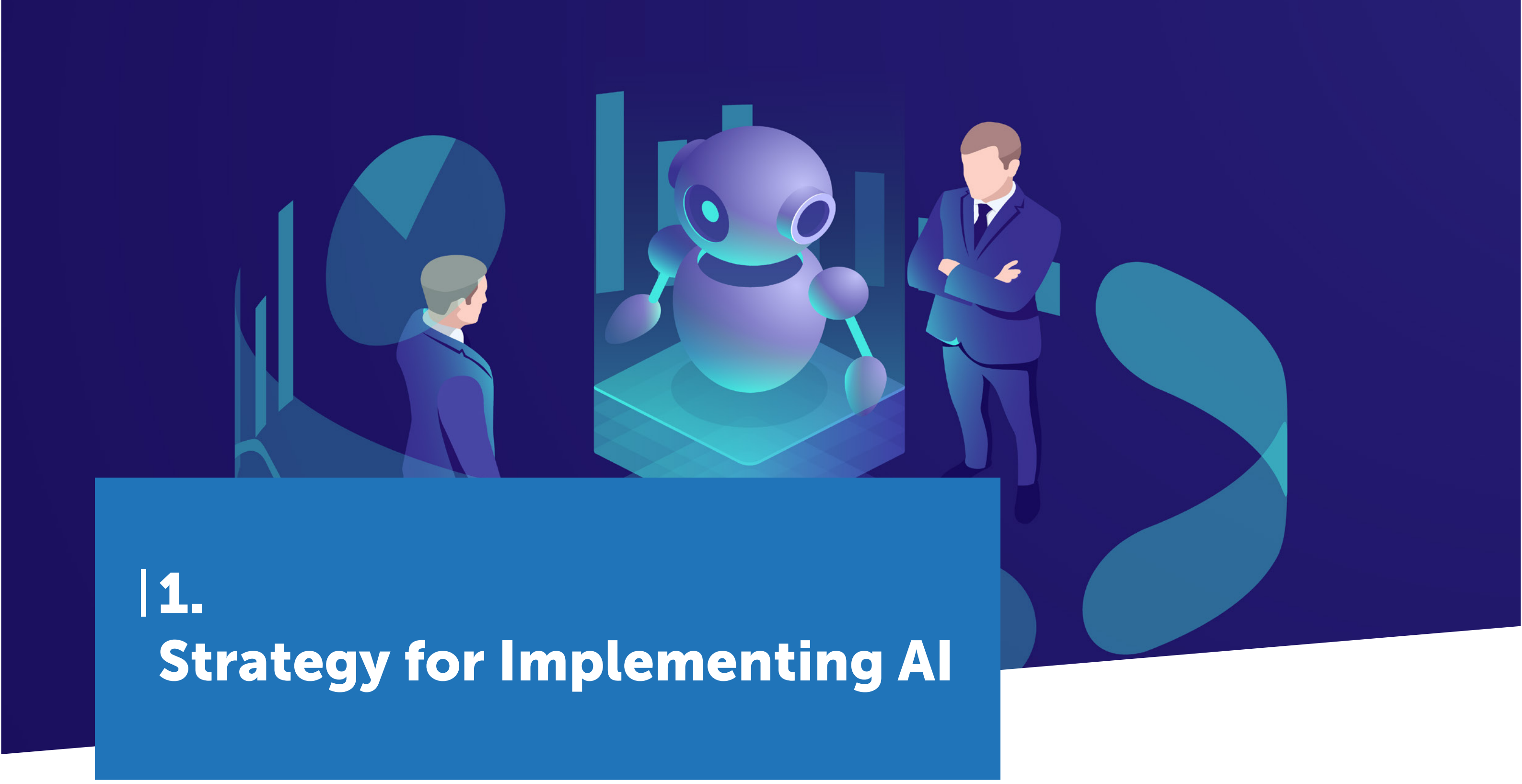


1.
Strategy for Implementing AI

Learning Objectives

By the end of this chapter, students will be able to know

1. Brief introduction of strategy for implementing AI in Business
2. How to implement various AI strategies such as Data strategy, Human resource management, implementation and operational strategies etc.
3. How to market and sell AI products.
4. How to build trust in AI.

Introduction to Strategy for Implementing AI

Gartner's key finding in the Top 10 technological strategic trend is that AI is the foundational catalyst for human engagement and automation (compared along with other technological trends such as IOT, Blockchain etc). According to Gartner by 2019, 37% of organizations have already integrated AI in some form. This shows the prominence of AI. AI is in the Late Adaptation Phase and moving towards the Early Majority Phase. This is the right time from the strategic point of view to invest in AI as people are starting to see the benefits of AI and the overall trust in AI is increasing.

The following figure shows the return of investment for different ranges of investment. It is seen that organizations those who spent more in investment saw more return from investment.

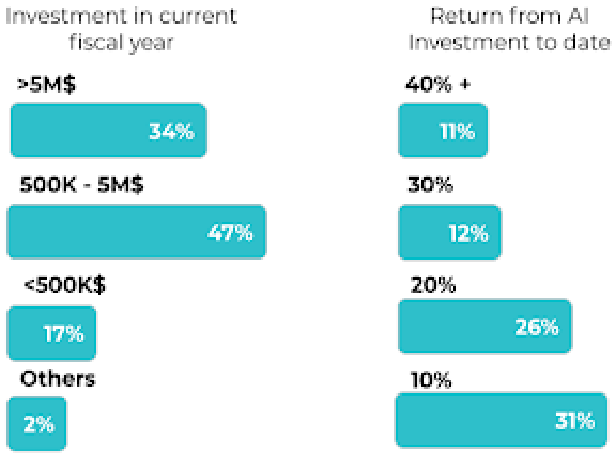


Figure:Amount of Investment in AI and the corresponding ROIs

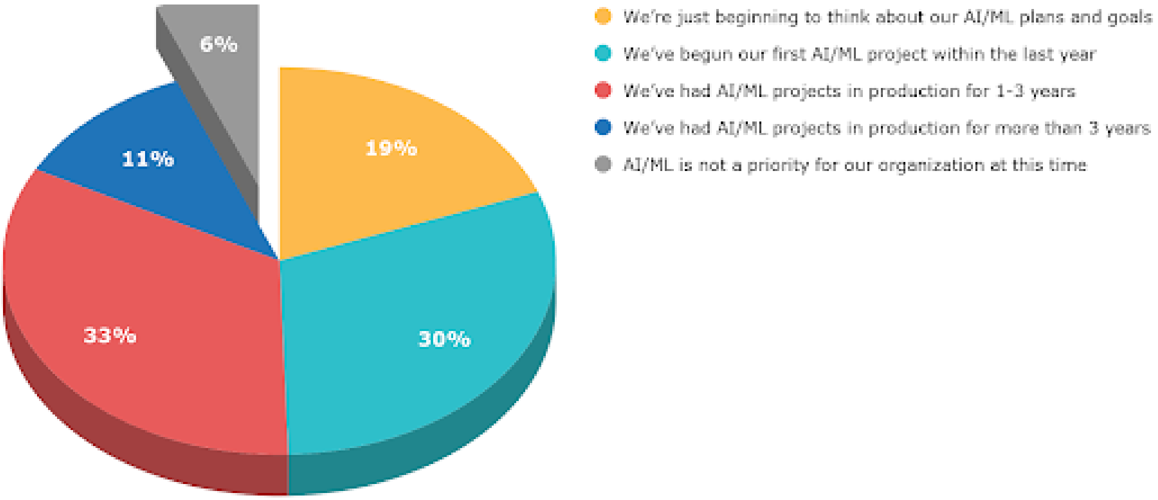
It was found that 34% of organizations invested more than 5 Million dollars and among them 11% saw a return of investment of more than 40%.

Similarly, 47% of organizations invested 500K-5M dollars and among them 12% reported a return of investment of 30%.

17% invested less than 500k dollars and among them 26% reported a return of investment of 20%.

2% did not disclose their investment and among them 30% reported a return of investment of 10%.

The following chart shows the percentage of organizations who have already implemented AI or in the process of implementing AI. The survey was conducted by Snaplogic together with independent research firm Vanson Bourne, among 300 IT Leaders representing organizations with more than 1,000 employees in the US and UK.



Source: The AI Skills Gap, Snaplogic
Figure: Organization considering AI to be top priority

In the chart it is found that more than 70% have already begun AI/ML projects. And 93% of organizations consider AI/ML projects to be the top priority. Organizations are seeing the potential and business benefits of AI and are investing in AI.

Business Benefits of AI

Among the Survey of 250 executives (Source Deloitte 2017 From "Artificial Intelligence for the Real World") who were familiar with their companies' cognitive technologies, to learn about their goals for AI initiatives, **more than half said that the primary benefit of AI is that it enhances existing products better.**

Other benefits include:

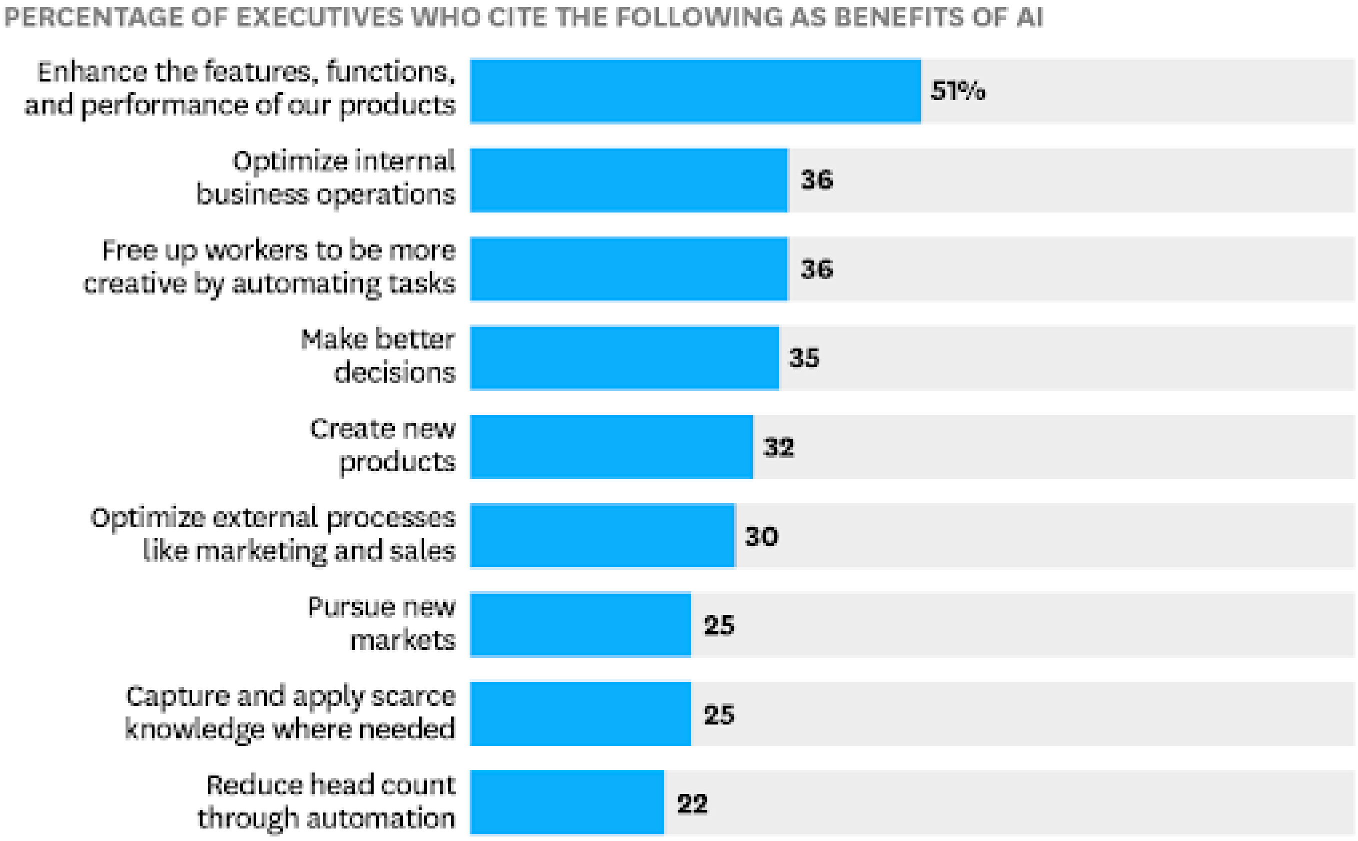


Figure: Benefits of AI

Challenges of AI

However we can not underestimate the risk that comes with the benefits of AI. Elon Musk in a comment on Edge.org worte referring to AI as "The risk of something seriously dangerous happening is in the five-year time frame. 10 years at most."

If we look at the statistics, the risks are more obvious. It is observed that 25% of the organizations worldwide that are already using AI reported upto 50% failure rate.

And the prime cause for this kind of failure rate is due to the unmanaged strategy. It was found that only 25% of AI companies have developed an enterprise-wide AI strategy.

According to the report by Deloitte 2017 From "Artificial Intelligence for the Real World", 47% of the attendees reported that it was hard to integrate cognitive projects with existing processes and systems. Other topmost strategic barriers for implementing AI are as follows:

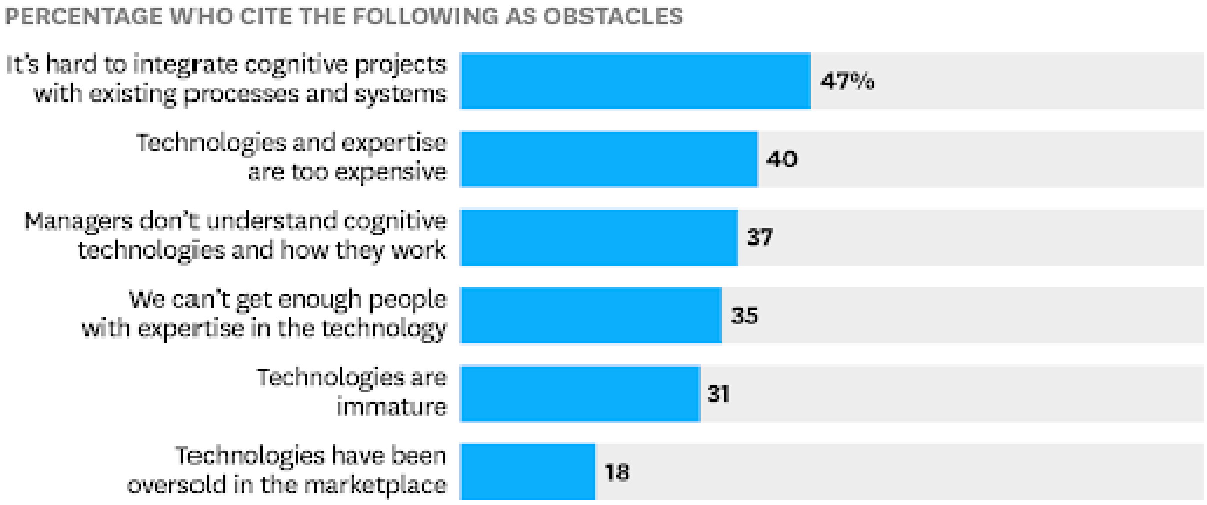


Figure: Challenges of AI

Strategy for Implementing AI

Organizations often deluge with the hype and forget to make the right foundations to excel in the process. One of the key ingredients for success always lies in asking the basic questions as shown the figure below.

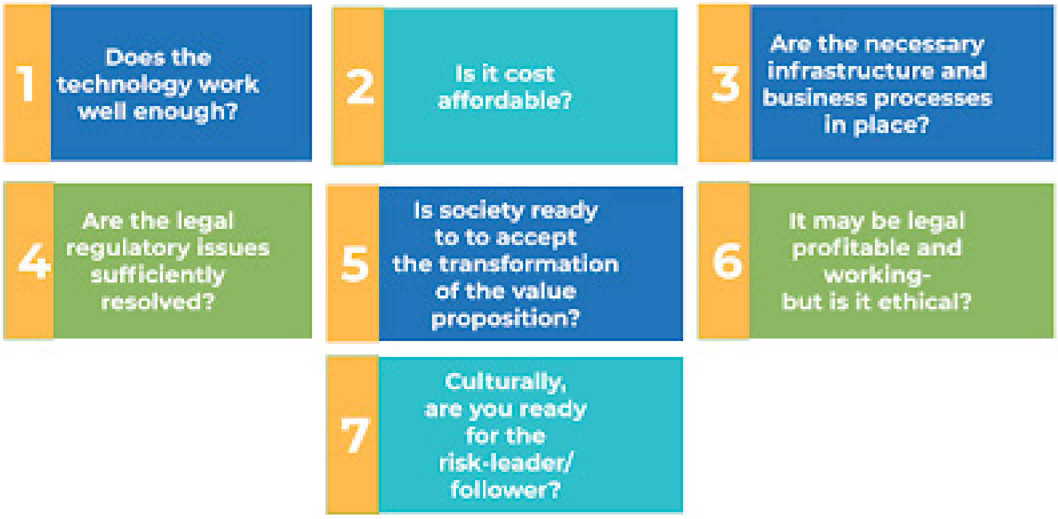

1
Does the technology work well enough?
2
Is it cost affordable?
3
Are the necessary infrastructure and business processes in place?
4
Are the legal regulatory issues sufficiently resolved?
5
Is society ready to to accept the transformation of the value proposition?
6
It may be legal profitable and working- but is it ethical?
7
Culturally, are you ready for the risk-leader/ follower?

