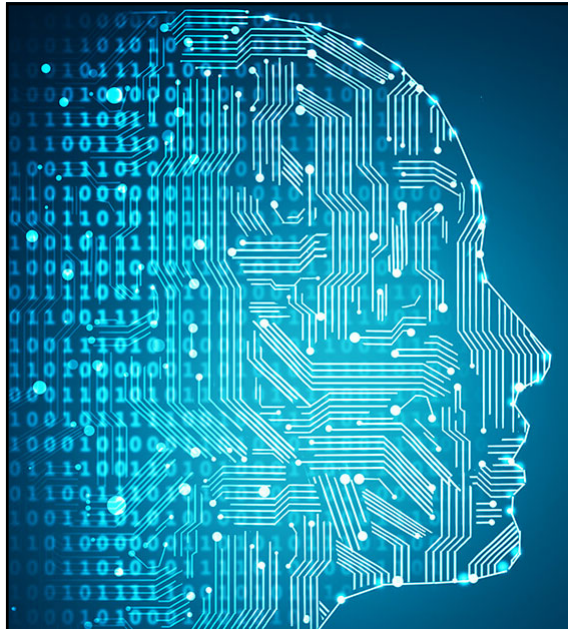


# What is AI

**By: Amin Jamili**

Main Reference: Andrew NG Course

[deeplearning.ai](https://deeplearning.ai)



# What is AI

## Introduction

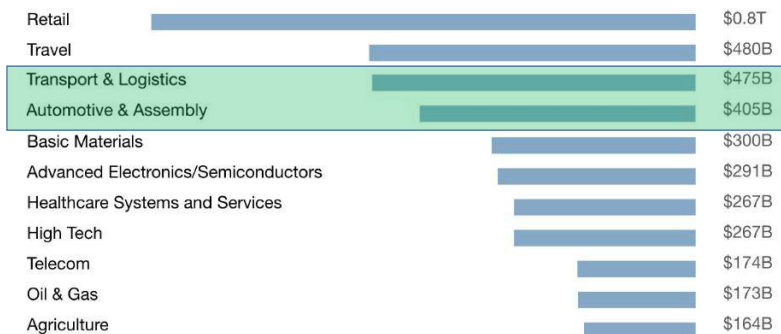
### What is AI- Part 1

in abstract

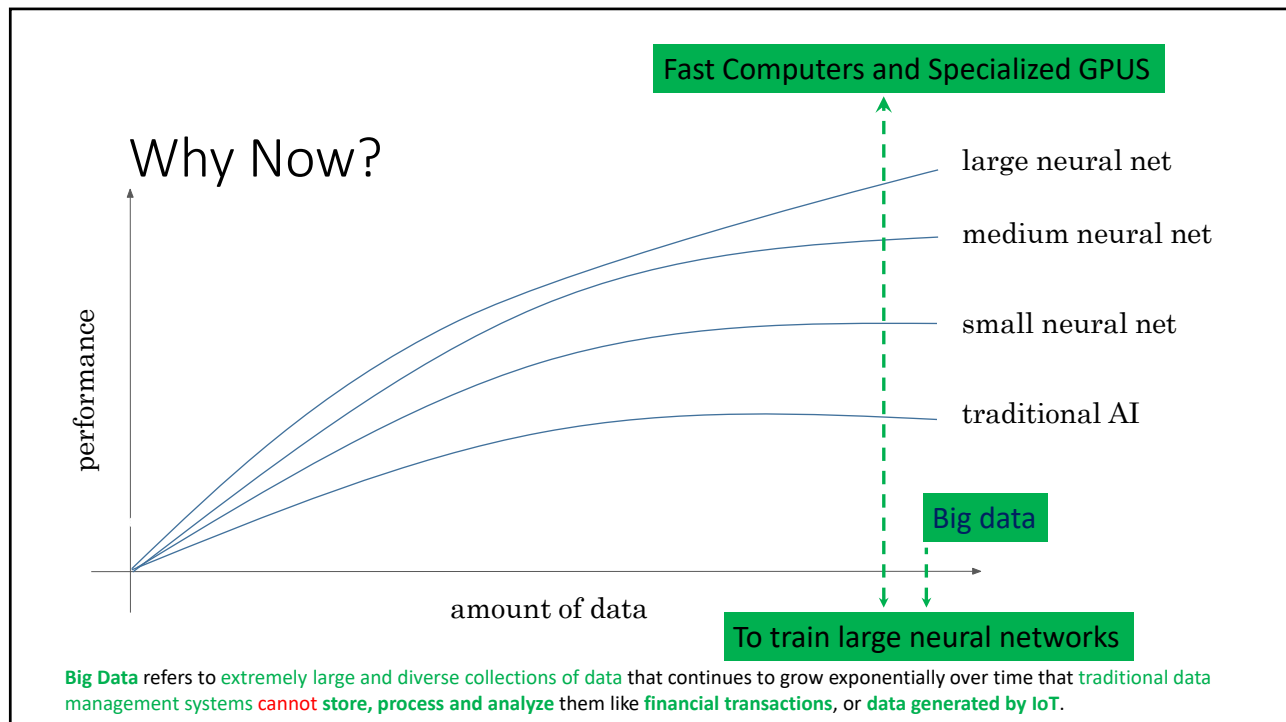
## Introduction

AI value creation  
by 2030

**\$13  
trillion**



[Source: McKinsey Global Institute.]



## CPU vs. GPU

**CPU: Computer processor:** A Central Processing Unit, often compared to the “**brains**” of a device.

**GPU: Graphics Processing Unit**

Historically is used for processing pictures, and rendering images and video but not it is demonstrated that it is highly useful for building very large NNs.



**GPU cores are less powerful than CPU cores and have less memory.** While CPUs can switch between different instruction sets rapidly.

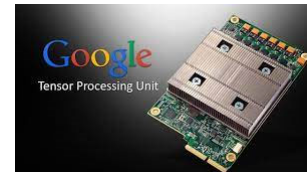
A GPU uses more power as compared to a CPU for the simple reason that a **GPU has many more cores than a CPU and uses parallel processing.**

A GPU simply takes a high volume of the same instructions and pushes them through at high speed.

# TPU

## TPU: **Tensor Processing Unit.**

TPU is Google's application-specific integrated circuit (ASIC) for deep learning and machine learning. Unlike other general processors like CPU and GPU, Google has developed matrix processor TPU for neural network workloads and machine learning for its TensorFlow software.



## Cloud vs. On-premises

Edge deployment (e.g. self driving car) the computation should be done where the data is collected to improve the response time.



# A lesson from the rise of the Internet

## Internet Era



## AI era

Shopping mall + website  
≠ Internet company

- A/B testing To measure the function of two different websites
- Short iteration time Making changes on sales methods, etc., very fast
- Decision making pushed down to engineers and other specialized roles Rather than the CEOs

Any company + deep learning  
≠ AI company

- Strategic data acquisition
- Unified data warehouse
- Pervasive automation
- New roles (e.g., MLE) and division of labor



# What is AI

Data

What is AI- Part 1

in abstract

## Acquiring data

### - Manual labeling



cat



not  
cat



cat



not  
cat

### - From observing user behaviors

user ID	time	price (\$)	purchased
4783	Jan 21 08:15.20	7.95	yes
3893	March 3 11:30.15	10.00	yes
8384	June 11 14:15.05	9.50	no
0931	Aug 2 20:30.55	12.90	yes

machine	temperature (°C)	pressure (psi)	machine fault
17987	60	7.65	N
34672	100	25.50	N
08542	140	75.50	Y
98536	165	125.00	Y

### - Download from websites / partnerships

## Data is messy

- Garbage in, garbage out

- Data problems

- Incorrect labels
- Missing values



ok



defect



ok



ok



defect



ok

• Mislabeled data

• Ambiguous label

## Data Cleaning Techniques

1. Clear formatting

2. Remove irrelevant data

3. Remove duplicates

4. Filter missing values

you can either delete the observations that have missing values or you can fill in the missing values.

5. Delete outliers

6. Convert data type

7. Standardize capitalization

8. Structural consistency

For example, terms like "Not Applicable" and "N/A", must be written in a consistent manner.

9. Uniform language

10. Validate the data






What is AI- Part 1  
in abstract

# What is AI

The terminology of AI

## Examples of Machine Learning (Supervised Learning)

Input (A) 	Output (B)	Application
email	spam? (0/1)	spam filtering
audio	text transcripts	speech recognition
English	Chinese	machine translation
ad, user info	click? (0/1)	online advertising
image, radar info	position of other cars	Self-driving car
image of phone	defect? (0/1)	visual inspection

## Computer Vision

- Image classification/Object recognition

- Face recognition



cat

register



new



✓



- Object detection



- Image segmentation



- Tracking moving objects in videos



## Natural Language Processing

- Text classification

- Sentiment recognition

Email → Spam/Non-Spam

Product description → Product category

“The food was good” → ★★★★★

“Service was horrible” → ★

- Name entity recognition

“Queen Elizabeth II knighted

Sir Paul McCartney for his services

to music at the Buckingham Palace.”

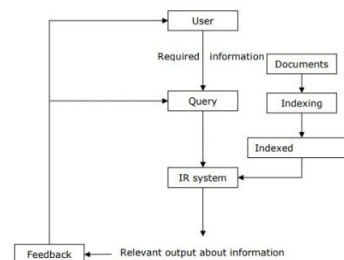
- Machine translation

AIは、新たな電気だ

AI is the new electricity

- Information retrieval

- E.g., web search

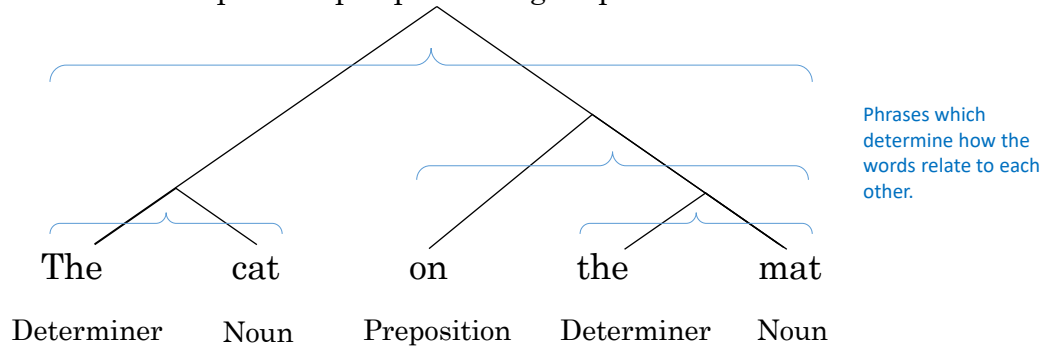




## Natural Language Processing

- Others: parsing, part-of-speech tagging

**Goal:** to figure out which of the words to pay more attention to. It is an important pre-processing step.



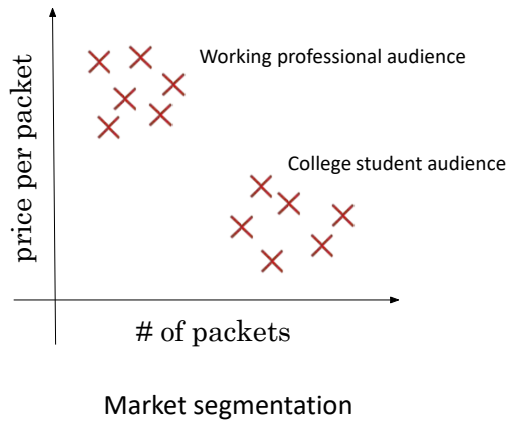
Speech



- Speech recognition (speech-to-text)
- Trigger word/wakeword detection
- Speaker ID:** verify the IDs by listening to someone speaks.
- Speech synthesis (text-to-speech, TTS)**  
The quick brown fox jumps over the lazy dog.

# Unsupervised learning

## Clustering Potato chip sales

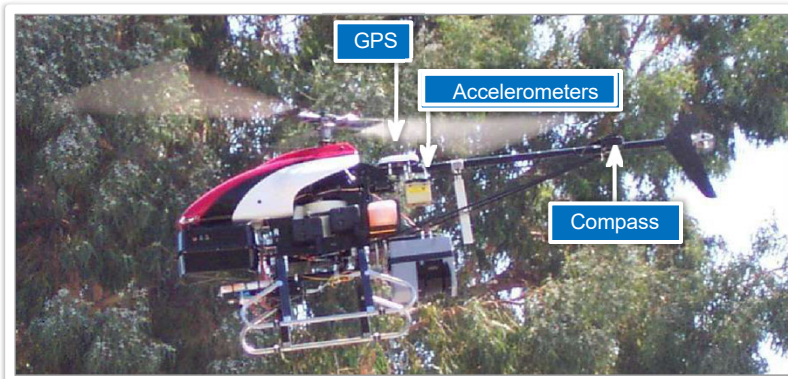


Given data (without any specific desired output labels), find something interesting about the data



Finding cats from unlabeled YouTube videos

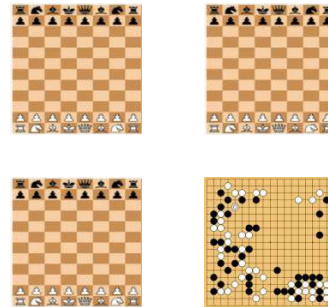
# Reinforcement learning



One may think of reinforcement learning as similar to how you might train a pet dog. So in this case you may **let the dog do whatever it wanted to do** and then whenever it behaved well we'll freeze it you say **good dog** and whenever it does something bad you would say **bad dog** and **over time it learns to do more of the good dog things and fewer of the bad dog things.** Reinforcement learning takes the same principle!

Use a “reward signal” to tell the AI when it is doing well or poorly. It automatically learns to maximize its rewards.

# Reinforcement learning



Use a “reward signal” to tell the AI when it is doing well or poorly. It automatically learns to maximize its rewards.

## GANs (Generative Adversarial Network)

Synthesize new images from scratch

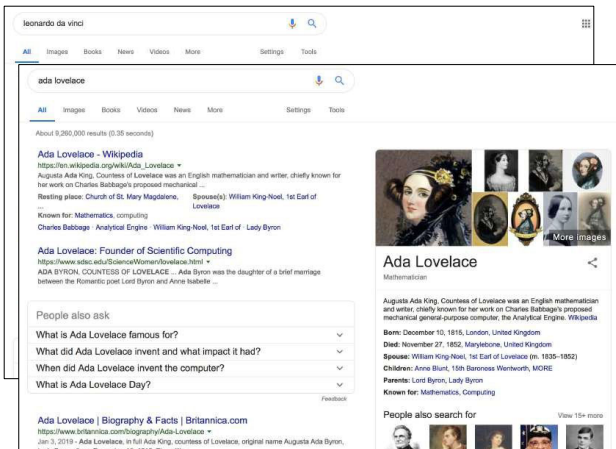
A **generative adversarial network (GAN)** is a class of machine learning frameworks and a prominent framework for approaching generative artificial intelligence. In a GAN, two **neural networks contest with each other** in the form of a zero-sum game, where one agent's gain is another agent's loss.

Given a training set, this technique learns to generate new data with the same statistics as the training set. For example, a GAN trained on photographs can generate new photographs that look at least superficially authentic to human observers, having many realistic characteristics.



[Source: Karras et al. (2018). Progressive Growing of GANs for Improved Quality, Stability, and Variation]

## Knowledge Graph



This information is drawn from a knowledge graph which basically means a database that lists people and key information about these people.

Ada Lovelace	
Born	Dec 10, 1815
Died	Nov 27, 1852
Bio	English mathematician and writer...

Northern Rooster Hotel	
Address	45 Rooster St, LA
Phone	(650) 555-3992
Wifi	yes
Pool	no

## Machine learning vs. Data science

Input:

Home prices

size (square feet)	# of bedrooms	# of bathrooms	newly renovated	price (1000\$)
523	1	2	N	100
645	1	3	N	150
708	2	1	N	200
1034	3	3	Y	300
2290	4	4	N	350
2545	4	5	Y	440

Output: Running AI system  
(e.g., websites / mobile app)

Homes with 3 bedrooms are more expensive than homes with 2 bedrooms of a similar size.

Newly renovated homes have a 15% premium.

# Machine learning vs. data science

## Machine learning

“Field of study that gives computers the ability to learn **without being explicitly programmed.**”

-Arthur Samuel (1959)



It results software.  
(e.g. the **Ads Software in YouTube**)

## Data science

Science of **extracting knowledge and insights from data.**



It results slide deck, e.g. PowerPoints. (e.g. The **sales team should focus more to** travel industries to have more impact ...)