Figure: Follow the Seven-Point Checklist

The figure signifies the need of Technical along with Business diligence before starting any project. Asking the five why questions, analyzing business with growth sharing matrix and validating the business requirements with Crisp-DM etc always help an organization move forward in all strategic directions.

After the technical and business diligence, it is advised to choose the strategic AI use cases such as AI in Retail, AI in Finance, AI in Healthcare etc. For example, if the organization uses AI in Retail as the strategic use case, the same data which is used for the Predictive Analysis can also be used for the application of customer experience. The ethics, bias, sales and marketing strategy also overlaps. In this way, the cross cutting AI strategic use cases is one of the foundational ingredients to meet business objectives.

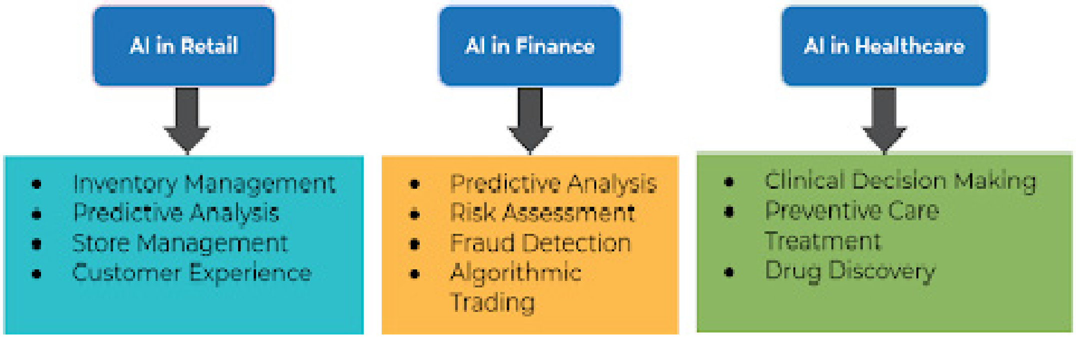


Figure: Choose the strategic AI use cases

The strategic leader should choose some use cases along with quick wins which one can implement in a shorter time and gain confidence and momentum.

The following figure explains the cross cutting strategy for implementing AI.

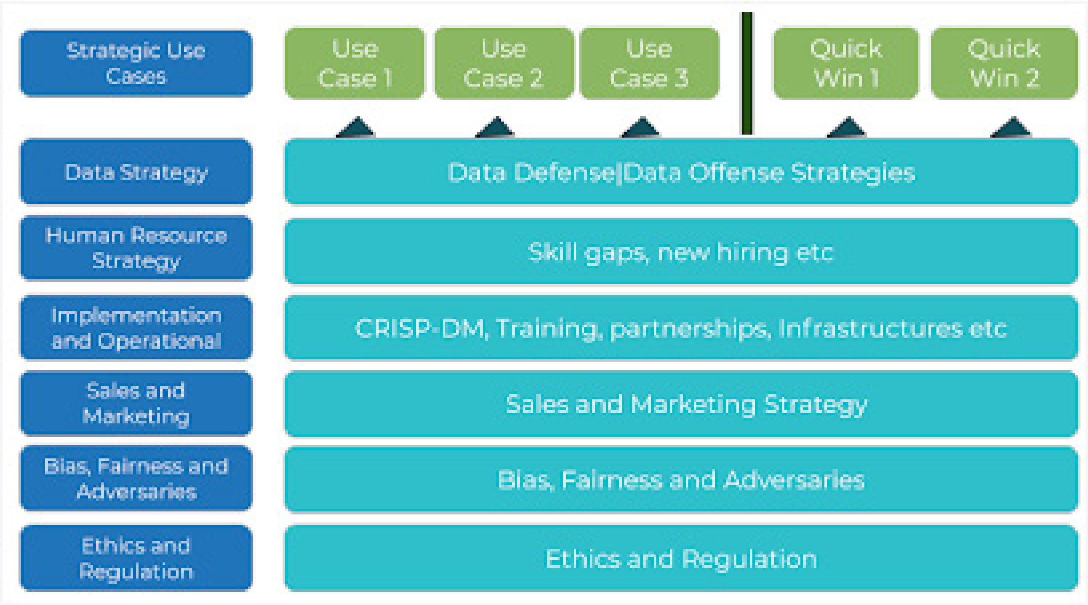

Strategic Use Cases
Use Case 1
Use Case 2
Use Case 3
Quick Win 1
Quick Win 2
Data Strategy
Data Defense|Data Offense Strategies
Human Resource Strategy
Skill gaps, new hiring etc
Implementation and Operational
CRISP-DM, Training, partnerships, Infrastructures etc
Sales and Marketing
Sales and Marketing Strategy
Bias, Fairness and Adversaries
Bias, Fairness and Adversaries
Ethics and Regulation
Ethics and Regulation

Figure: Cross cutting AI strategy

In data strategy, the leader should be able to implement various data defense and data offense strategies. In human resource strategy the leader will build plans to overcome skill gaps in AI, new hiring for AI teams etc. In Implementation and Operation Strategy the leader will implement CRISP-DM and AIDR framework, training and developments for the AI team and across the company and manage infrastructure required for AI projects. In Sales and Marketing, the leaders should be able to implement various strategies for Marketing AI products. In Bias, Fairness and Adversaries the leaders will understand how to remove bias and build trust in AI. In ethics and regulation, the leaders will know about various ethics and regulatory aspects of implementing AI.

Let's look at each of these strategies one by one in more detail.

1. Data Strategy

Data Understanding and Preparation

Essentially, when AI technologies are integrated with a product properly, it is self improving with a positive feedback loop where the product continuously improves with data, creating more users. As the number of users increases, the amount of data they generate increases as well, which in turn can be used to further improve the AI product. This is known as the Flywheel effect or the virtuous cycle of AI. Data is thus the crucial part of any AI product.

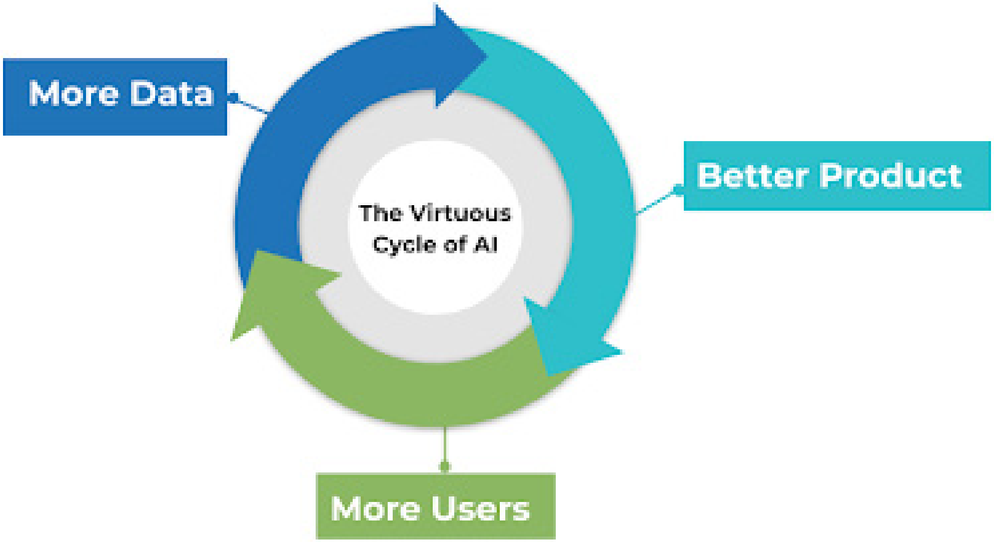


Figure: Virtuous Cycle of AI

Data in a company may come from various sources such as excel spreadsheets, employee records, etc. The data may come from the web. The data may be semi structured or unstructured. All of the data may not be useful for AI use cases. So we need to filter and prepare the required data for ML models.

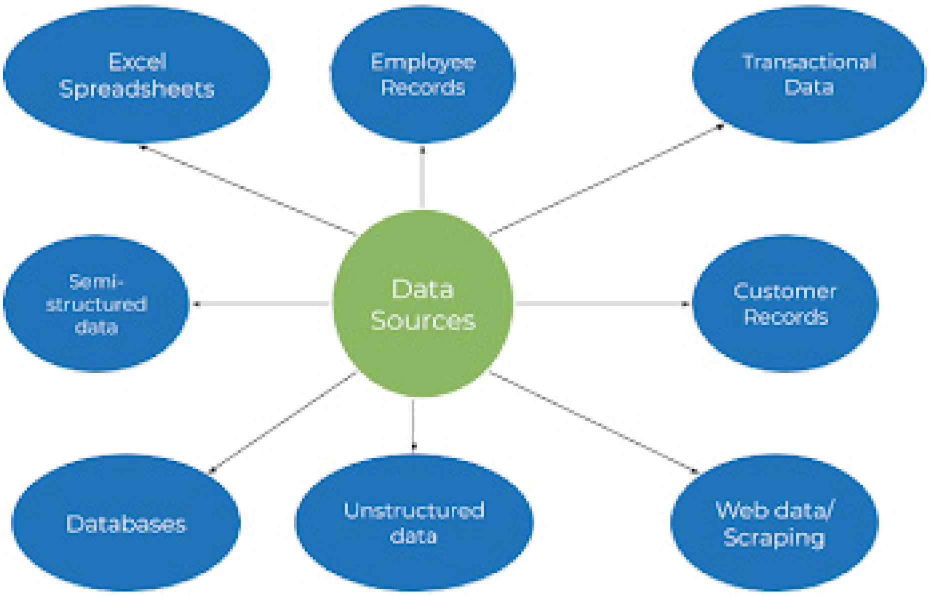


Figure: Various Sources of Data

Data revolves in all parts of the CRISP-DM from business understanding to model deployment. Let's look at each phase of CRISP-DM and the data strategy for each phase.

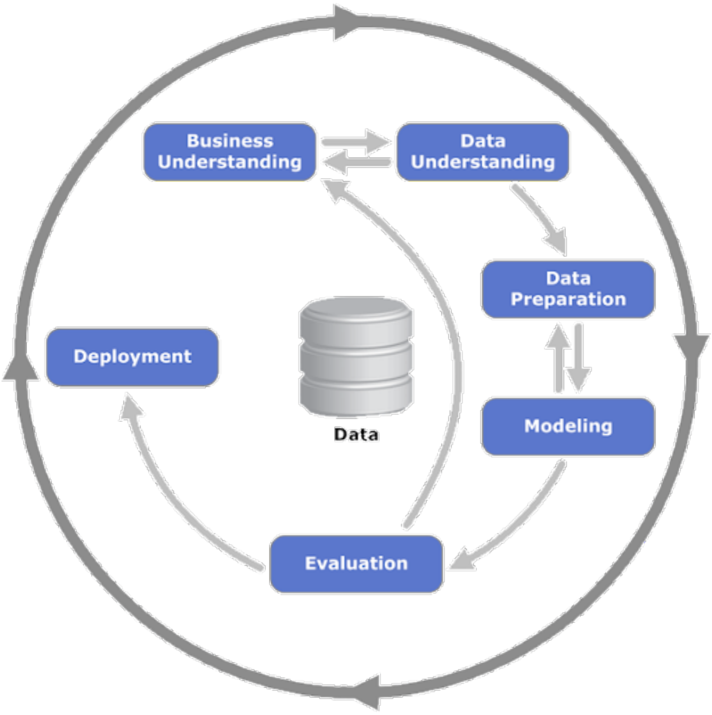


Figure: CRISP-DM

In the Data understanding part we acquire and explore the data. Data acquisition task contains identifying, collecting and integrating all the data related to the problem. Data exploration is the preliminary exploration of data to understand what we have to work with. In the data preparation part of CRISP-DM, We also address the data quality issues and we select features to use and prepare and process data for modeling. We will discuss in more detail about data modeling and evaluation in the section Strategy for Implementation of AI.

Data Defense Vs Data Offence Strategy

"Data defense is about minimizing downside risk: ensuring compliance with regulations, using analytics to detect and limit fraud, and building systems to prevent theft."

"Data offense focuses on supporting business objectives such as increasing revenue, profitability, and customer satisfaction."

The data defense focuses more on control while data offense provides flexibility.

Let's see some data defense issues or data privacy concerns.

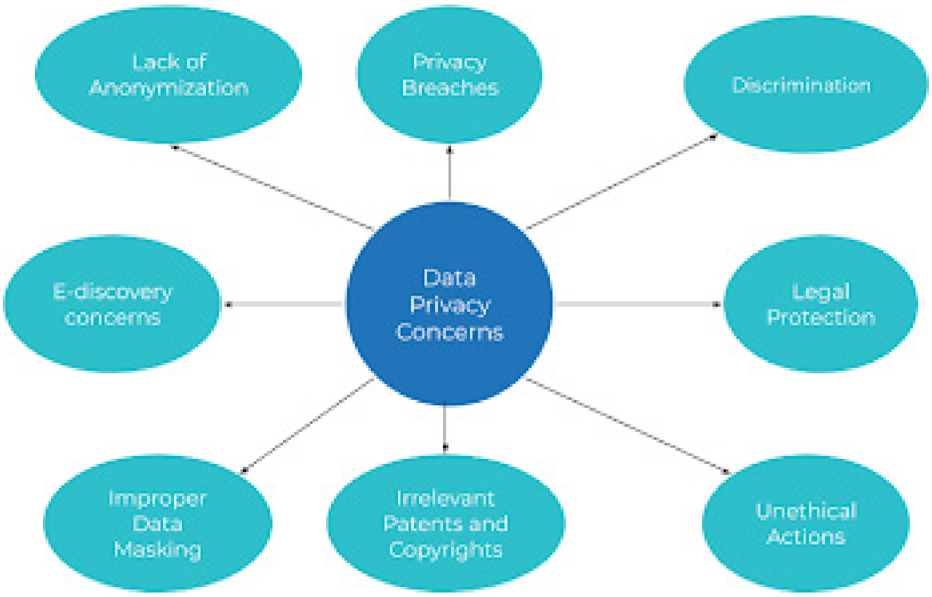


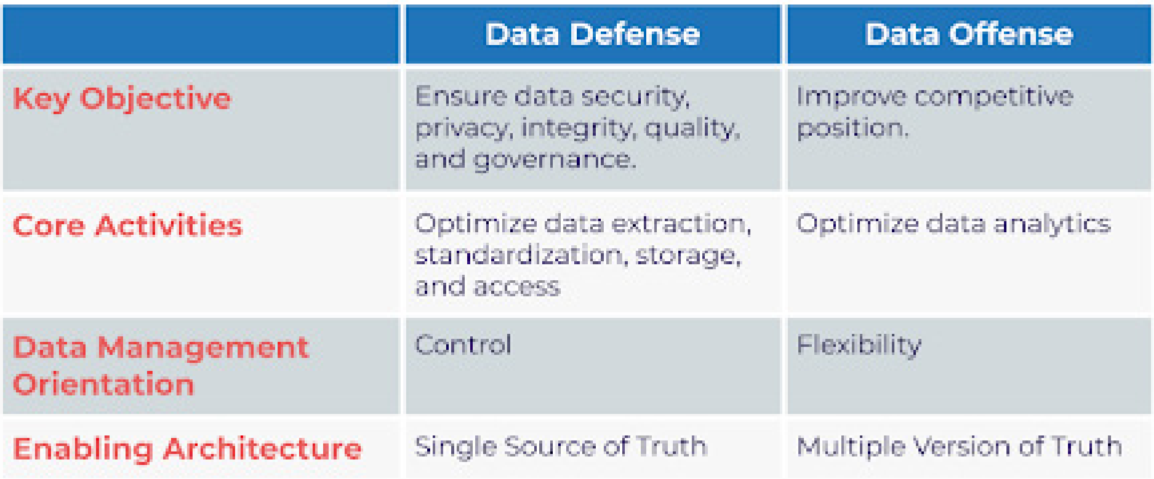
Figure: Data Privacy Concerns

In organizations,
Data breaches and stealing are common possibilities.
The data bias and discrimination are another issue that should be tackled.
The data should be protected by legal jurisdiction.
We should also protect data from unethical actions such as hacking.
The data may face irrelevant patents and copyright issues.
Sometimes it may be necessary for hiding original data with modified data for data privacy protection. This type of task sometimes may be improperly done and it may cause another issue.
E-discovery and legal frameworks governing data privacy and protection are necessary for organizations to safeguard various data privacy concerns.
It may also be needed to anonymize data to hide personal identifiable information.
Lack of such type of anonymization are also the issues for data privacy concerns.

These types of privacy concerns should be addressed with data defense strategies. It is crucial to deal with data privacy concerns to win the customer's trust and confidence.

In a research by Deloitte University Press, **73% of customers stated that easier to understand privacy policies would increase their trust in companies. And in the same research, it was found that 80% of customers are likely to buy from companies that protect their information.** So, effective information security and transparent privacy policies are key to winning customer trust.

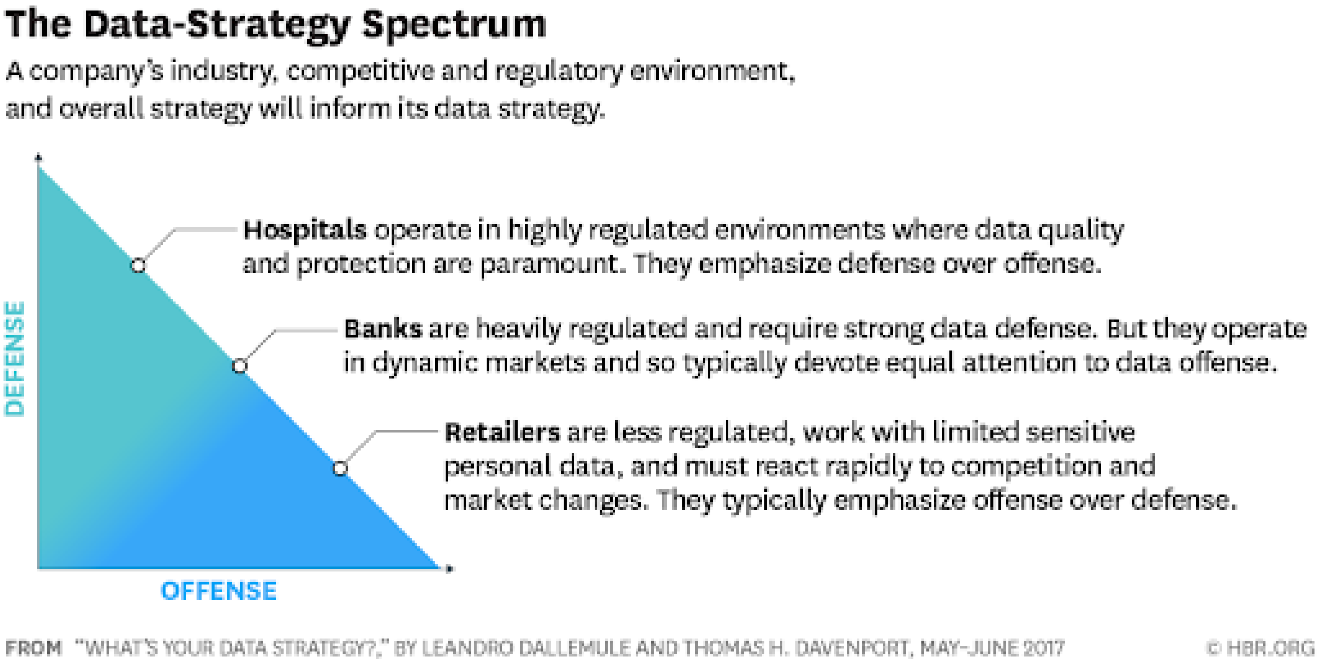
In an organization, data is stored as a single source of truth in a data warehouse in a data defense strategy while meaningful insights and multiple versions of the data are developed in data offense strategy from the single source of truth. The following table shows the key difference between data defense and data offense strategy.



	Data Defense	Data Offense
Key Objective	Ensure data security, privacy, integrity, quality, and governance.	Improve competitive position.
Core Activities	Optimize data extraction, standardization, storage, and access	Optimize data analytics
Data Management Orientation	Control	Flexibility
Enabling Architecture	Single Source of Truth	Multiple Version of Truth

Figure: The elements of Data Strategy

The data offense and data defense strategy have different purposes and specifics. The regulation and balancing of these two strategies may vary according to the business needs and objectives. The following spectrum shows the data strategy applied in healthcare, finance and retail sectors



The Data-Strategy Spectrum

A company's industry, competitive and regulatory environment, and overall strategy will inform its data strategy.

Hospitals operate in highly regulated environments where data quality and protection are paramount. They emphasize defense over offense.

Banks are heavily regulated and require strong data defense. But they operate in dynamic markets and so typically devote equal attention to data offense.

Retailers are less regulated, work with limited sensitive personal data, and must react rapidly to competition and market changes. They typically emphasize offense over defense.

FROM "WHAT'S YOUR DATA STRATEGY?," BY LEANDRO DALLEMULE AND THOMAS H. DAVENPORT, MAY–JUNE 2017 © HBR.ORG

Figure : The Data-Strategy Spectrum

2. Human Resource Strategy

The block diagram of a Human Resource process in an AI team is shown below.

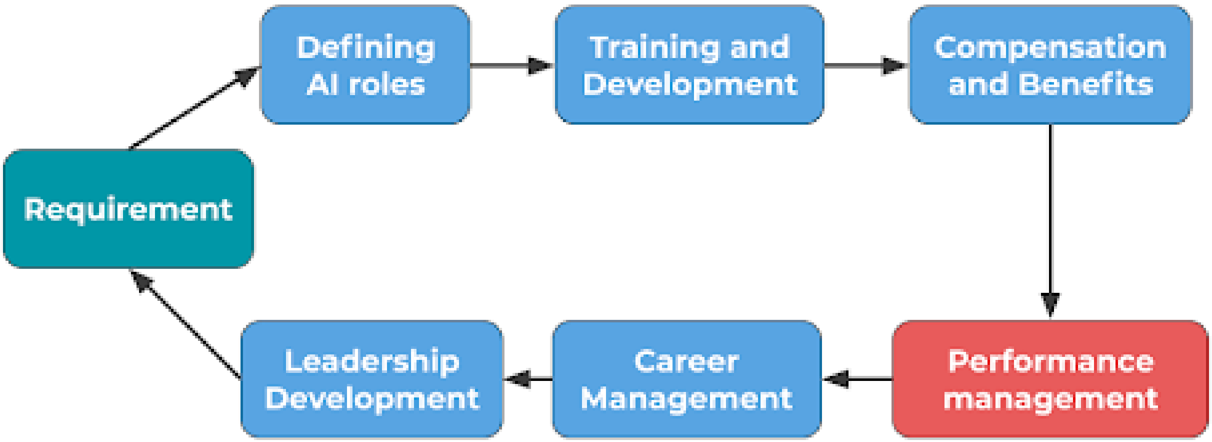


Figure: Human Resource Strategy

Defining AI Roles

The AI team needs talents from various sectors ranging from data collection, Data storing and preparation to Model Building and testing Machine Learning models in production.Talent shortage is one of the most crucial barriers in implementing AI.

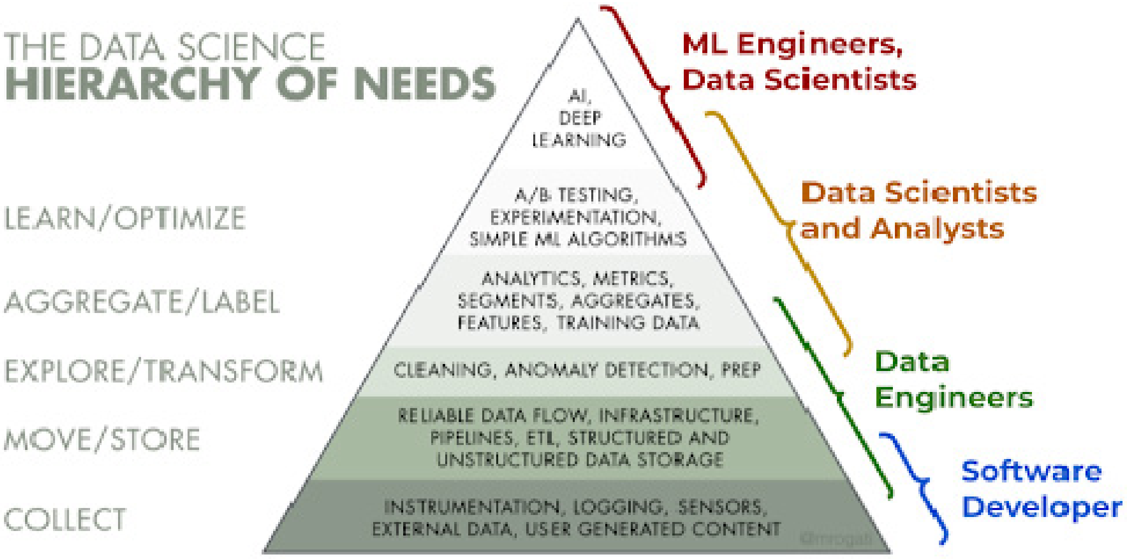

THE DATA SCIENCE
HIERARCHY OF NEEDS
LEARN/OPTIMIZE
AGGREGATE/LABEL
EXPLORE/TRANSFORM
MOVE/STORE
COLLECT
AI, DEEP LEARNING
A/B TESTING, EXPERIMENTATION, SIMPLE ML ALGORITHMS
ANALYTICS, METRICS, SEGMENTS, AGGREGATES, FEATURES, TRAINING DATA
CLEANING, ANOMALY DETECTION, PREP
RELIABLE DATA FLOW, INFRASTRUCTURE, PIPELINES, ETL, STRUCTURED AND UNSTRUCTURED DATA STORAGE
INSTRUMENTATION, LOGGING, SENSORS, EXTERNAL DATA, USER GENERATED CONTENT
@mrogati
ML Engineers, Data Scientists
Data Scientists and Analysts
Data Engineers
Software Developer

Figure : The Data Science Hierarchy of Needs

In the data science hierarchy of needs, the role of Software Development is to collect data from various sources such as logging user behaviour on a website, tracking sensor data etc.

Data engineers are required to store data in a data warehouse and to make pipelines to move data between places. Also the task of checking data accuracy and data cleaning to use for downstream tasks also comes under this role.

Data Scientists and Analysts aggregate and summarize the data. They run experiments to estimate the impact of the decision of forecasts. They perform these tasks for reporting and analytics purposes.

Finally Data Scientist and Machine Learning Engineers build Machine Learning models and integrate with the system. Furthermore Machine Learning Researcher and Scientists work on building new state of the art models.

These roles are generally overlapping.

Furthermore other roles such as AI product Manager can help decide what to build and Project managers can help manage the projects.

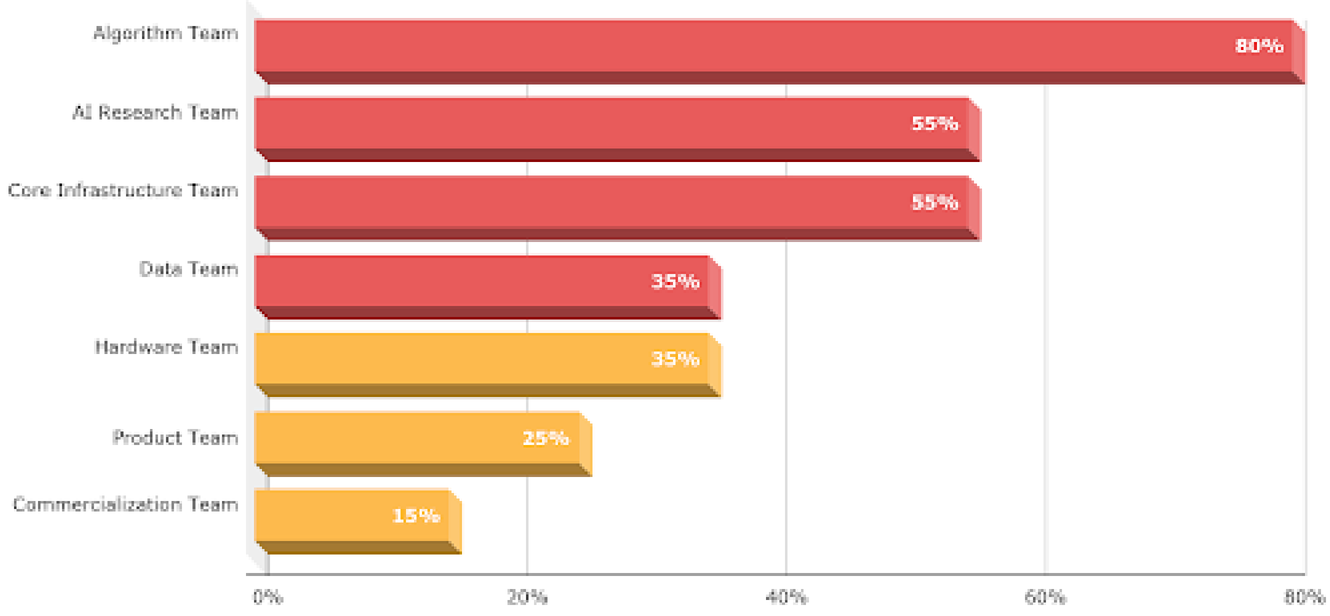
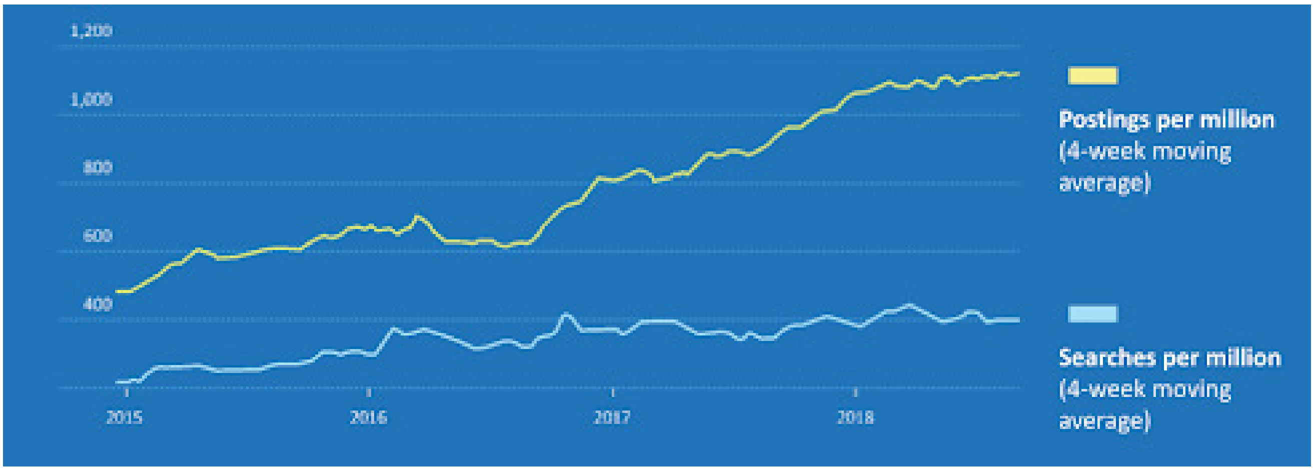


Figure: AI Talent Demand by Team Structure

The above figure shows that domain specialists such as Machine Learning Engineers or Computer Vision or NLP are the most sought out professions in AI companies. This is followed by an AI research team containing AI researchers and a core infrastructure team which consists of engineers such as backend engineers or devops engineers.



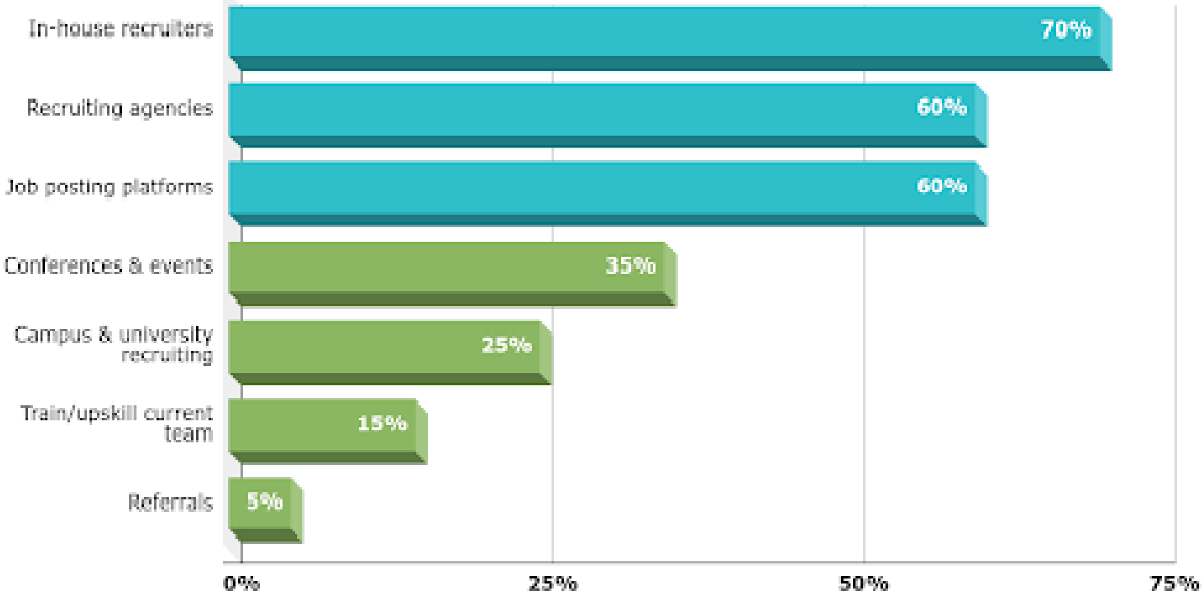
Source: Indeed.com, Ann Saphir | REUTERS GRAPHICS

Figure: Job searches vs job openings

Also, if we look at the above graph, the job openings are rising faster than job seekers. This represents the talent gap in AI. As we discussed earlier AI builders such as AI researchers, data scientists and project managers are the roles on which the talent crisis is obvious. The leaders should make a necessary plan to overcome this skill gap.