## Key steps of a **data science** project

### *Example: Manufacturing line*

Mix clay



Shape mug



Add glaze



Fire kiln



Final inspection



Clay Batch #	Supplier	Mixing time (minutes)
001	ClayCo	35
034	GooClay	22
109	BrownStuff	28

1. **Collect data**

2. **Analyze data**

Iterate many times to get good insight

3. **Suggest hypotheses/actions**

Deploy changes

Re-analyze new data periodically

Mug Batch #	Country	Humidity	Temperature in kiln (F)	Duration in kiln (hours)
301	Spain	0.002%	1410°	22
302	USA	0.003%	1520°	24
303	Malaysia	0.002%	1420°	22

## Key steps of a **data science** project

### *Example: Optimizing a sales funnel*

1. Collect data

User ID	Country	Time	Webpage
2009	Spain	08:34:30 Jan 5	home.html
2897	USA	13:20:22 May 18	redmug.html
4893	Philippines	22:45:16 Jun 11	mug.html

2. Analyze data

Iterate many times to get good insights

3. Suggest hypotheses/actions

Deploy changes

Re-analyze new data periodically



## Key steps of a **machine learning** project

### *Example: Speech recognition like Echo / Alexa*

1. Collect data

2. Train model

Iterate many times until good enough

→ Fine-Tuning or adapting the Model

3. Deploy model (Experimentally)

Get data back (Voice recognition with UK accent)

Maintain / update model



Amazon  
Echo / Alexa



Apple  
Siri



## *“Hey device, tell me a joke”*

### Steps to process the command:

1. **Trigger word/wakeword detection** Audio → “Hey device”? (0/1) Output
2. **Speech recognition** Audio → “tell me a joke” Mapping audio to a text transcript
3. **Intent recognition** “tell me a joke” → {joke?, time?, music?, call?, weather?}
4. **Execute joke** Map to one of those limited defined intents or commands.  
 here'll be a software engineer that has written a piece of code to randomly select a joke and to play the joke back through the speaker.

A. AG Joke: why are there so many shocking results in AI because AI is the new electricity

## Key steps of a **machine learning** project

### *Example: Self-driving car*

1. **Collect data** image → position of other cars



2. **Train model**

Iterate many times until good enough

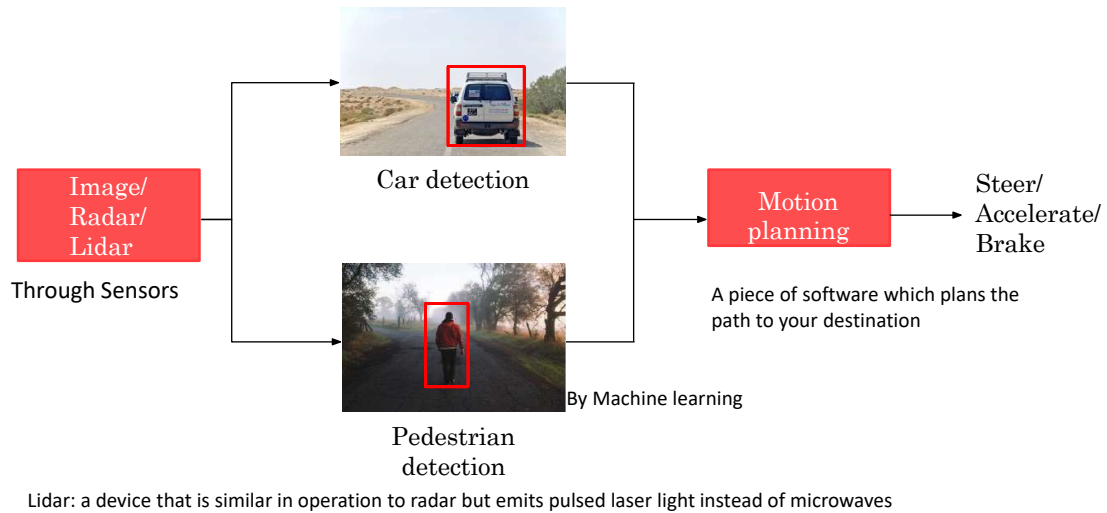


3. **Deploy model**

Get data back (e.g. Golf cars can be detected correctly)  
Maintain / update model



## Steps for deciding how to drive

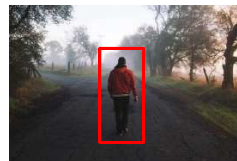


### Key steps:

1. Car detection



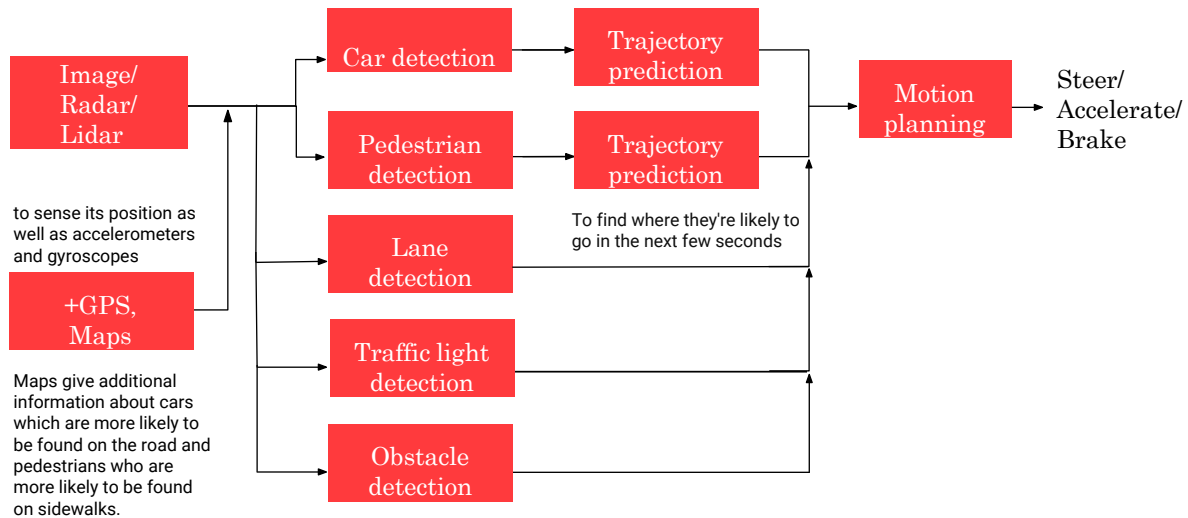
2. Pedestrian detection



3. Motion planning



## Steps for deciding how to drive



## Manufacturing line manager

### Data science



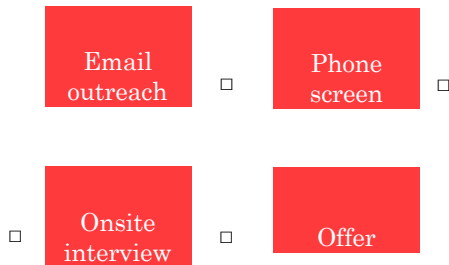
### Machine learning



### Automated visual inspection

## Recruiting

### Data science



Optimize recruiting funnel

### Machine learning

Jane Doe	
Personal Info	
Education	
Professional	
Employment	

☐ Yes

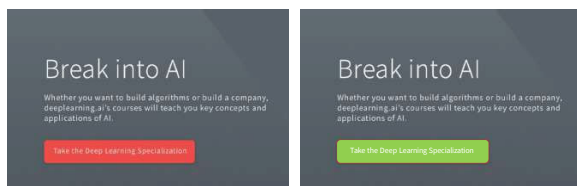
Tiffany Doe	
Personal Info	
Education	
Professional	
Employment	

☐ No

Automated resume screening

## Marketing

### Data science



A

B

A/B testing

### Machine learning

Recommended for you



Customized product recommendation

## Agriculture

### Data science



### Crop analytics

Today farmers are already using data science for crop analytics where you can take data on the soil conditions, the weather conditions, the prices of different crops in the market and have data science teams make recommendations to what to plant when to plant and so on.