Guide to AI talent Acquisition

There can be several strategies for AI talent acquisition. In a report by Talentseer 2020, AI talents are mostly recruited in house by more than 70% of the researched audiences. AI talents are recruited through recruiting agents and job posting platforms by 60% of the audiences. Training and upskilling current team had a low number of audiences of 15%.



Source: Talentseer, 2020 AI Talent Report

Figure: Guide to AI talent Acquisition

According to Deloitte analysis based on Deloitte's AI in the Enterprise, 2nd Edition survey of 1,900 AI early adopters in seven countries, 56% tend to replace employees with new talent which is 3 times more than the tend to keep and retrain current employees which is 18% and 24% keep and replace employees in equal measure.

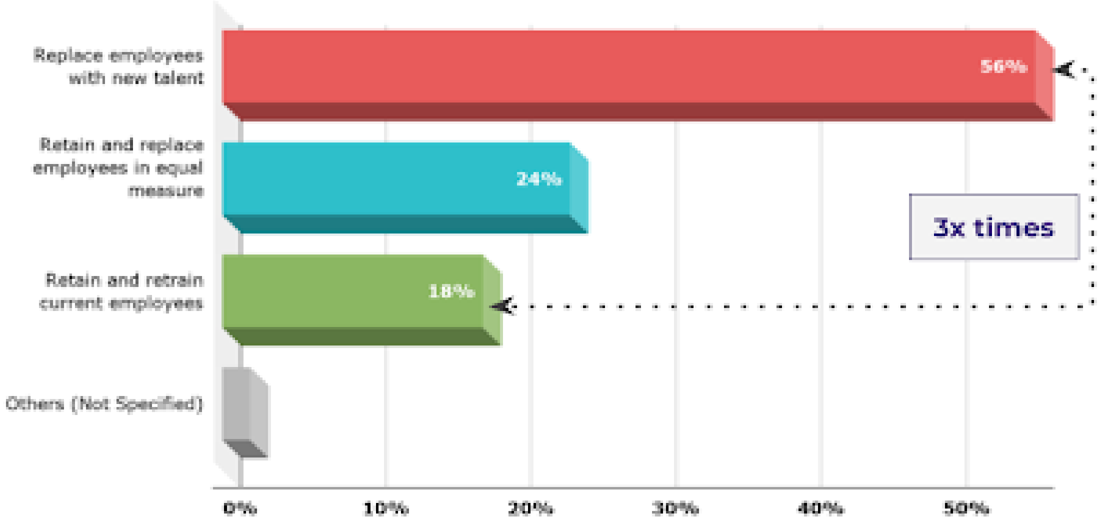
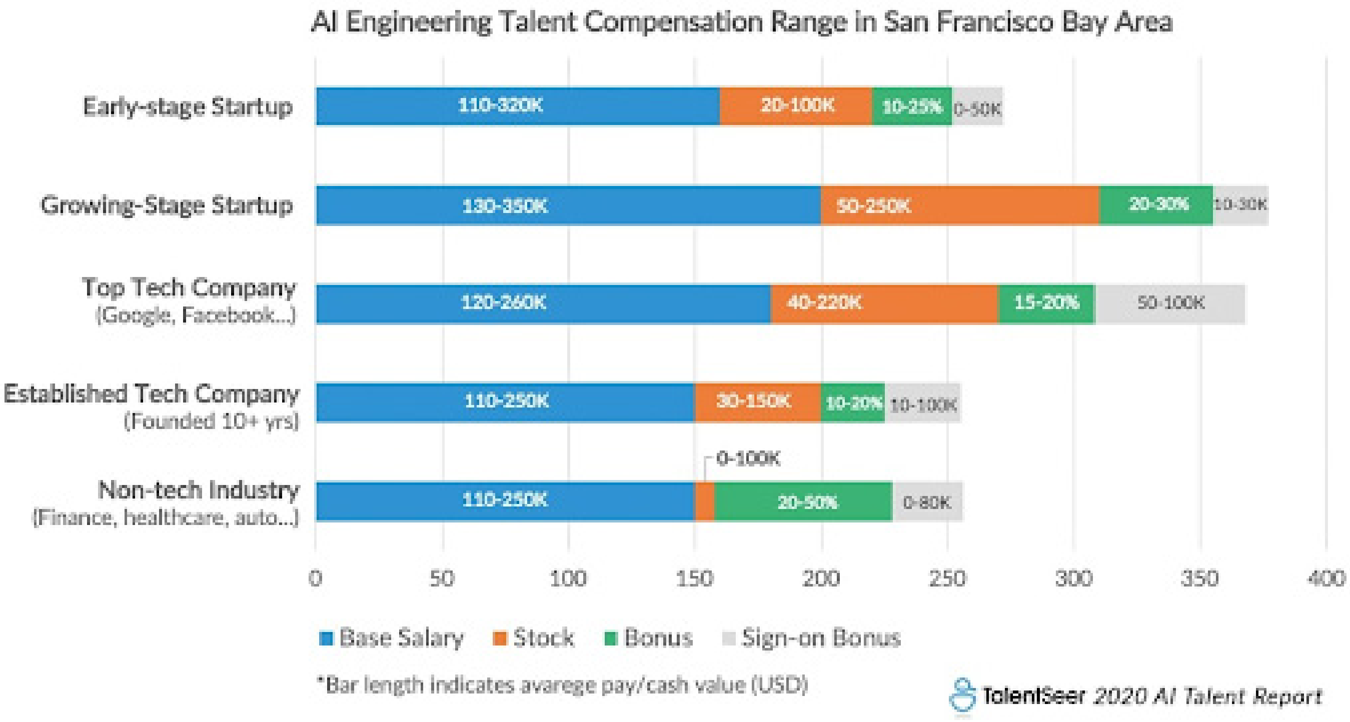


Figure: Trend to hire new talents

The trend shows that AI adopters prefer hiring new AI talents to keeping and retaining current workers. So it poses a challenge on how to retain the current employees. Training programmes, compensation and benefits, performance and leadership management etc are necessary steps for retaining current workers.

Compensation and benefits

Compensation and benefits are crucial parts for Human resource management. Companies should provide compensation and benefits according to industry standards. The following figure shows the AI talent compensation range in the San Francisco Bay Area.


AI Engineering Talent Compensation Range in San Francisco Bay Area

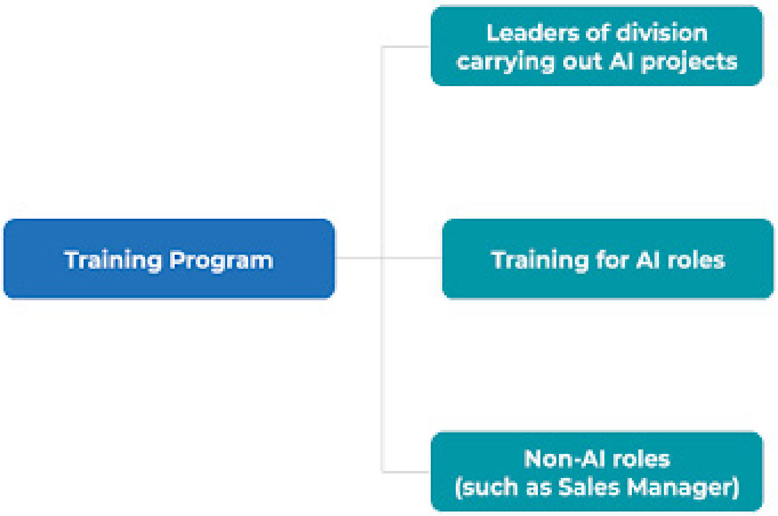
*Bar length indicates avarege pay/cash value (USD)

TalentSeer *2020 AI Talent Report*

Figure: Compensation and benefits

Training and development

Different training and development activities should be carried out within the company for the AI team. For instance training for Leaders of divisions carrying out AI projects should be provided so that they will be able to set direction for AI projects, allocate resources, monitor and track progress, and make corrections as needed to ensure successful project delivery.

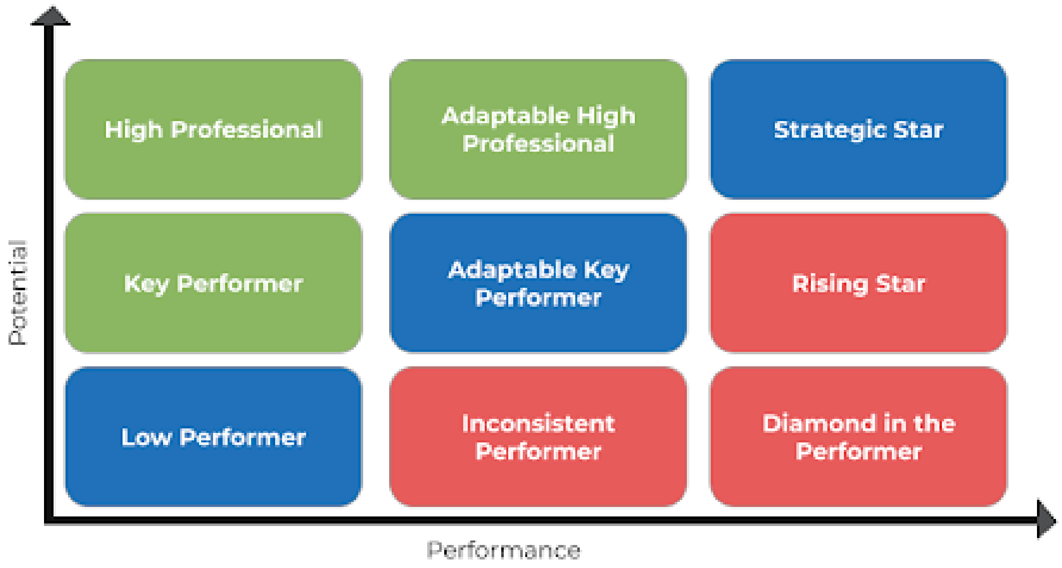

Training Program
Leaders of division carrying out AI projects
Training for AI roles
Non-AI roles (such as Sales Manager)

Training for AI roles should be provided so that the newly trained engineers will be able to gather data, train AI models, and deliver specific AI projects.

Also training for non AI roles such as Product and Sales should be provided so they are aware of the overall process of AI project development.

Performance/Career and Leadership development

The organization can access the performance and potential of the employees with performance and potential matrix. The organization should perform a career and performance review of the AI team. Leadership management for AI roles is also necessary for a successful human resource management.



High Professional	Adaptable High Professional	Strategic Star
Key Performer	Adaptable Key Performer	Rising Star
Low Performer	Inconsistent Performer	Diamond in the Performer

Figure: Performance vs Potential Matrix

3. Implementational and Operational Strategy

A robust AI team has an interdepartmental collaboration and data sharing between various teams. Let’s see various departments of a robust AI team.

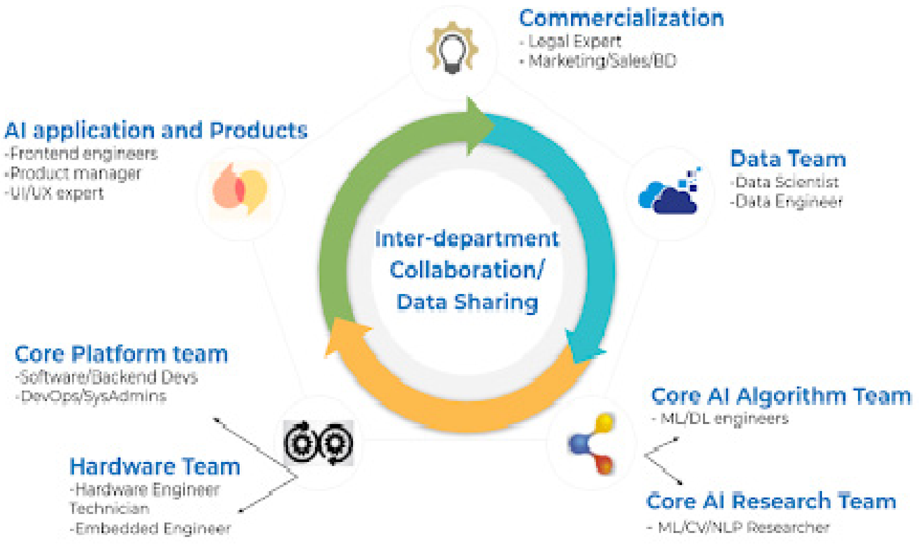


Figure: Various Departments of a robust AI team

The various departments of a robust AI team has:

1. Data team containing data engineers and data scientists
2. Core AI algorithm team containing ML and DL engineers
3. Core AI research team containing ML and DL researchers.
4. Core Platform team containing software, backend and devops engineers and
5. Hardware team containing hardware engineer, technician and embedded engineer.
6. AI application and product team containing frontend engineers and product managers.
7. Commercialization Team containing legal experts and Marketing and sales persons.

Data sharing and inter-department collaboration within every team is necessary in each part of the project development lifecycle for consistency and successful implementation of the project.

Engagement Process to Implement AI

At fusemachines we perform a three phase engagement process to implement AI.

In Phase I,

- We understand business requirements
- We assess and understand the data and
- We prepare and annotate the data

In Phase II,

- We select the features
- We train the model
- And we validate the model

In Phase III,

- We optimize the model
- And finally, we deploy Model

PhDs are involved in the discovery phase to understand business requirements and to understand and prepare data and in the deployment phase to optimize the model.
Team Lead involves all phases and AI engineers and developers annotate data, select features, train and validate data and optimize and deploy the model.

In all of the phases we collaborate with business people throughout the process to validate the business objectives.

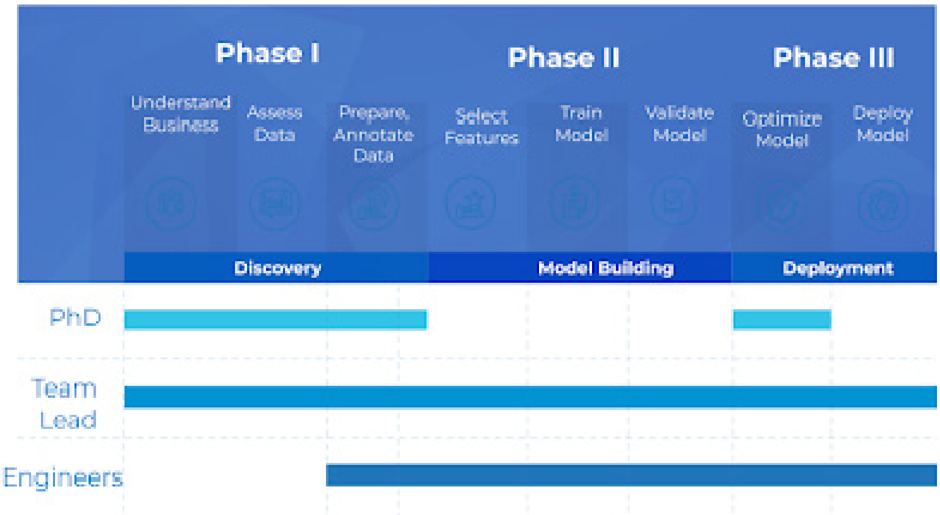


Figure: Engagement Process to implement AI

Implementing AI with CRISP-DM

Business Understanding

Business understanding involves several processes such as requirement gathering and feasibility analysis.

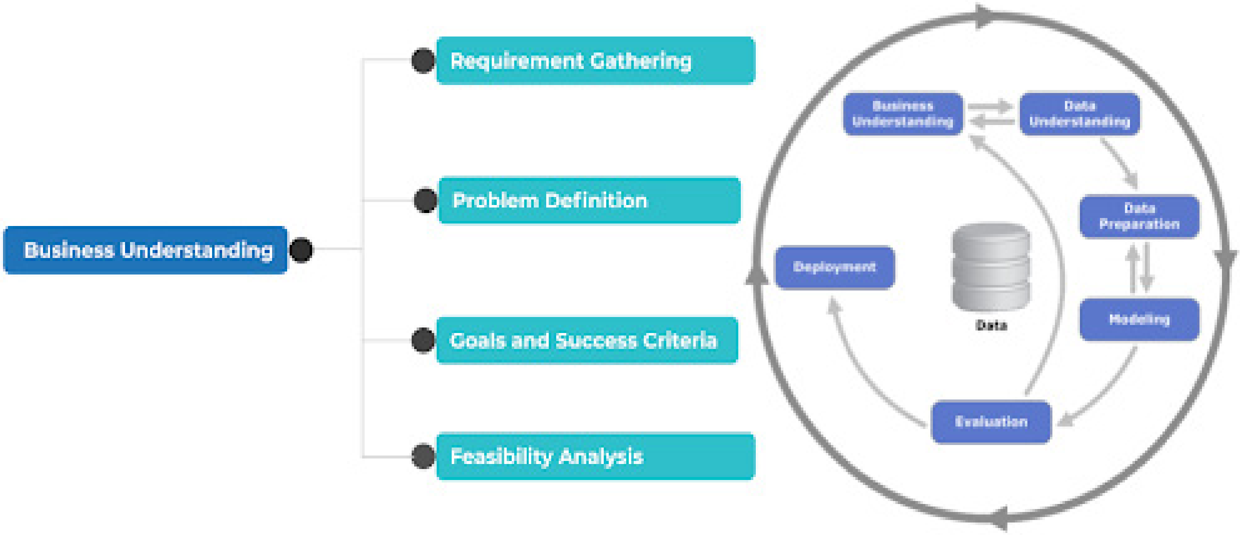


Figure: Business Understanding with CRISP-DM

It is necessary to gather the requirements of the problem such as required resources and requirements, risk, costs and benefits. The requirement gathering process should include Business Questions such as what can be done to increase revenue, decrease cost, improve certain processes etc? The questions such as which data are we using? Which features are important, which Model is preferable? What are we trying to Predict and how does it improve the business?