### Machine learning



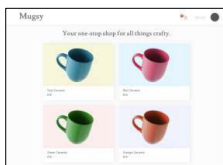
### Precision weed killing

To increase both helping farmers increase crop use and preserve the environment

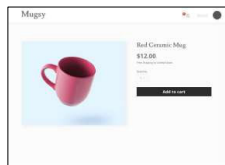
## Sales

### Data science

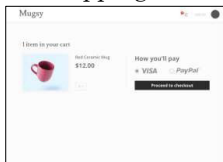
#### Visit website



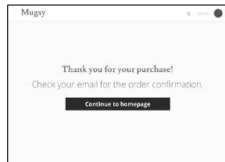
#### Product page



#### Shopping cart



#### Checkout



### Optimize sales funnel

### Machine learning

Name	Title	Company size	Email	Priority
Tayler	CEO	3050	tay@a..	high
Janet	Manager	230	jan@b..	medium
David	Intern	30	dave@c..	low

### Automated lead sorting

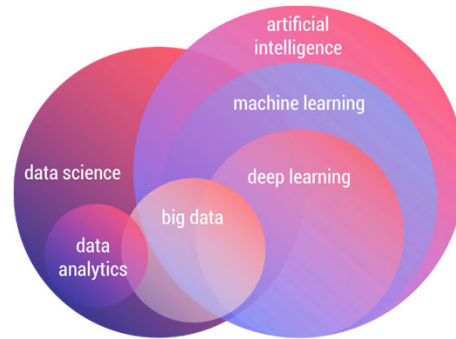
## AI has many tools

Machine learning and data science

-Deep learning / neural network

-Other buzzwords:

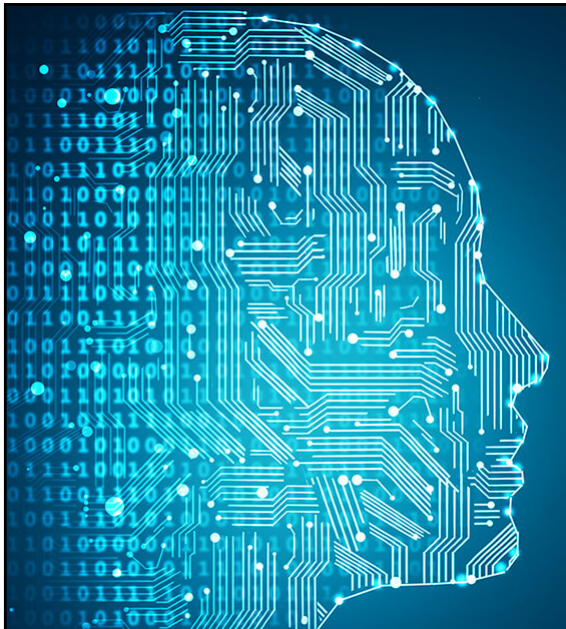
Unsupervised learning, graphical models, planning, knowledge graph, ...



Some scientists believe that data science is a subset of AI. Some others say AI is a subset of data science

It would be better to say that data science is a cross-cutting subset of all of these tools.

Big Data refers to extremely large and diverse collections of data that continues to grow exponentially over time that traditional data management systems cannot store, process and analyze them like financial transactions, or data generated by IoT.



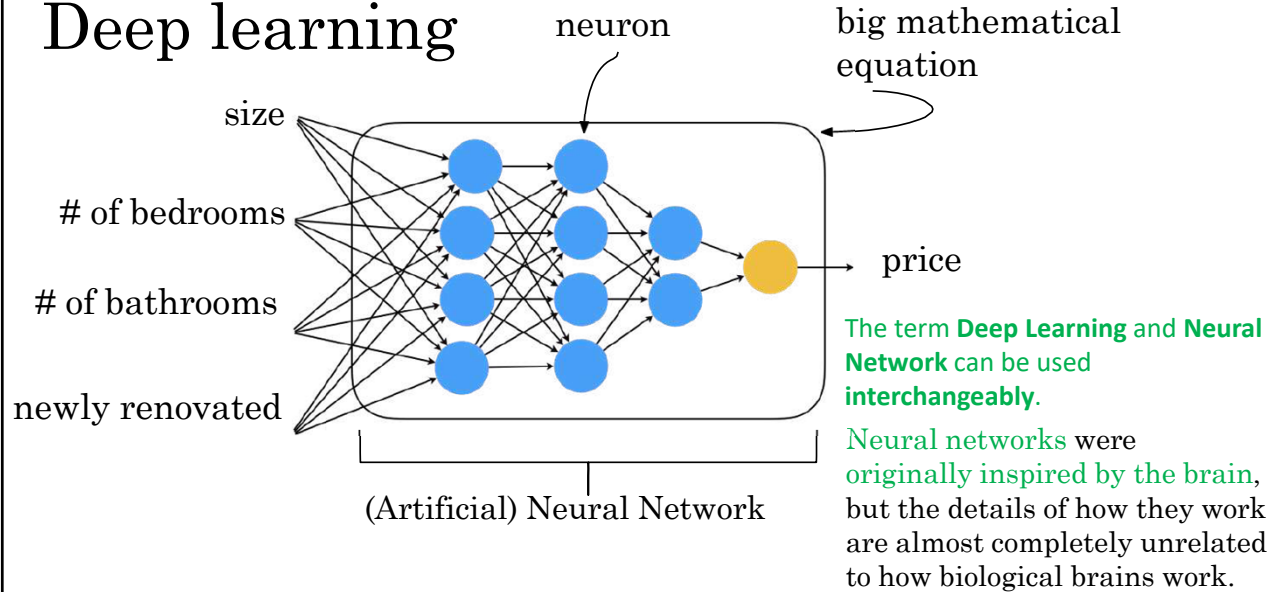
What is AI- Part 1  
in abstract

## What is AI

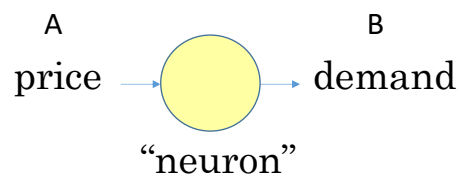
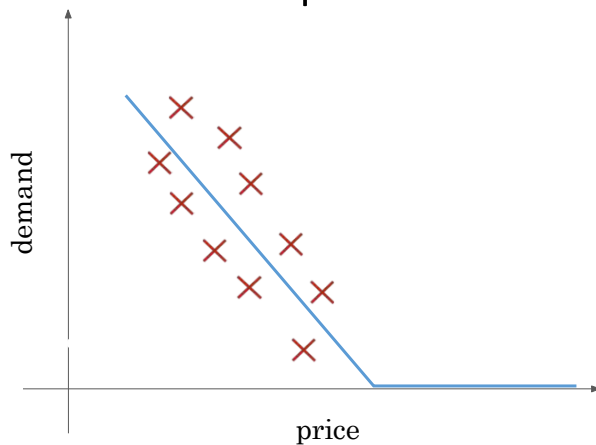
Non-technical explanation of deep learning