After the requirement gathering process we formulate the problem and define the goal and success criteria for the project. Success criteria can be either business metrics (such as increase in revenue or decrease in cost etc) or the model accuracy metrics. The success criteria of the problem should be defined clearly with the required feasibility analysis.

At Fusemachines, we perform business diligence with the AIDR framework.

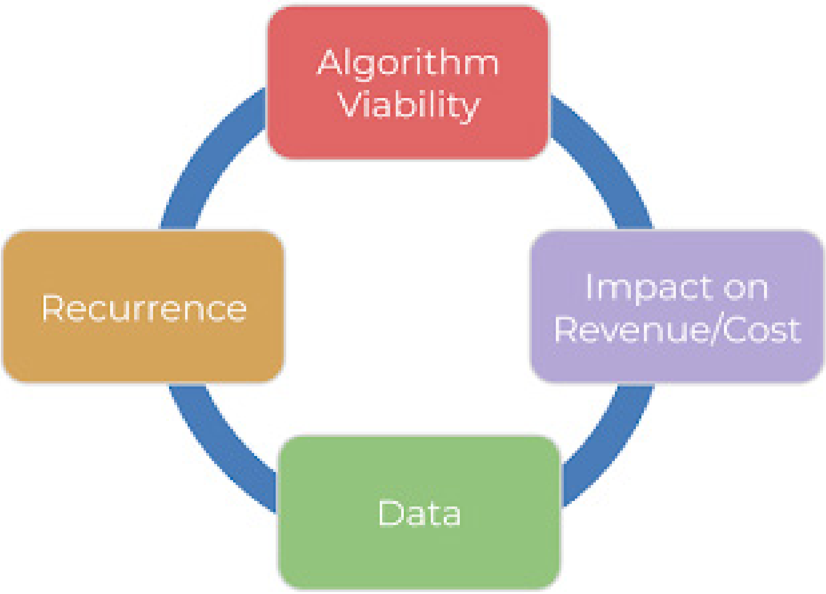


Figure: AIDR Framework

In the AIDR framework, at first we validate the viability of the problem and its solution. We then consider the impact on revenue or cost for the product. We access and check the quality of the data and we also check the consistency or the recurrence of the problem.

Data Understanding and Preparation

Data understanding and preparing is the most time consuming task. It covers almost 80% of the project task. Remaining 20% of the task is required for model training, optimizing and deployment of the project.

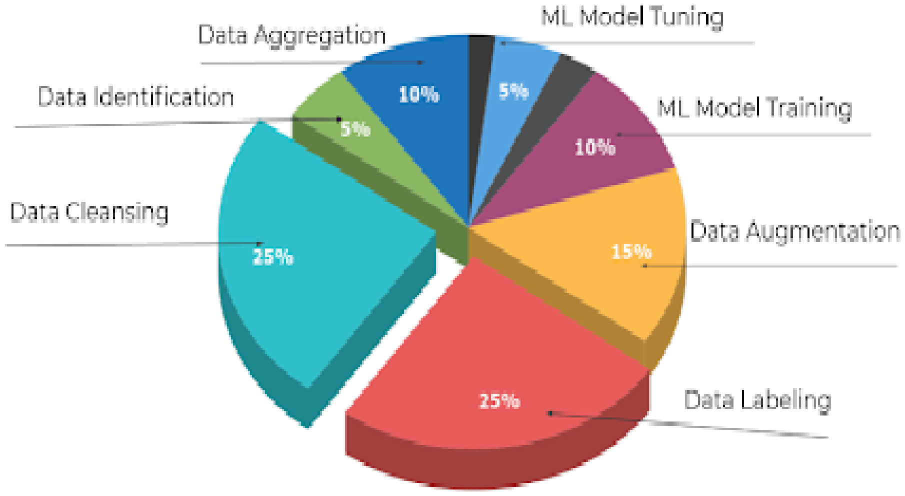


Figure: Percentage of time allocated for machine learning projects

Model Development and Evaluation

In the model development strategy, we should either predict the scores or classes or cluster the data according to the problem definition. One should also set the right metrics to evaluate the performance of the model. For instance a regression task is a problem where data is mapped to scores and the required metrics for the problem could be MSAE or R square. The right model should be chosen for the type of problem and suitable metrics should be defined for the problem to meet the business objectives.

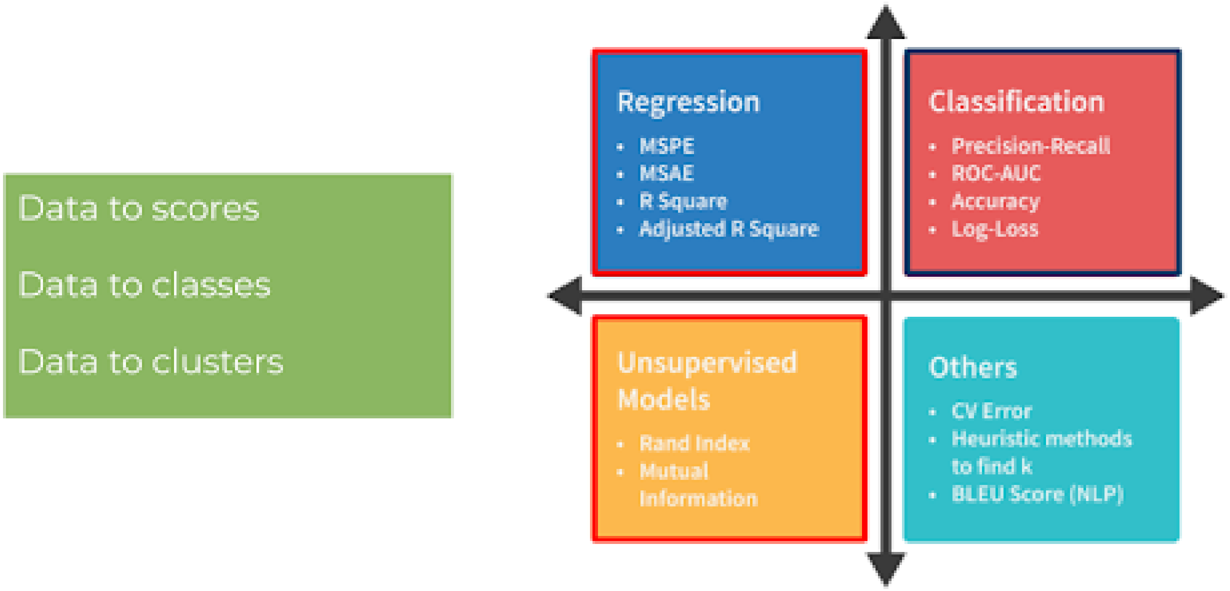


Figure: Algorithm Dev, Model Training and Evaluation

MLOps

MLOps is a practice for collaboration and communication between data scientists and operations professionals to manage production ML lifecycle. The aim of MLOps is to increase automation and improve the quality of production of machine learning projects while focusing on business and regulatory requirements. MLOps applies to the entire lifecycle - from integrating with model generation and deployment to health, governance and business metrics.

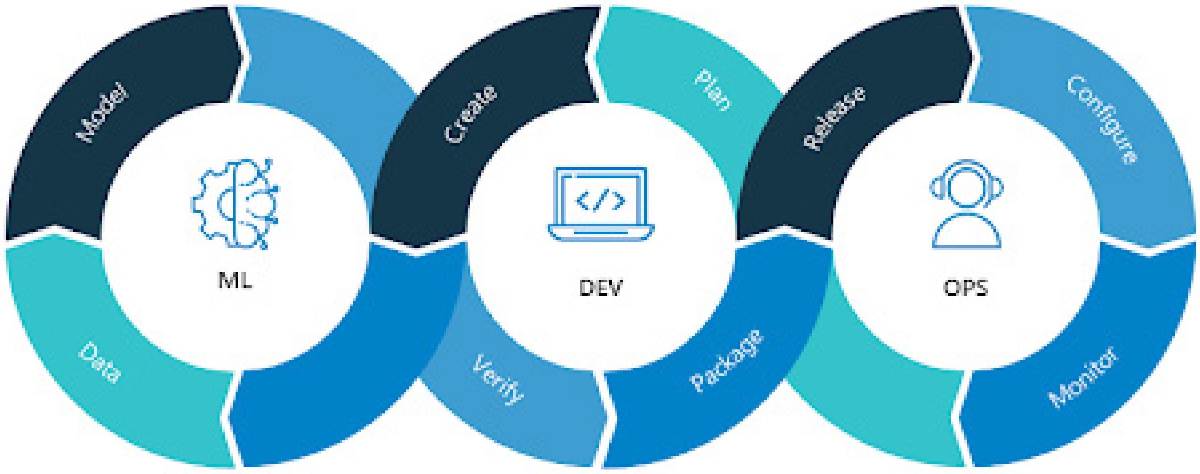
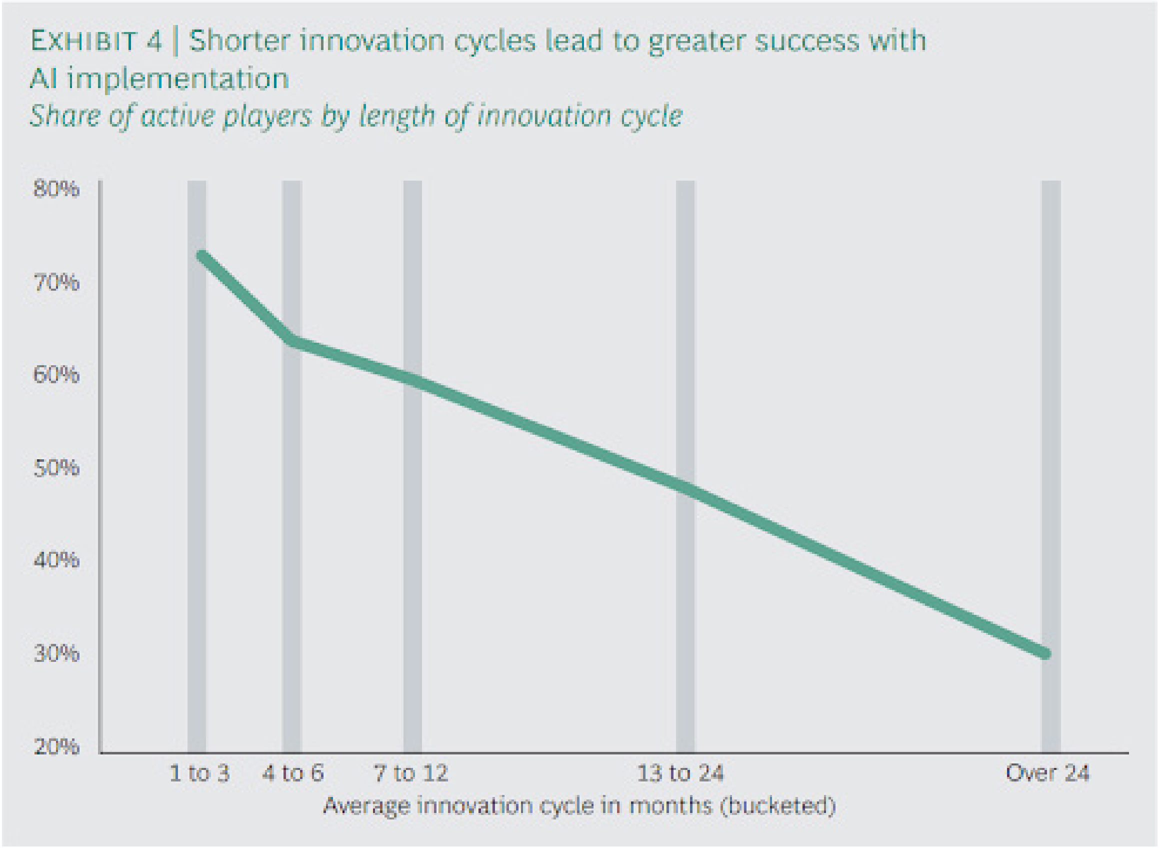


Figure: MLOps

The time taken for overall implementation of an AI product may vary according to the nature of the AI product.



Source: Mind the (AI) Gap,
Sylvain Duranton, Jörg Erlebach, and Marc Pauly,
December 2018

Figure: Innovation Cycle for AI products

It is found that the shorter innovation cycles lead to greater success with AI implementation. The following curve shows that the shorter innovation cycle from one months upto 1-2 years led to greater success with AI implementation.

Key Problems in AI Implementation

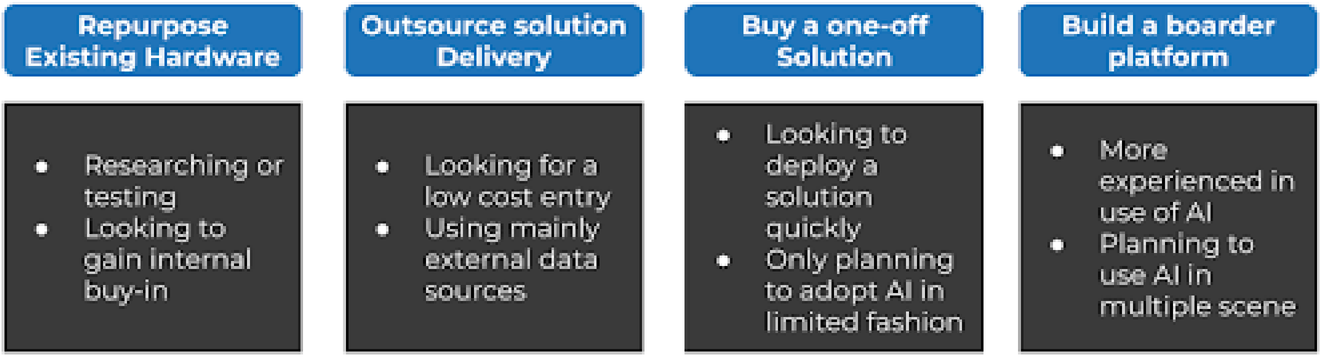
The major problems faced in AI implementation are:

1. AI integration on cognitive projects is difficult with existing system and processes,
2. AI technology is expensive to implement
3. AI awareness and education across the company is still a major hurdle.

Now let's see how we can tackle these issues.

Managing System and Resources for AI projects

The existing system and processes might be incapable to integrate cognitive projects. So, we need to acquire new systems according to the need of the organization.The figure below shows the various hardware requirements according to the need of the project.



Repurpose Existing Hardware

- Researching or testing
- Looking to gain internal buy-in

Outsource solution Delivery

- Looking for a low cost entry
- Using mainly external data sources

Buy a one-off Solution

- Looking to deploy a solution quickly
- Only planning to adopt AI in limited fashion

Build a boarder platform

- More experienced in use of AI
- Planning to use AI in multiple scene

Figure: Choose resources according to the need of the project

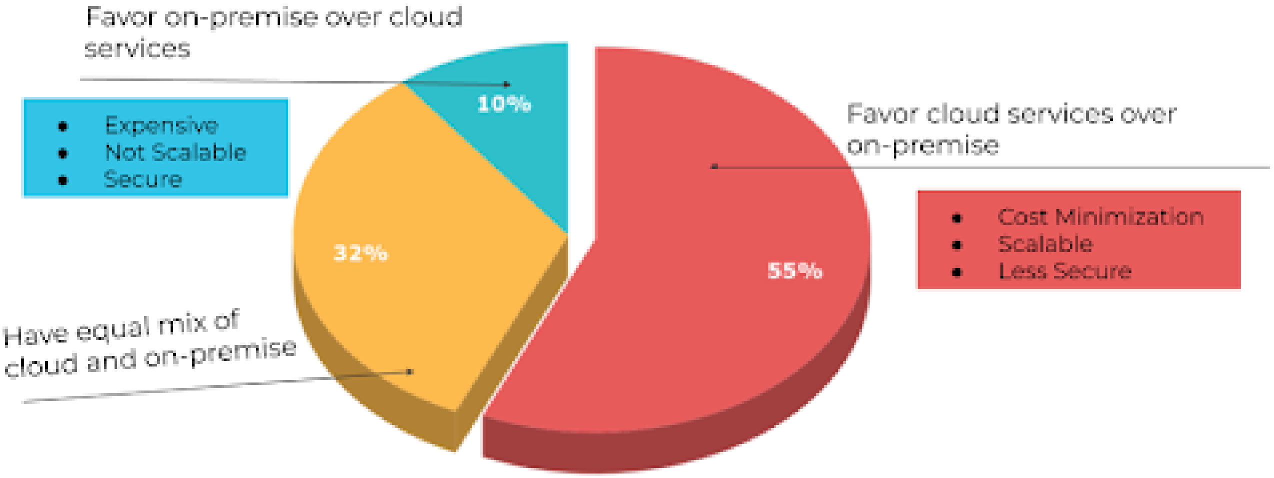


Figure: On-premises vs Cloud Services

However, cloud is less secure than on-premises. On-premise services are expensive and not scalable. However, it is more secure. So, AI startups could rely on cloud services for cost minimization and to gain an initial momentum.

Outsourcing and Insourcing Human Resources

Similarly, acquiring and retaining qualified AI talent is also quite expensive. If one wants to gain a faster initial momentum, outsourcing partners with deep technical AI expertise would be helpful. However, in the long run it would be efficient to execute some projects with an in-house AI team.

Company Wide AI Training

Finally, lack of AI education and awareness can be addressed by providing company wide training. Company wide training is necessary for all teams in an AI company for AI awareness.

1. Training for executive and senior business leaders to understand what AI can do for their enterprise and to begin developing AI strategy.
2. Training for AI Team leaders so they would be able to set direction for AI projects, allocate resources and monitor and track AI projects.
3. Training for AI engineers is necessary so that they would be able to gather data, train AI models, and deliver specific AI projects.
4. And finally AI for non technical staff is necessary so they would be aware of AI tech nology, terminologies and basic understanding of the project workflow.

Venture Funding

Venture capitalists are investing their share for promising AI startups. For instance in 2017 alone, the number of deals for venture capital raised upto 800 deals with 5 Billion dollars investment.

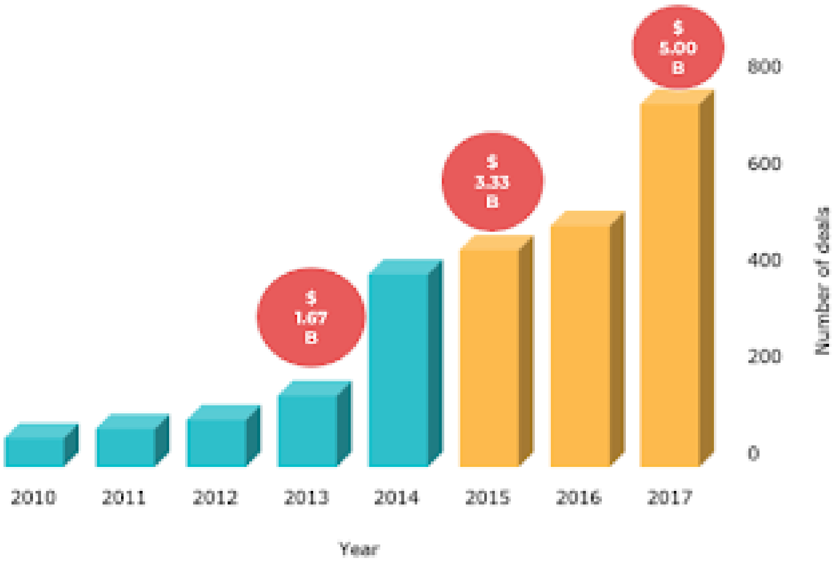


Figure: Venture Funding For AI products

Integrating cognitive projects with existing systems and processes, getting expensive technologies and training and developing AI talent require a huge amount of capital. Venture funding can be one of the alternatives to collect funds for startups with promising business proposals.

4. Sales and Marketing Strategy

There are several challenges in marketing AI. The following figure shows various issues and challenges on marketing AI.

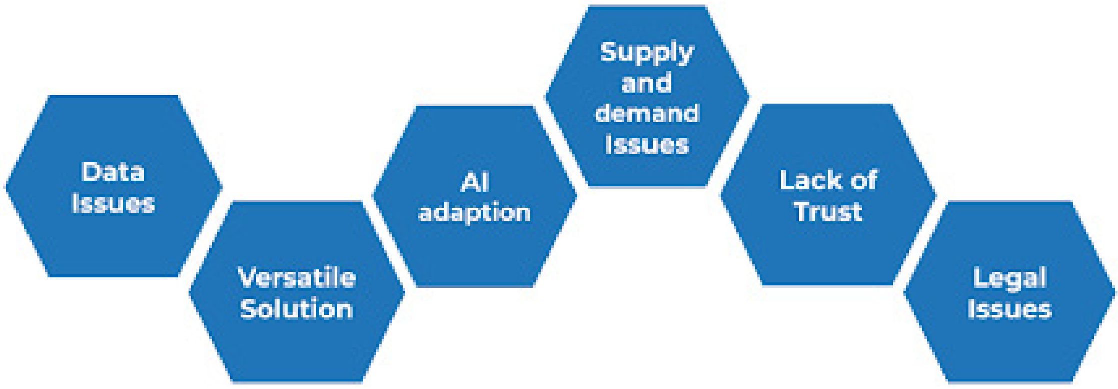


Figure: Challenges of Marketing AI

Let's briefly see how these issues affect marketing AI.

1. There are businesses who do not have sufficient data to start. And there may be other businesses that may have decades long unusable data. Stale and obsolete data pose a challenge for Marketing AI.
2. AI products are not versatile and it can not upgrade to multiple business problems and solutions. The solution for one specific problem will not be valid for another type of business problem.
3. Adoption of AI in business is a costly affair. Startups and small businesses do not separate funds available like the tech giants to implement AI into business operations. Moreover, integrating AI to existing systems is complex and expensive.
4. AI products require GPUs and TPUs which are very costly and hard to manage. Supply and demand issues for computational needs is another barrier for marketing AI products.
5. Lack of trust in AI due to bias, over expectation and hype is another hurdle for marketing AI products.
6. The AI products may not be legally viable. This poses another challenge for marketing AI Products.

Now, let's see how to overcome these challenges.

Apprehension of Responsible AI system

One of the key ingredients for marketing AI products is through the apprehension of Responsible AI. Responsible AI systems treat all people fairly. Responsible AI systems perform reliably and safely. Responsible AI systems are secure and respect privacy. Responsible AI systems empower everyone and engage people. Responsible AI systems are understandable. And Responsible AI systems make people accountable.

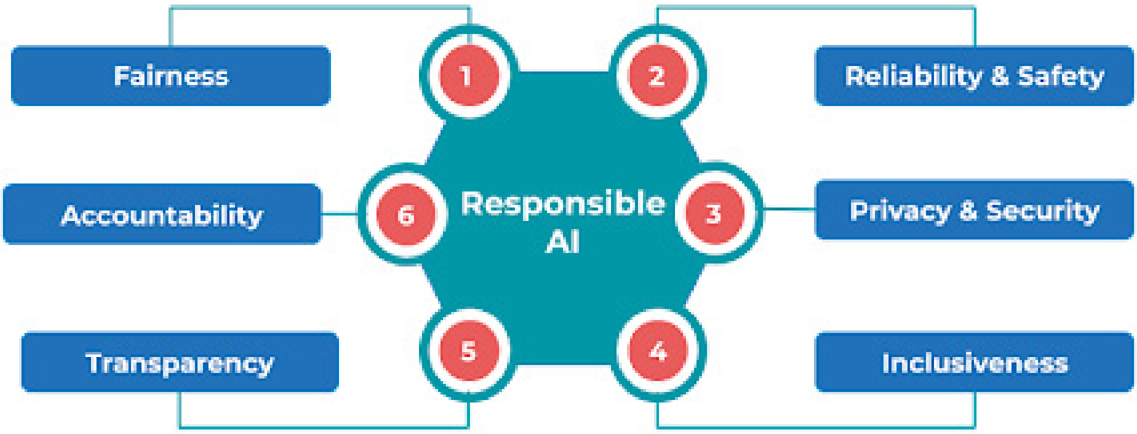


Figure: Responsible AI

It is necessary for a marketing person to provide clear, trustworthy and compelling evidence about the positive benefits AI can deliver. The advantages of AI should be explained carefully and use cases and positive impacts that AI can make to society should be explained carefully.

Marketers should demonstrate the positive impact of AI through the apprehension of a responsible AI system.

Humanize AI

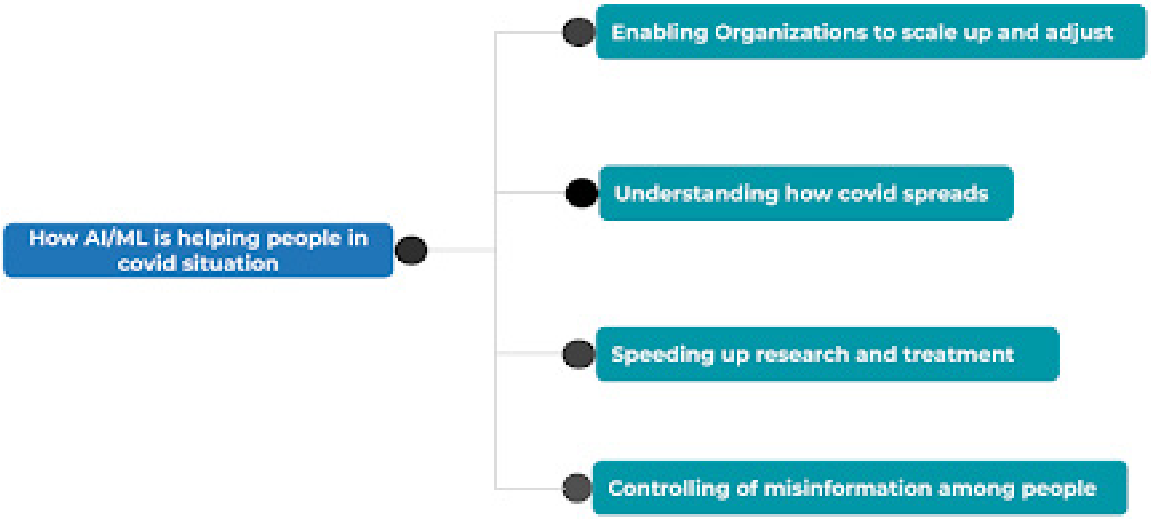
‘Humanizing AI is a significant strategy for marketing AI products. It is necessary to position AI as convenience technology which makes people’s life easier through relatable examples.

Figure: Examples of Humanizing AI

For example, Amazon go and smart mirrors provide a convenient shopping experience. Similarly, Alexa is a virtual assistant and buoy is a smart online symptom checker. One should consider opportunities for promoting AI as more than mere technology – a coach, counselor or companion.

Frame AI as defender that helps people stay safe

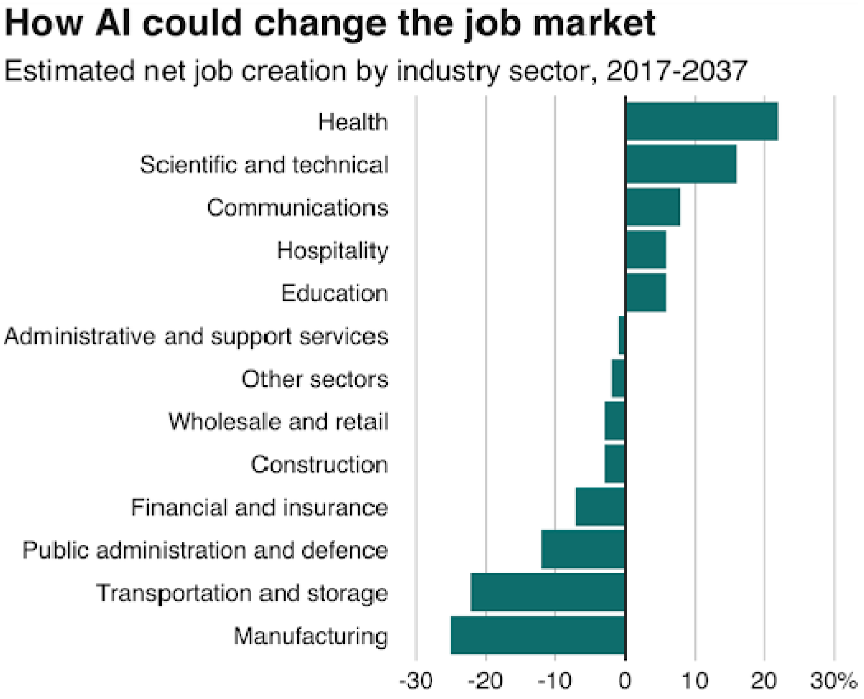
It is necessary to Frame AI as a defender that helps people stay safe and secure.


How AI/ML is helping people in covid situation
Enabling Organizations to scale up and adjust
Understanding how covid spreads
Speeding up research and treatment
Controlling of misinformation among people

For example, in a Covid situation AI enabled organizations to scale up and adjust. It helped to understand how covid spread. AI/ML speed up the research and treatment process. It also helped in controlling misinformation among people.

Communicate AI as augmenting human intelligence

There is a fear among people that AI is here to take their jobs. It is essential for marketers to communicate AI as augmenting human intelligence rather than replacing it. AI frees up workers to more creative tasks by automating repetitive tasks.

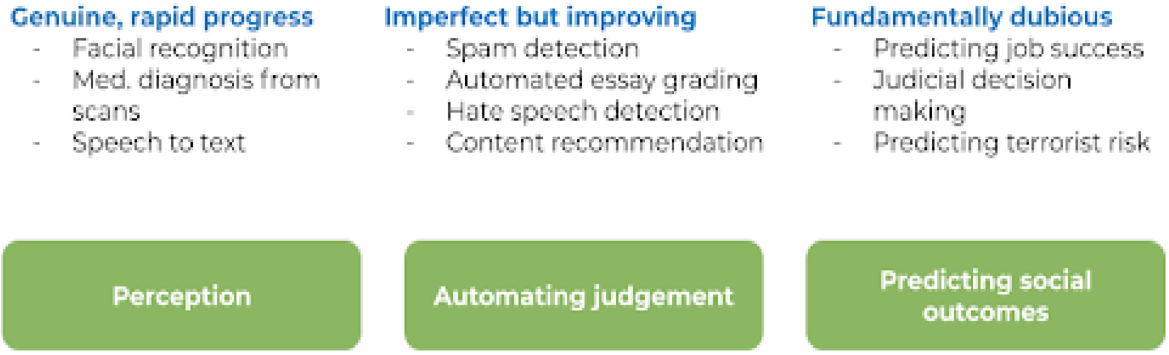


Source: PwC

The following figure shows the potential job loss and job creation by industry sectors. The repetitive and risky tasks such as manufacturing and transportation are likely to be replaced by AI and more jobs are expected to be created in healthcare and scientific and technical sectors.

Sales:

AI has reached a different level of expertise in different types of tasks. The following figure shows the status of various applications of AI.



Genuine, rapid progress
- Facial recognition
- Med. diagnosis from scans
- Speech to text

Perception

Imperfect but improving
- Spam detection
- Automated essay grading
- Hate speech detection
- Content recommendation

Automating judgement

Fundamentally dubious
- Predicting job success
- Judicial decision making
- Predicting terrorist risk

Predicting social outcomes

In perception tasks, applications such as face recognition and speech to text are genuine and making rapid progress using AI technology. In the case of automating judgment tasks, applications such as spam detection and content recommendations etc are imperfect but are improving gradually.

AI is good at some of these tasks, but using AI to predict social outcomes such as job success and risk prediction etc is fundamentally dubious.

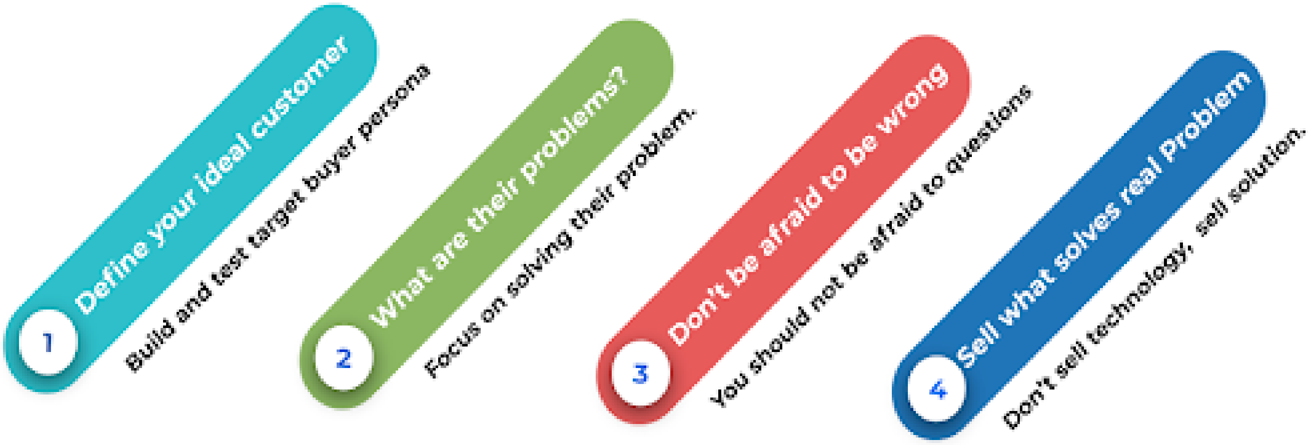
It is easy to over-promise and under-deliver the product so a salesperson should be careful on what AI can deliver and what it can not.

The AI product should be viable and be concrete. And after the initial POC with the customer, the final product should be built within the time frame of the discussion.

If a company is stuck doing POC after POC and never going from pilots to production, that means it is on the wrong path.

Steps to Sell AI products

The general steps to sell AI products are shown in the figure below.


1
Define your ideal customer
Build and test target buyer persona
2
What are their problems?
Focus on solving their problem.
3
Don't be afraid to be wrong
You should not be afraid to questions
4
Sell what solves real Problem
Don't sell technology, sell solution.