# Deep learning

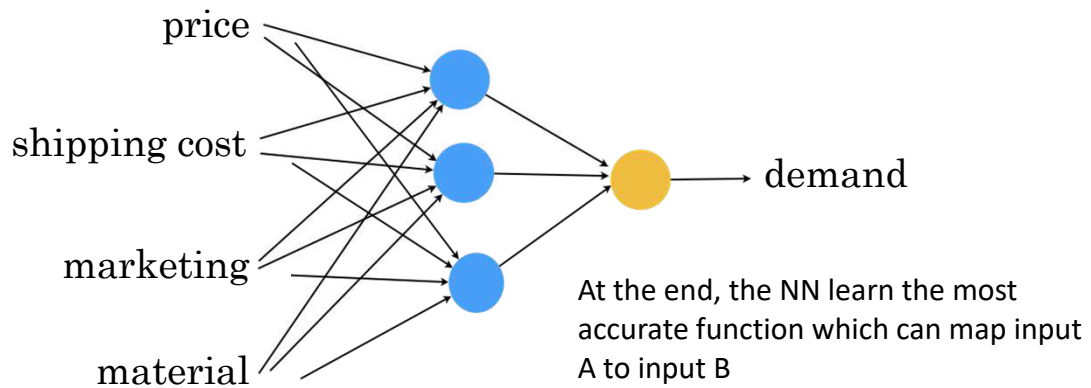


## Demand prediction

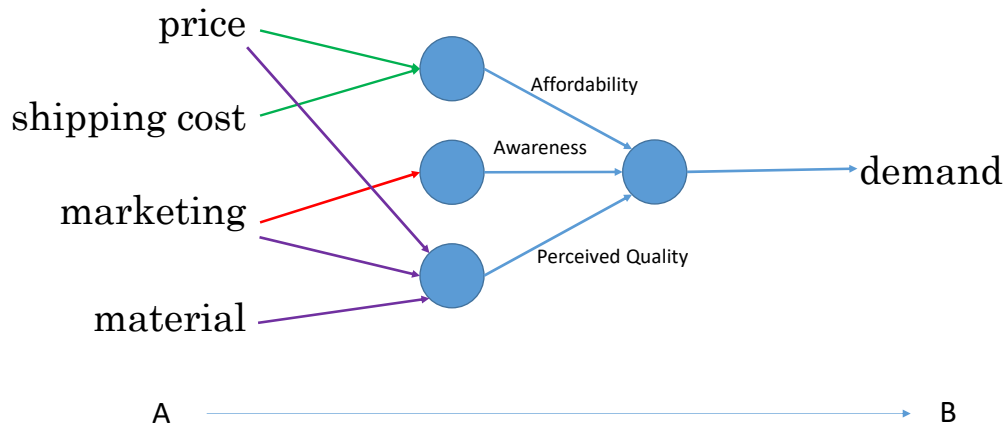


## Demand prediction

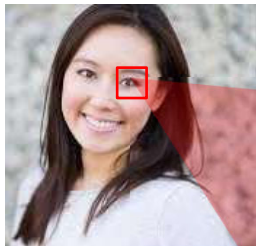
In neural networks we give input A and output B and the NN figures out all the things in the middle by itself.



## Demand prediction



## Face recognition



30	32	22	12	10	10	12	33	35	30
12	11	12	234	170	176	13	15	12	12
234	222	220	230	200	222	230	234	56	78
190	220	186	112	110	110	112	180	30	32
49	250	250	250	4	2	254	200	44	6
55	250	250	250	3	1	250	245	25	3
189	195	199	150	110	110	182	190	199	55
200	202	218	222	203	200	200	208	215	222
219	215	220	220	222	214	215	210	220	220
220	220	220	220	221	220	221	220	220	222

Pixel brightness values



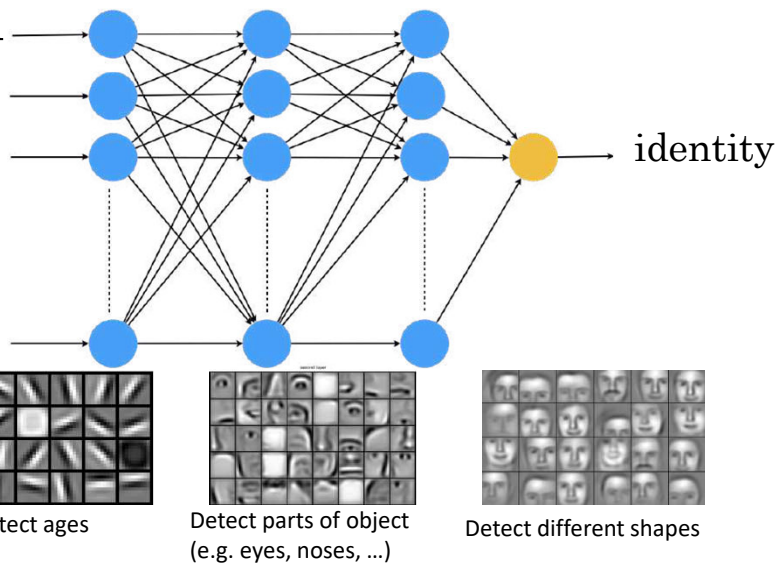
## Face recognition



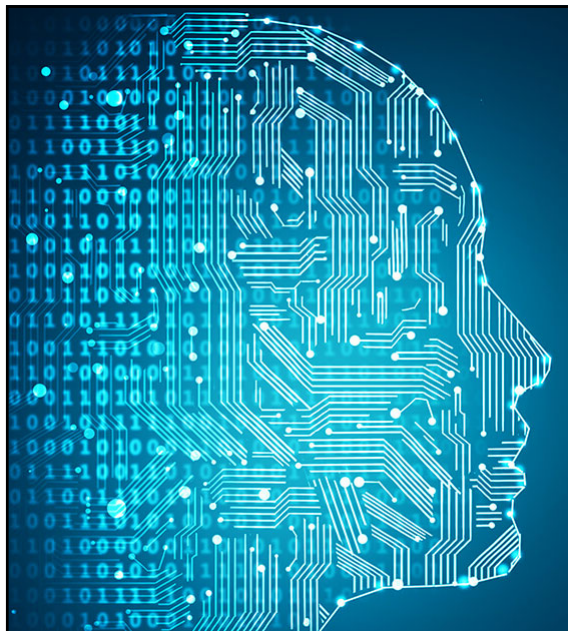
1000  
Pixels

1000  
Pixels

No. of inputs= 1M  
(color pics= 3M)



- The magic of neural networks is that you don't really need to worry about what it is doing in the middle.
- All you need to do is give it a lot of data (e.g. pictures) as well as of output (e.g. the correct identity), and the learning algorithm will figure out by itself what each of these neurons in the middle should be computing.



What is AI- Part 1  
in abstract

## What is AI

Examples of what machine learning can and cannot easily do

## Self-driving car

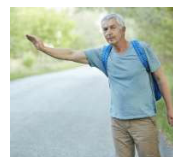
Can do



Cannot do (e.g. Human Gesturing)



stop



hitchhiker



bike turn  
left signal

1. Data (No. of gestures are very hard) especially as the input is a video instead of pictures
2. Need high accuracy compared to detecting the cars

## X-ray diagnosis



Can do

Diagnose pneumonia from  
~10,000 labeled images

Cannot do

Diagnose pneumonia from  
10 images of a medical textbook  
chapter explaining pneumonia

## Strengths and weaknesses of machine learning

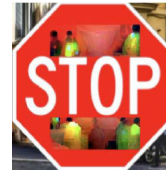
(Examples which hone the intuition about what AI can and can not do)

ML tends to work well when:

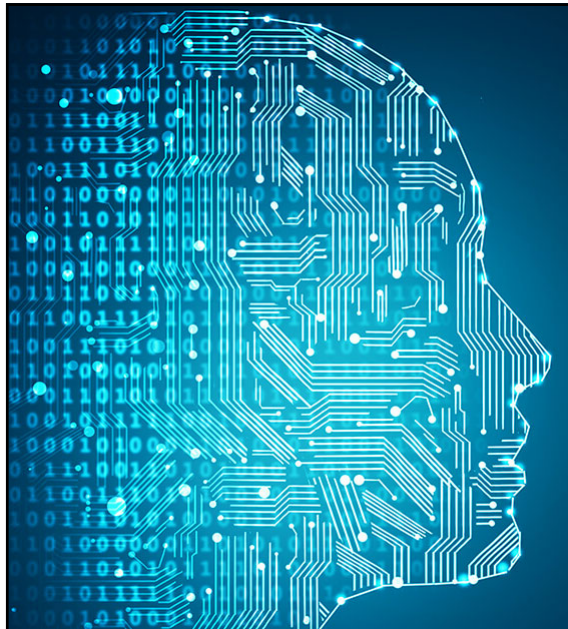
1. Learning a “simple” function (those human can do in less than a second)
2. There is lots of data available

ML tends to work poorly when:

1. Learning complex functions from small amounts of data
2. It is asked to perform on new types of data that it learned from  
(AI system can be much less robust than human doctors)



Fails to see stop sign



What is AI- Part 3  
in abstract

## Building AI in your company



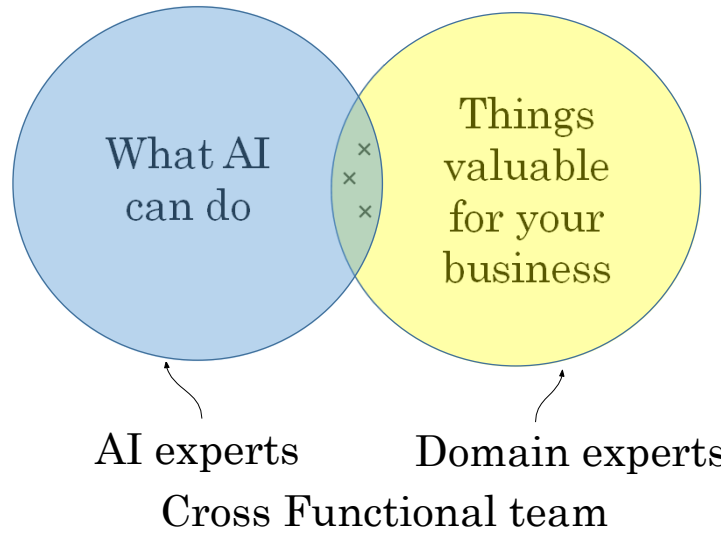
## AI Transformation

1. Execute pilot projects to gain momentum  
(Probably through outsourcing)
2. Build an in-house AI team
3. Provide broad AI training
4. Develop an AI strategy
5. Develop internal and external communication  
(To align all stakeholders with how the company is navigating the rise of AI)