While selling AI products,

1. It is necessary for a sales person to define the target buyer.
2. Then it is crucial for a sales person to look from the viewpoint of their ideal customers and what they are seeking in buying the product.
3. It is essential to know their problems and how the AI product that one is selling benefits or solves their problem.
4. The salesperson should not be afraid to ask questions to the customers and get more intuition about their problem.
5. And one should be careful not to sell AI as technology but as a solution that solves real problems.

Marketing Tactics and Channels

The various kinds of marketing tactics and channels are shown in the figure below.

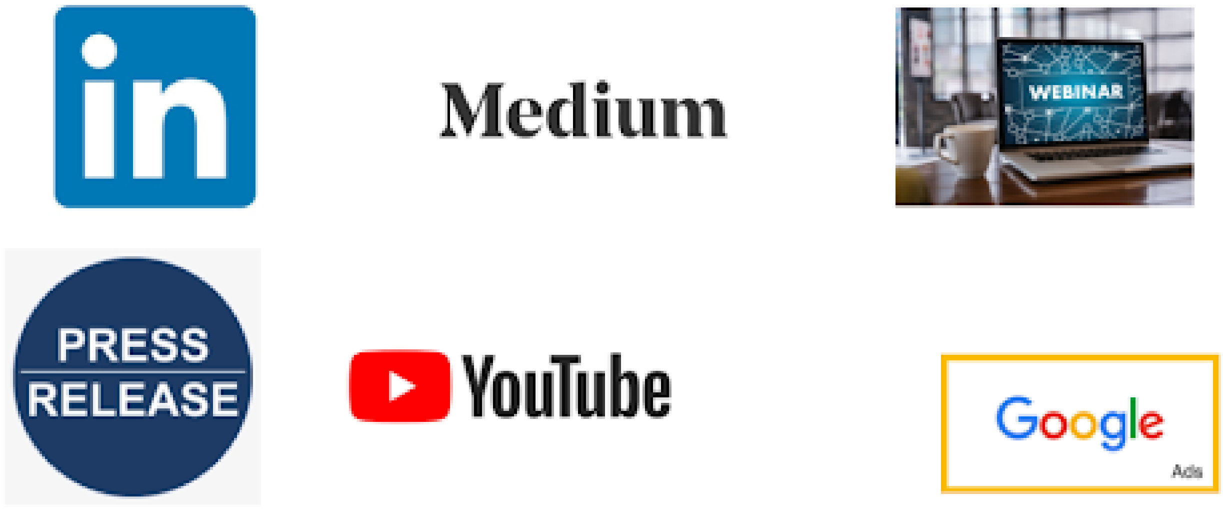
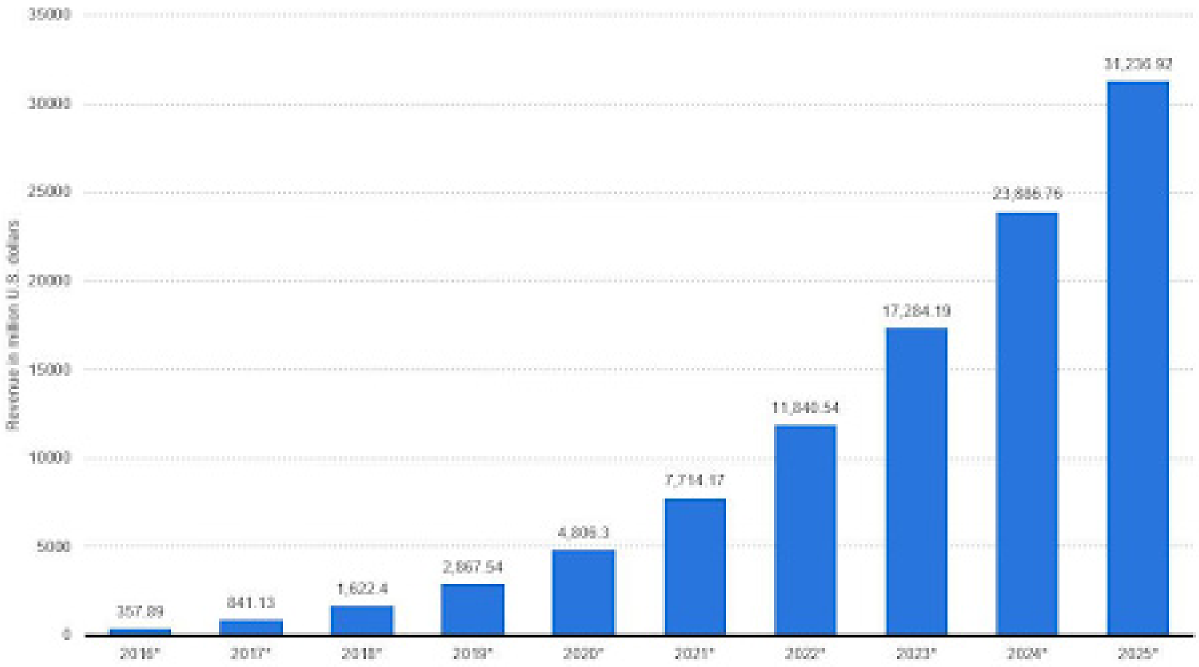


Figure: Marketing Tactics and Channels

Marketing or a sales person should choose the marketing tactics and channels such as blog and LinkedIn posts to generate awareness about AI products. Press releases and webinars can re-engage interest and nurture inactive leads. Podcasts and Youtube channels create a community and build a brand over time. Paid advertisements are a prominent way for marketing AI products.

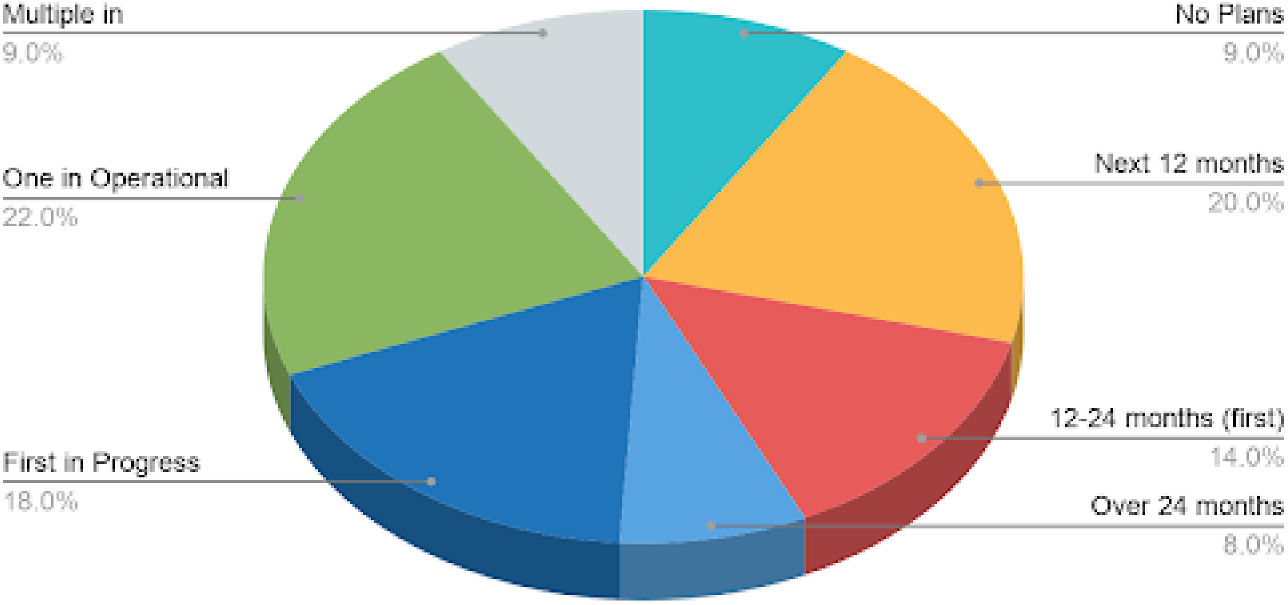
5. Trust in AI

As the AI industry starts to grow, more and more businesses adopt AI that has been puffed up to be godlike in its capabilities. Not only that, it is getting rare to find any technology venture that is not using AI. Image recognition and tagging, patient data processing, localization and mapping, predictive maintenance, use of algorithms and machine learning to predict and prevent security threats, intelligent recruitment, and HR systems are a few of the many enterprise application use cases predicted to fuel the projected rapid growth of AI in the enterprise. A study showed that the revenue generated from enterprises with AI assistance would grow from 1.62 billion in 2018 to 31.2 billion by 2025 monotonically. It also shows that the industry is projected to grow a massive 26 billion within the next five years, a staggering amount.



Source: Statistia

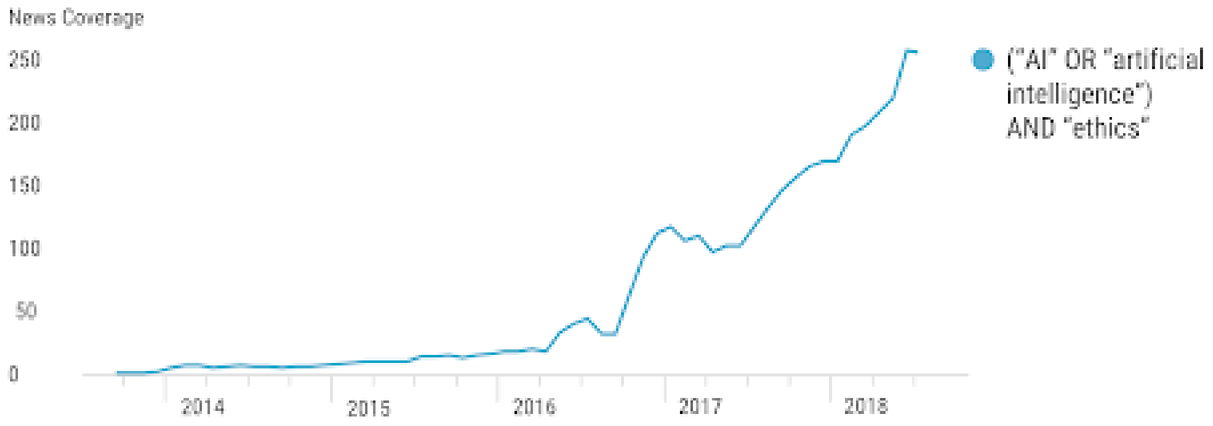
Despite such high expectations for AI, in a survey conducted among 1500 decision-makers in multiple industries and regions, **only 9% of the business enterprises have incorporated AI into their product/service offerings with multiple AI projects in place.** Further, 9% are yet to make any plans, and over 40% have at least one project running.



Source: Cognilytica, 2020

However, as technologies' influence continues to grow in our lives, a vital question emerges: **What level of trust can--and should-- we place in these AI systems?** Will these systems make decisions that humans will perceive reasonably, and will these decisions be aligned and aware of the human values & norms? Trust is a social bond that allows humans to bond with other humans, its environment, and even technology. With keywords like "Trust in AI," "Trustworthy AI," or "Trusted AI," organizations like European Union and IEEE refer to maintaining explainability, bais free predictions, accountability, transparency, privacy and ethics in AI.

But it has been very evident that AI can not only be used to bring positive changes and reforms, it can also be used to bring negative impacts on society. Not only the steep increase in revenues for many businesses, the number of news coverages on ethics in AI and its challenges has also been in an increasing trend as shown in the figure below.

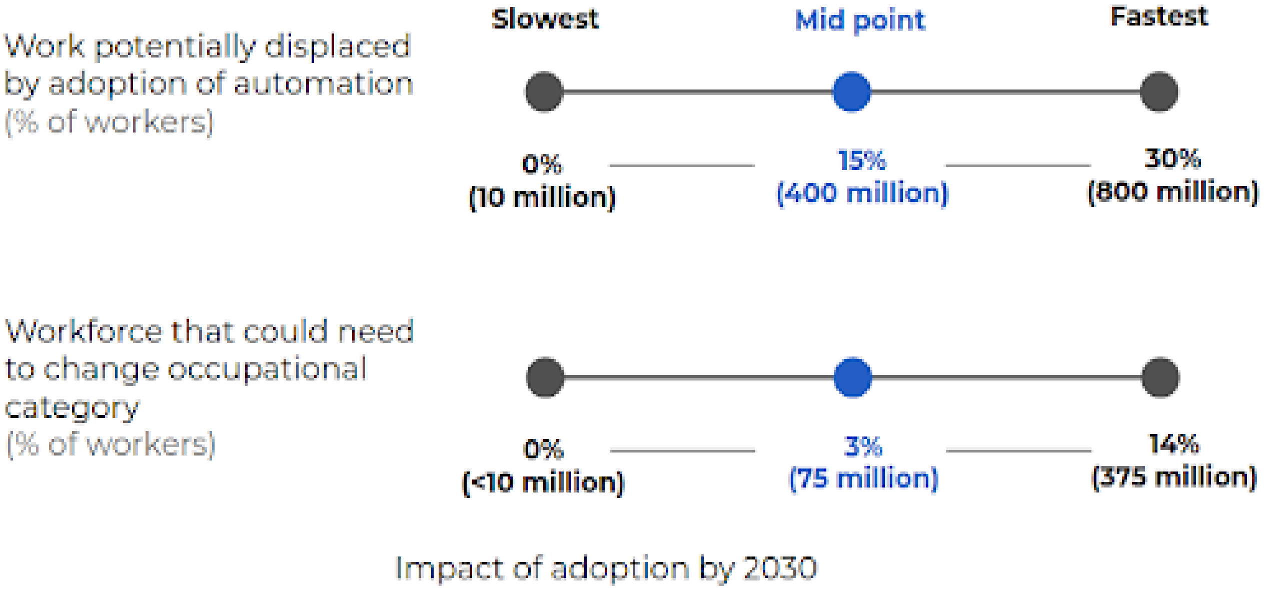


Source: *CSINSIGHTS*

Some of the most common ethical issues concerning AI and its applications are:

- **Job loss and wealth inequality**
  As integration of AI and its applications continues to grow, one's single primary concern is the jobs of the future. Automation with AI means many people losing their job and quite possibly their livelihood. The latest study compiled by Mckinsey Global Institute proclaims that by the year 2030, as many as 800 million jobs could be lost worldwide to automation and over 375 million people are in urgency to change their occupational category as shown in the figure below.

  Similarly, the economy's current scenario is to pay the workforce an hourly wage, pay the government with the tax and other expenses. However, what happens when we introduce AI automation in the picture? These automated machines work tirelessly without having to be paid and are not liable to tax. The company's profit saved from payable tax and reduced wages creates an imbalance in the wealth distribution among the stakeholders and the employees..



Source: *J. Manyika et al.: McKinsey*

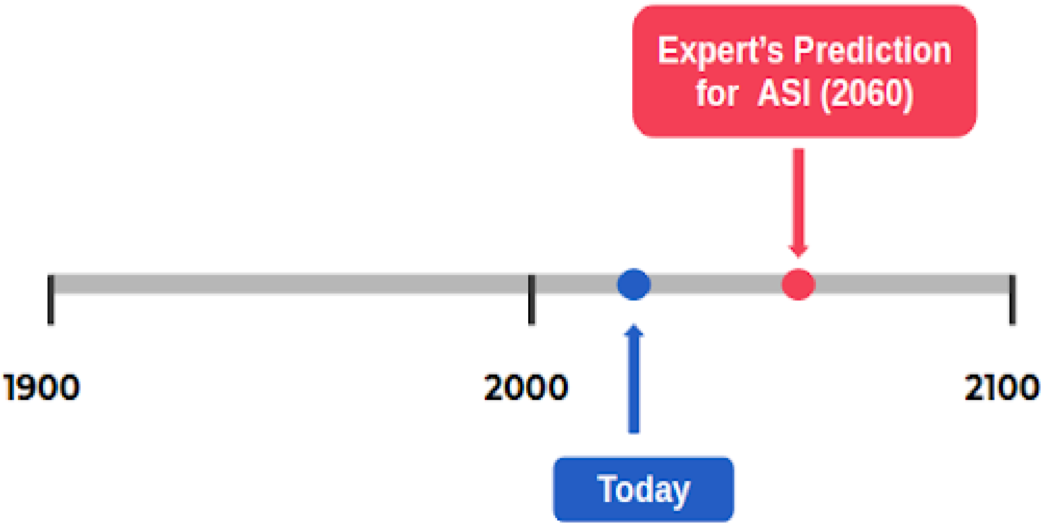
- **Imperfect AI**
  AI and Machine learning algorithms are fueled by the data they are provided. With useful data, AI can perform well, but when AI is fed with insufficient data and potential developing errors, each prediction, and tasks performed by AI can be harmful as they are not immune to making mistakes. A profound example of such imperfection can be best understood by taking the example of Tay, Microsoft's AI chatbot, which was trained using tweets from Twitter users. The bot soon learned to *spew racists slurs and Nazi propaganda* and was immediately stopped. So, an imperfect AI is a significant ethical concern.

- **Should AI be allowed to kill?**
  There are AI softwares that writes its own updates and renews itself which implies that the machine is not programmed to do what the programmer wants it to do rather it does what it learns to do. An incident with a computerised gun, Tallon, fired killing 9 and injur ing 14 demonstrates the seriousness of AI with the ability to kill.
  Similarly, the presence of predator drones carrying armed missiles invokes the necessity for laws and regulations to monitor the use of such applications of AI.