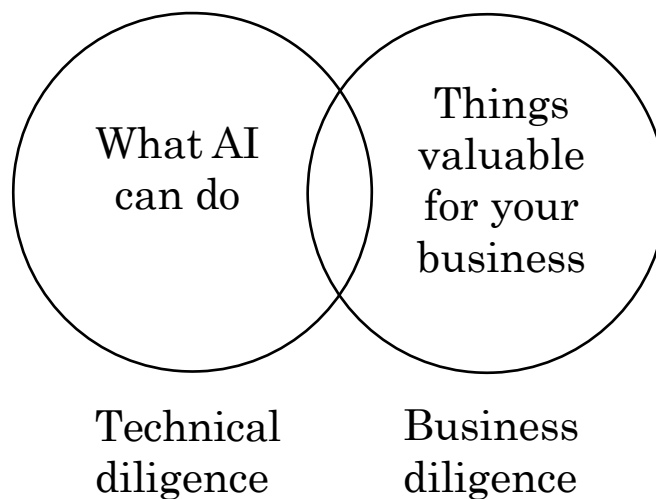
### 1. Execute pilot projects to gain momentum

- More important for the initial project to succeed rather than be the most valuable
- Show traction (Becoming popular) within 6-12 months
- Can be in-house or outsourced

## AI knowledge and domain knowledge



## Due diligence on project



## Due diligence on project

### Technical diligence

- Can AI system meet desired performance
- How much data is needed
- Engineering timeline

### Business diligence

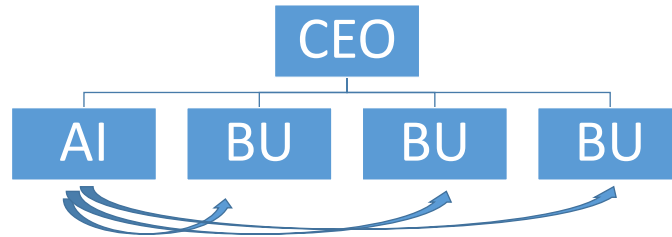
- Lower costs
  - Increase revenue
  - Launch new product or business
- } current business
- } new business

Even we can think about ethical diligence (what is good for society)

## Build vs. buy

- ML projects can be in-house or outsourced
- DS projects are more commonly in-house
- Some things will be industry standard – avoid building those. (Do not sprint in front of trains)

## 2. Build an in-house AI team



BU= Business Unit

AI function can be under CTO, CIO, CDO, etc. or a new CAIO

The CEO provides funding to build up the AI unit rather than require the AI unit to get funding from the business units eventually after the initial investment of the initial ramp up the AI unit will have to show its value that it's creating for the business units.

## Example roles

- **Software Engineer**
  - E.g., joke execution, ensure self-driving reliability, ...
- **Machine Learning Engineer**
  - Applied ML Scientist
- **Machine Learning Researcher**
  - Extend state-of-the-art in ML

## Example roles

- **Data Scientist**
  - Examine data and provide insights
  - Make presentation to team/executive
- **Data Engineer**
  - Organize data
  - Make sure data is saved in an easily accessible, secure and cost effective way (especially for big data)
- **AI Product Manager**
  - Help decide what to build; what's feasible and valuable

1 MB (megabyte)  
 1,000 MB = GB (gigabyte)  
 1,000,000 MB = TB (terabyte)  
 1,000,000,000 MB = PB (petabyte)

A self-driving car may collect multiple gigabytes of information every single minute of operation

## Getting started with a small team

- 1 Software Engineer , or
- 1 Machine Learning Engineer/Data Scientist , or
- Nobody but yourself

## Use and mis-use of data

A few CEOs approach: give me three years to build up my IT we're collecting so much data and then after three years i'll have this perfect data set and then we'll do AI.

Instead of this strategy, it is recommended to every company that **once you started collecting some data go ahead and start showing it or feeding it to an AI team to use convey the feedbacks to your IT team on what types of data to collect and what types of IT infrastructure to keep on building.**

**An example:** an AI team can look at your factory data and say requires to collect data from this big manufacturing machine not just once every 10 minutes but instead once every one minute.

Don't throw data at an AI team and assume it will be valuable.

### 3. Provide broad AI training

Role	What they should learn
Executives and senior business leaders	<ul style="list-style-type: none"> <li>• What AI can do for your enterprise</li> <li>• AI strategy</li> <li>• Resource allocation</li> </ul>
Leaders of divisions working on AI projects	<ul style="list-style-type: none"> <li>• Set project direction (technical and business diligence)</li> <li>• Resource allocation</li> <li>• Monitor progress</li> </ul>
AI engineer trainees	<ul style="list-style-type: none"> <li>• Build and ship (become available) AI software</li> <li>• Gather data</li> <li>• Execute on specific AI projects</li> </ul>

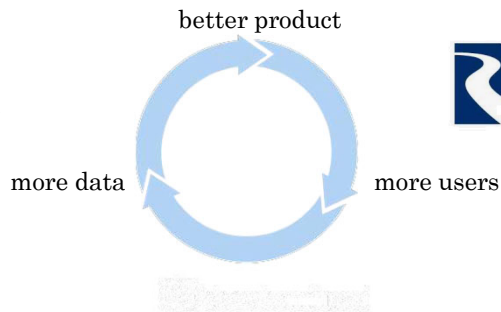
The smart CLO knows they should *curate* rather than *create* content, i.e. he gathers contents relevant to industry from trusted sources rather than create them.



#### 4. Develop an AI strategy

- Leverage AI to create an advantage specific to your industry sector
- Design strategy aligned with the “Virtuous Cycle of AI”

By this loop it is very difficult for a new entrant to break into this self-reinforcing positive feedback loop called the virtuous cycle of AI



Blue River. makes agricultural technology using AI. What they did was build these machines that would be towed behind a tractor in a big agricultural field and this machine would take pictures of crops and figure out which is a crop and which is a weed and use precision AI to kill off just the weeds but not the crop.

#### 4. Develop an AI strategy

- Consider creating a data strategy
  - Strategic data acquisition
  - Unified data warehouse
- Create network effects and platform advantages
  - In industries with “winner take all” dynamics, AI

**can be an accelerator** (like ride sharing Companies there are platforms that connect drivers with passengers, where it's quite difficult for a new entrant to accumulate both a large rider audience and a large passenger audience at the same time. Moreover, social media platforms like twitter and facebook are also very defensible because they are very strong network effects where having a lot of people on one platform makes that platform more attractive to other people so it's very difficult for a new entrant to break in a business with these types of winner take all dynamics)

- now AI can also fit into more traditional strategy frameworks for example michael porter many years ago had written about low-cost and high-value strategies.
- If your company has a low-cost strategy then perhaps AI can be used to reduce costs for your business or if your company has a high value strategy to deliver really valuable products but a higher cost then you might use AI to focus on increasing the value of your products and so AI capabilities can also help augment existing elements of a broader corporate strategy lastly as you're building these valuable and defensible businesses.

## 5. Develop internal and external communications

- Investor relations
- Government relations
- Customer/user education
- Talent/recruitment
- Internal communications

Detailed AI Transformation Playbook: <https://landing.ai/ai-transformation-playbook/>



What is AI- Part 4  
in abstract

# AI and Society

A realistic view of AI

## AI and society

- **AI and hype** (There's been a lot of unnecessary hype about it)
- **Limitations of AI**
  - **Bias** AI can be biased and discriminate unfairly against minorities or against other groups
  - **Adversarial attacks** There are spammers that are trying to attack spam filters and even some of the new technologies may be susceptible to new types of attacks as well if people are deliberately and on purpose trying to fool it.
- **AI, developing economies, and jobs** Developed economies such as the U.S and china are already using AI extensively which has a big impact on developing economies and on the global jobs
- **Conclusion and wrap up**

AI and  
Ethics

## Goldilocks rule for AI

- Too optimistic: Sentient / super-intelligent AI killer robots coming soon
- Too pessimistic: AI cannot do everything, so an AI winter is coming
- Just right: AI can't do everything, but will transform industries

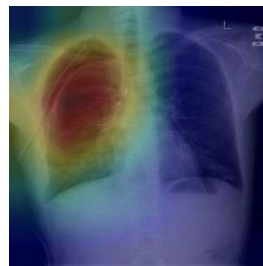
## Limitations of AI

- Performance limitations
- Explainability is hard (but sometimes doable)

Many high-performing AI systems are black boxes meaning that it works very well but the AI doesn't know how to explain.



Right-sided  
Pneumothorax  
(collapsed lung)



In this example by the heat map, the AI is telling us what part of the image it is looking at in order to make this diagnosis

[Rajpurkar et al. (2018). CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning.]

[Wang et al. (2017). ChestX-ray8: Hospital-scale Chest X-ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases. IEEE CVPR]

[Images source: NIH Clinical Center Image dataset: <https://nihcc.app.box.com/v/ChestXray-NIHCC>]

As AI is a relatively new thing, the lack of **explainability** is sometimes a **barrier to acceptance** and also sometimes if an AI system isn't working then **its ability to explain itself will also help us figure out how to go in and make the AI system work better.**

So explainability is one of the major open research areas and a lot of researchers are working on what it is seen in practice. When an AI team wants to deploy something the AI team is often able to come up with an explanation that is good enough to enable the system to work and be deployed.

## Limitations of AI

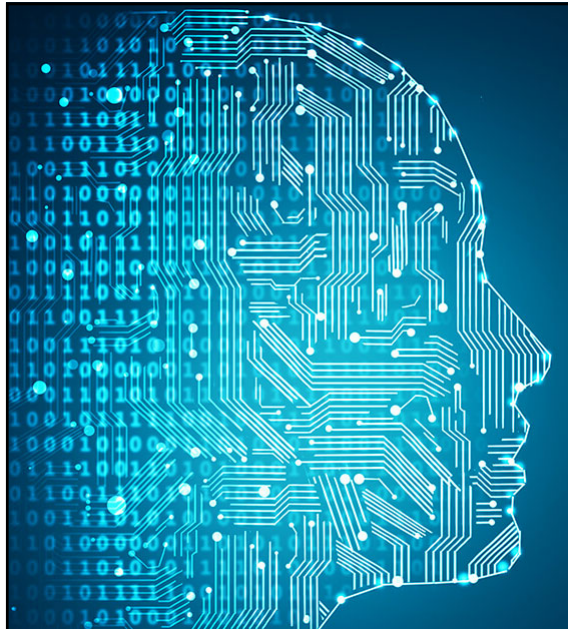
- **Biased AI through biased data**

**As a society we do not want to discriminate against individuals based on their gender based on their ethnicity** and we want people to be treated fairly **but when AI systems are fed data that doesn't reflect these values then an AI can become bias or can learn to discriminate against certain people.** Now the AI community is working hard and is making good progress on these issues.

- **Adversarial attacks on AI**

**Some AI systems are open to adversarial attacks if someone else is deliberately out to fool your AI system.** So depending on your application it may be important to make sure that you are not open to these types of attacks on your AI systems.

The issues of AI and discrimination or and bias as well as the issue of adversarial attacks on AI are important both to you as a potential builder and user of AI as well as to society



What is AI- Part 4  
in abstract

# AI and Society

## Discrimination / Bias

### AI learning unhealthy stereotypes

- **Man** : **Woman** as **Father** : **Mother**
- **Man** : **Woman** as **King** : **Queen**
- Man : Computer programmer as  
Woman : Homemaker → Computer programmer

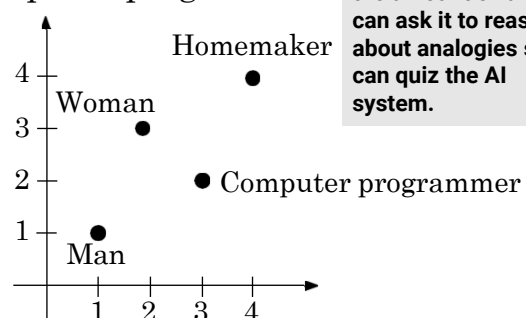
The way an AI system stores words is using a set of numbers. The way an AI system comes up with these numbers is through statistics of how the word man is used on the internet.

Man: (1,1)

Computer programmer: (3,2)

Woman: (2,3)

Homemaker: (4,4)



A group at Microsoft found this remarkable result that when AI learns from text found on the internet it can learn unhealthy stereotypes.

**As a technical solutions for reducing the amount of bias we can ask it to reason about analogies so we can quiz the AI system.**

Bolukbasi et al. (2016). Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings.

## Why bias matters

- **Hiring tool that discriminated against women**
- **Facial recognition matching dark skinned individuals to criminal mugshots**
- **Bank loan approvals**
- **Toxic effect of reinforcing unhealthy stereotypes**

for example if an **eight-year-old girl goes to an image search engine and searches the chief executive officer** if they see **only pictures of men** or if they see no one that looks like themselves either by gender or ethnicity **we don't want them to be discouraged from pursuing a career** that might lead her to someday be a chief executive.

## Combating bias

- **Technical solutions:**
  - E.g., “zero out” the bias in words
  - Use less biased and/or **more inclusive data**

for example if you are building a face recognition system and make sure to include data from multiple ethnicities and all genders then your system will be less biased and more inclusive.

- **Transparency and/or auditing processes**  
so that we can constantly check what types of bias if any. these AI systems are exhibiting so that we can at least recognize the problem if it exists and then take steps to address it. **for example many face recognition teams are systematically checking how accurate their system is on different subsets of the population** to check whether it is more or less accurate on dark skin versus light-skinned individuals
- **Diverse workforce** **are more likely to be able to spot different problems** and maybe they'll help make your data more diverse and more inclusive
  - Creates less biased applications





What is AI- Part 4  
in abstract

# AI and Society

## Adversarial attacks on AI

### Adversarial attacks on AI

Computers see pictures differently than humans.



Hummingbird

Minor perturbation

to change the pixel values just a little bit which is almost imperceptible change to most people.



Hammer



Hare

Minor perturbation



Desk

an adversarial attack on an AI system is an attempt to make it do something other than what it was intended to do such as trying to forward into outputting incorrect classifications

## Physical attacks

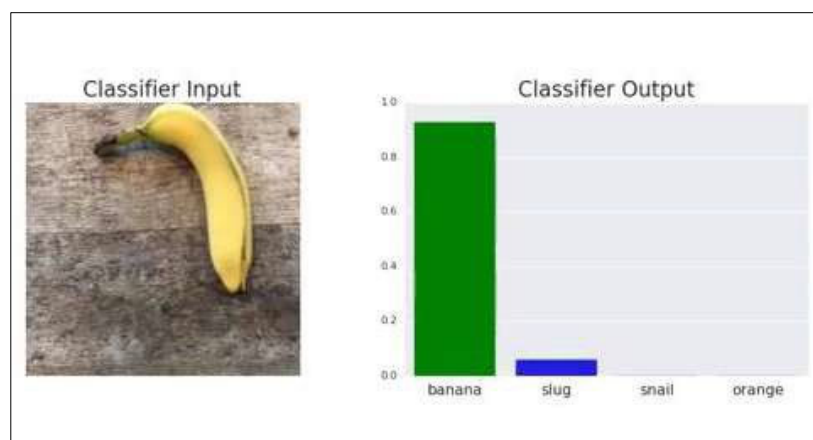


“Milla Jovovich”



Fails to see stop sign

## Physical attacks

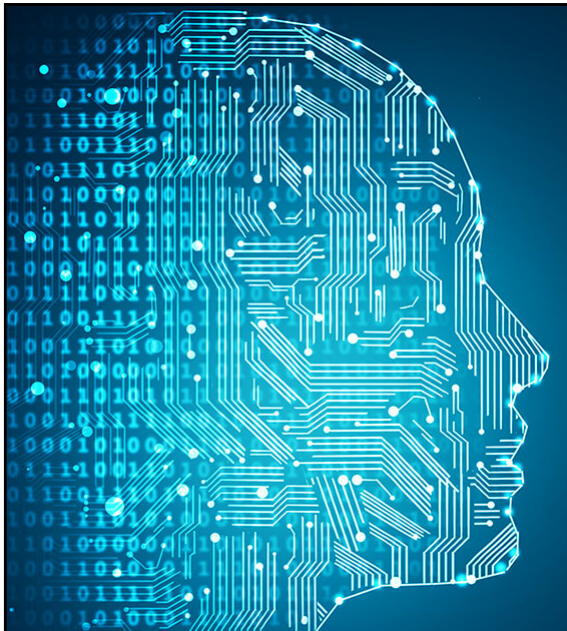


[Sharif et al. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition.]  
 [Eykholt et al. (2018). Physical Adversarial Examples for Object Detectors.]  
 [Brown et al. (2018). Adversarial Patch.]

## Adversarial defenses

- Defenses do exist, but **incur some cost**, for example **the AI system may run a little bit slower** but this is an area of **ongoing research** and we're far from having adversarial defenses that seem good enough.

Similar to spam vs. anti-spam, or anti-fraud systems (and not e.g. mug scratch detection) we may be in an arms race for some applications and the AI teams will be at war in what might feel like a zero-sum game against adversaries.



## AI and Society

Adverse uses of AI

What is AI- Part 4  
in abstract

## Adverse uses of AI

- **DeepFakes**

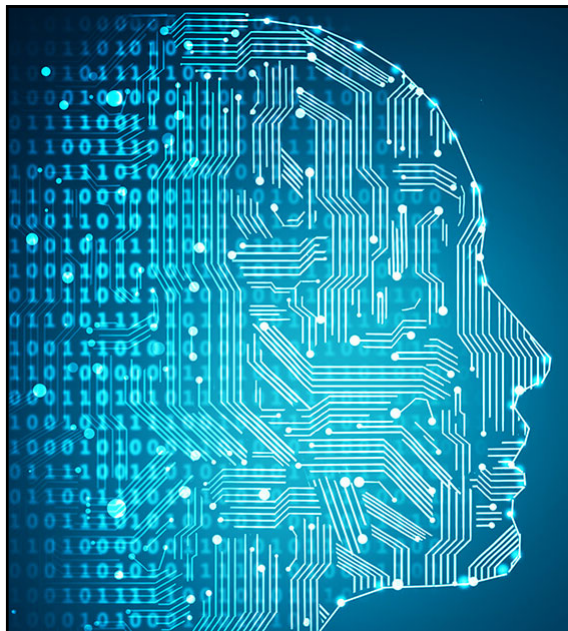
**Synthesize video of people doing things they never did**, like website BuzzFeed which created a video of former us president Barack Obama saying things that he never did

- **Undermining of democracy and privacy**

**Oppressive monitoring of individuals** by oppressive regimes which instead of uplifting their citizens, are not doing the right things by their citizens

- **Generating fake comments** of products or about political matters

- **Spam vs. anti-spam and fraud vs. anti-fraud**  
(battles)



## AI and Society

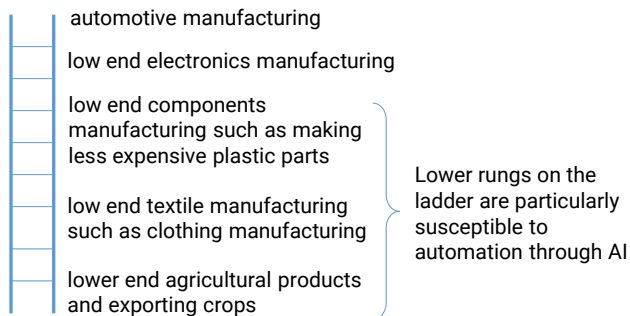
AI and developing economies

What is AI- Part 4

in abstract

## Developing economies

AI creates tremendous wealth that it uplifts all nations both developed and developing economies.



“leapfrog”

-Land lines to **Mobile phones**

-Credit cards system to **Mobile payments**

-Physical schools and universities to **Online education**



## How developing economies can build AI

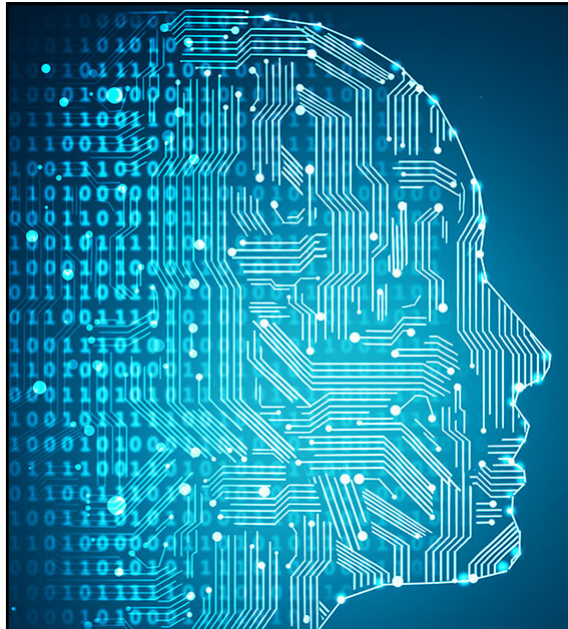
- US and China are leading, but all AI communities are still immature and this gives every nation an opportunity to be a large part of creating this value that hasn't been created yet.

## How developing economies can build AI

- **Focus on AI to strengthen a country's vertical industries.** Most countries today should not try to build their own web search engine, they're already great web search engines and that was last decade's competition, instead if a country has a very strong vertical industry in say coffee bean manufacturing then that country is actually uniquely qualified to do work in AI for coffee manufacturing and it would even further strengthen what that country is already good at.

## How developing economies can build AI

- **Public-private partnerships to accelerate development**
- **Invest in education** AI is still so immature and there's still plenty of room for every nation to learn more about AI



What is AI- Part 4  
in abstract

# AI and Society

## AI and jobs

### AI's impact on jobs worldwide

Jobs replaced  
by 2030

**400-800**<sub>mil</sub>

Jobs created  
by 2030

**555-890**<sub>mil</sub>

[Source: McKinsey Global Institute.]

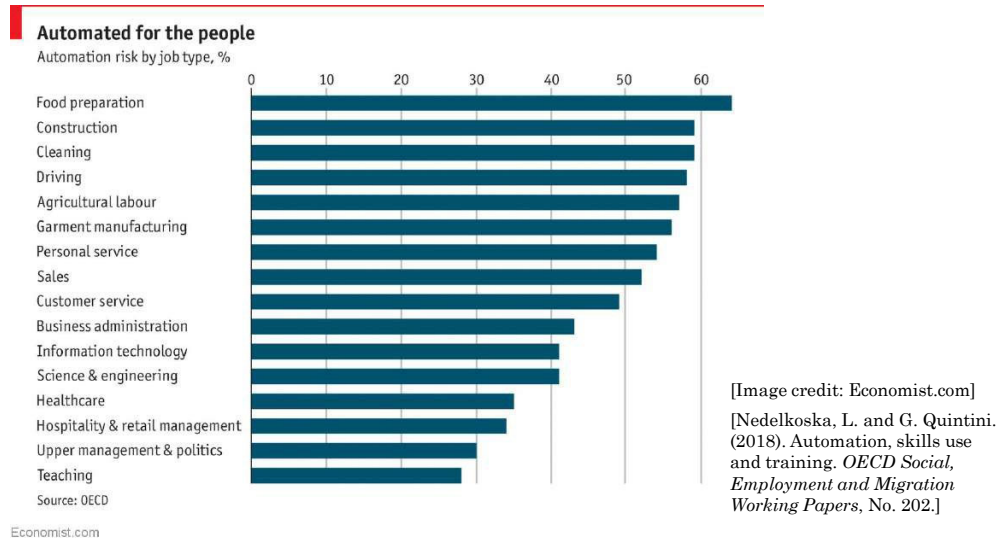
↓ Bank

↑ Drone traffic optimizer or 3d printed clothing designer or in healthcare will have custom DNA based drug designers

For each of the tasks estimate how amenable it is to automation through AI and if a job comprises mainly tasks that are highly automatable then the risk of the job being displaced will be higher.



## AI's impact on jobs worldwide



How do we help citizens and nations navigate the coming impacts of AI on jobs:

Some solutions

- **Conditional basic income:** provide a safety net (Universal Basic Income) but incentivize learning
- **Lifelong learning** society
- **Political solutions** being explored everything from incentivizing or helping with new job creation to legislation to make sure that people are treated fairly.



Take whatever you are already knowledgeable in and learn some AI and do your area plus AI then you might be more uniquely qualified to do very valuable work by applying AI to whatever area you are already an expert in.

Thank you!