Source: *J. Manyika et al.: McKinsey*

- **Rogue AIs**
  Since we know that AI is prone to mistakes, it is quite obvious to assume that an AI can go rogue or create unintended consequences from its actions in pursuing seemingly harm less goals. Movies like Terminator, Avengers-End game, and TV shows demonstrate the possibility of an intelligent AI-powered system refusing to be under human control. It is only a matter of time when AI-powered supercomputers give these intelligent machines the ability of self-awareness and consciousness. These concerns have been dwelling since the dawn; nevertheless, they need to be adequately addressed.

- **Singularity and Keeping Control over AI**
  The point of time where technological advancement surpasses human intelligence is termed as "*technological singularity*". Although with speculative statistics, most of the opinions from experts in the AI community believe 2060 is a very reasonable estimate for the arrival of potentially world altering ASI (AI that is way smarter than human), which is only 40 years from now.



Source: *Wait but Why (2019)*

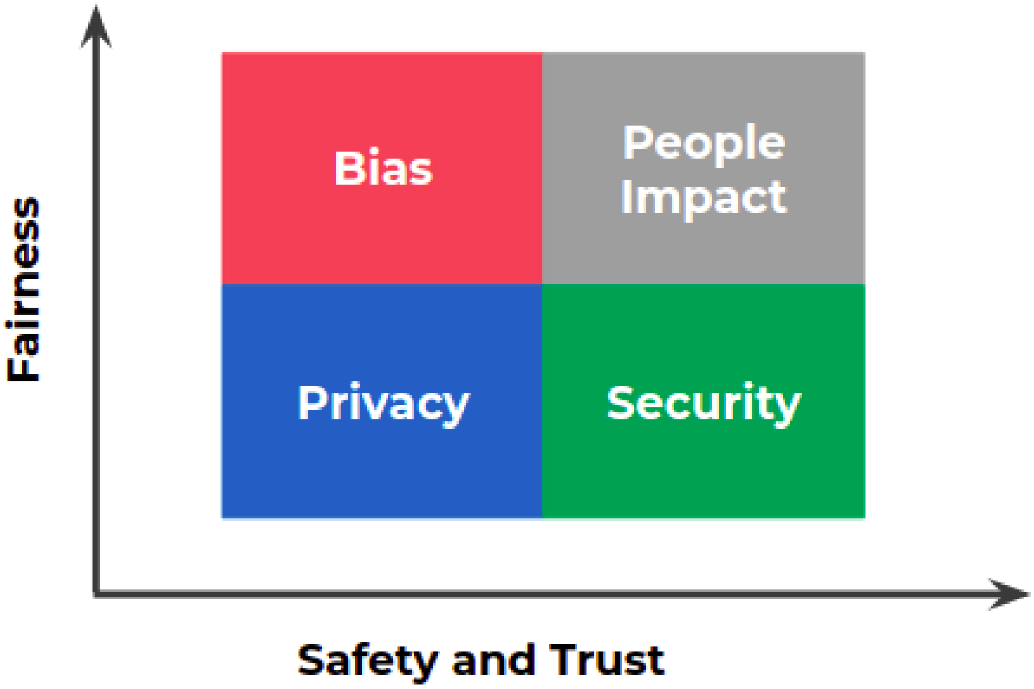
Such singularity is believed to trigger extinction of the human race, which is why the advancement in AI is scary for many people.

- **How should we treat AI?**
  What if such steep advancement in AI and robotics makes them capable of feelings? With feelings, where will AI align in our social status? Should they be given citizenships or rights like humans and animals? Humanoid robot Sophia was granted citizenship in Saudi Arabia. Although this was more of a marketing stunt, it paves the way for AI robots' rights in the future.

Source: *Wikimedia Commons*

- **AI Bias**
  As mentioned before, AI machines are fueled and trained with the data they are provided with. The data used to train these systems can itself be biased for a particular group of community. When such vulnerable information is used to train these machines, the actions performed and the results produced undoubtedly contain biases and irregulari ties. The examples of such biases destroying the reputations of the company are visible over the years. From IBM's *facial recognition software* to *Amazon's hiring automation*, these biases have been proven fatal towards discrimination based on race, gender, reli gion, or ethnicity.

These issues are real and must be addressed for us to trust an AI powered system. In the framework for "Trust in AI" there are two axes: fairness and Safety & Trust.



Source: *JOSH BERSIN (2019)*

These two axes to trustworthy and ethical AI arises primarily allow us to answer the following questions:

- How fair is the data based algorithm you are using? Does the algorithm produce biased free results ?
- Should we be scared of this algorithm and our data being misused? Does the system maintain privacy, confidentiality and security of our personal data? Who can access our data and can they change it as they want?

Furthermore, These dimensions invoke four regions of trust namely:

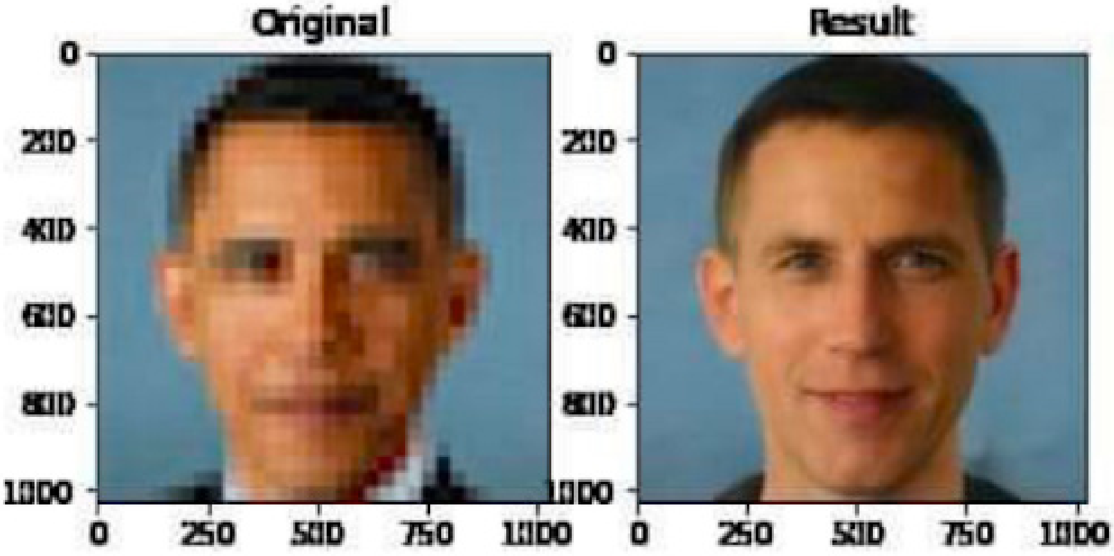
- Bias
- Privacy
- Security &
- People Impact

All the AI applications are primarily based on pre-existing data, and pre-existing data are biased. So trivially, the outcomes generated by an intelligent system are prone to bias and partiality for specific groups. Bias nature of a system revolves around understanding these questions:

- How will my age, gender, race, education, qualifications, income, degree, and other such information be used?
- Are there any preventive measures and screening layers to identify and prevent the biased nature of the results?
- How will the biased nature of an intelligent system affect my personal and professional life?

AI bias results in discrimination of a particular group of people due to false assumptions during the learning process.

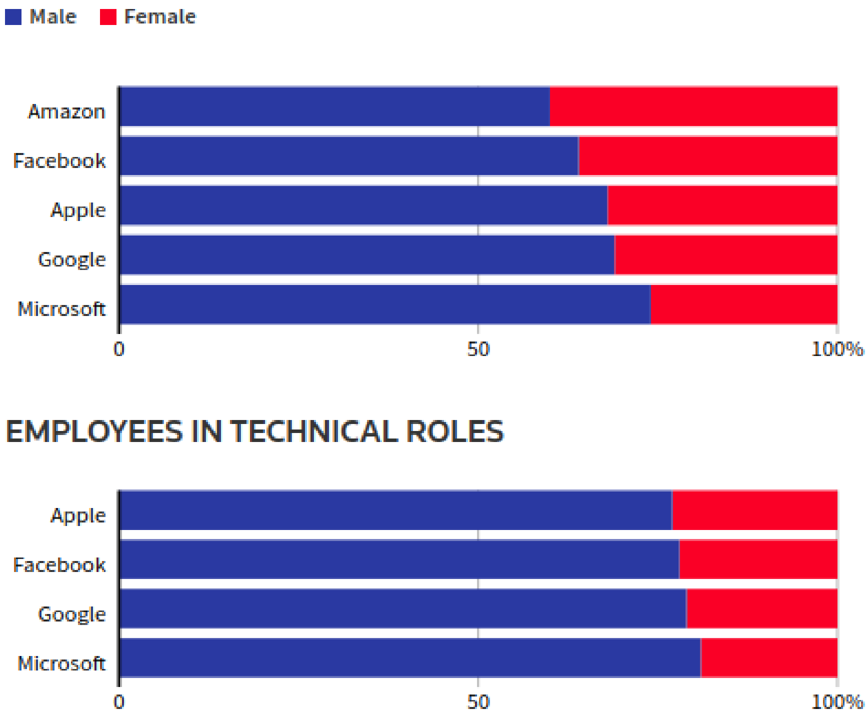
The data collected by human beings, either manually or generated, are never perfect. Every single decision we make involves a certain kind of bias. Similarly, Each of those biases is multiplied many folds while training an intelligent system. Ideally, we would like an intelligent system to make rational decisions free of biases to ensure better social accountability and justice. For example, equal opportunities for individuals and groups (such as minorities) within society to access resources, have their voices heard be represented in society.



Upsampling pixelated image of Obama

Source: @hardmaru on Twitter

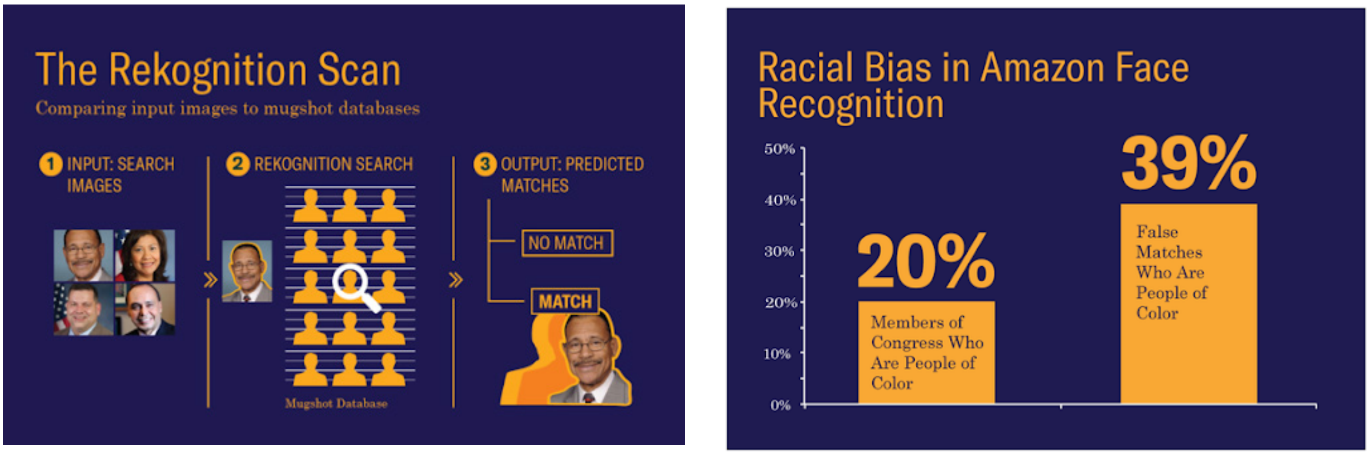
As we can see in the given above figure, a pixelated image of Barack Obama is upsampled to a picture of a caucasian male by a face upsampling machine learning (ML) model amplifying racial inequality instead of alleviating it. The upsampling system was initially trained on *FlickFaceHQ*, which primarily contained images of white people. Since the machine learning algorithm best fits the attributes that occur frequently and the original data is found to be already biased towards the darker race, the results from the model upsampling are nothing out of the ordinary. Similarly, another example demonstrating the gender-based biased nature of an intelligent system is **Amazon's automatic recruiting tool.** Amazon's recruiting automation showed bias against women because the computer models were trained to vet applications by observing patterns in resumes previously submitted to the company over ten years. As most of the applications came from men, it is evident that the data to the model was biased



Han Huang | REUTERS GRAPHICS

To already a male dominated industry, such automations further aids in increasing that gap. The above figure represents a global headcounts of employees by sex/gender in leading tech companies. As one can see the results are clearly unilateral.

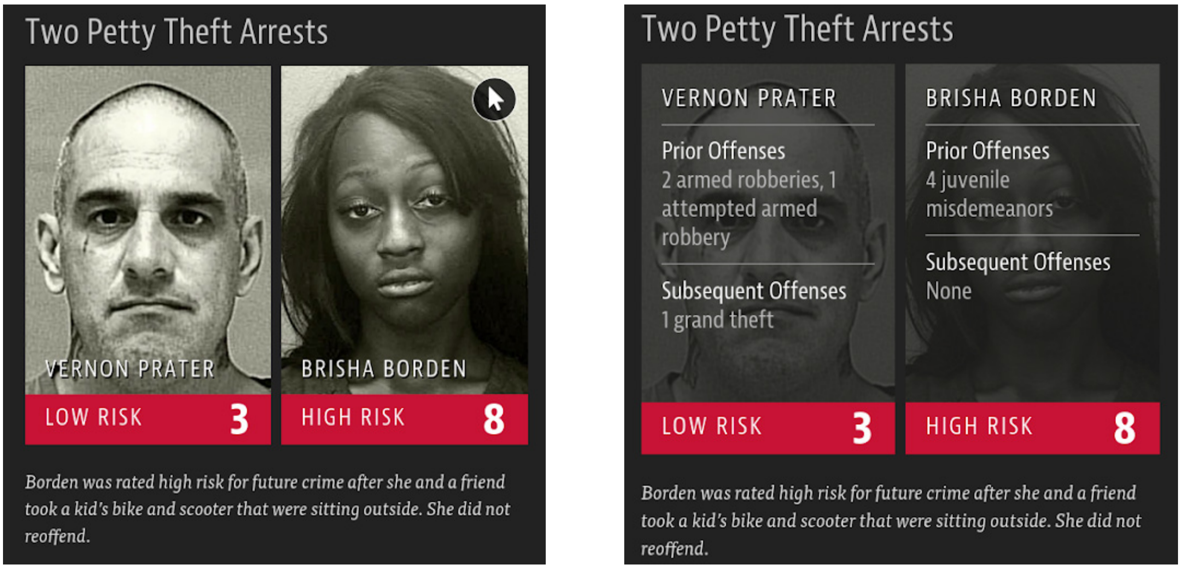
Continuing with the examples of machine learning and AI bias we also have Amazon's face recognition software that falsely matched twenty-eight members of the Congress with the samples of mugshots.



Source: *J. Snow: American Civil Liberties Union (2018)*

To conduct the test, the exact same facial recognition system was used that Amazon offers to the public, which anyone could use to scan for matches between images of faces. With this test the software, *Rekognition*, incorrectly matched 28 members of the Congress identifying them as people who have been arrested for a crime.

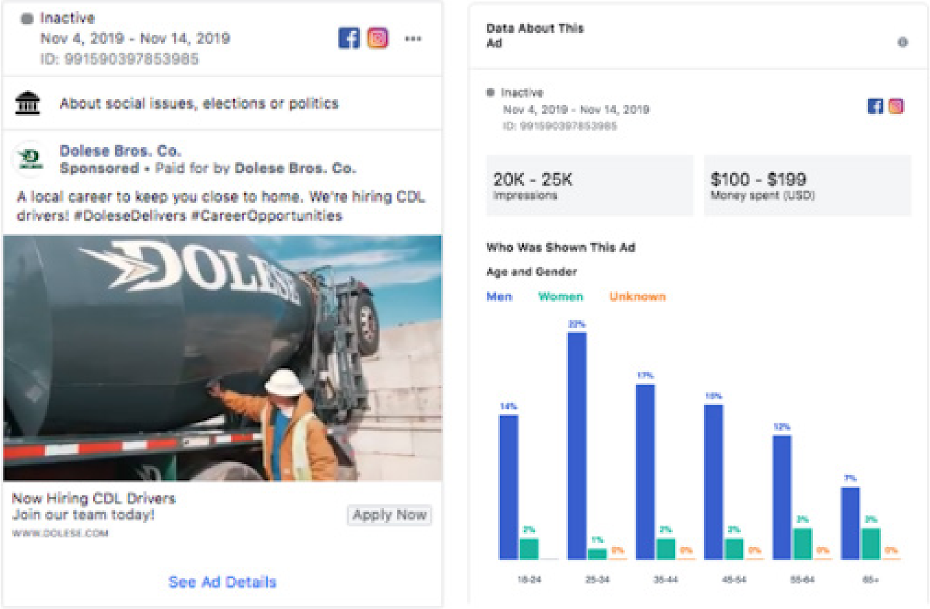
Similarly, one of the most prominent examples of bias nature of AI is the **COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)** algorithm used in US court systems to predict the likelihood of a defendant committing further crimes.


Two Petty Theft Arrests
VERNON PRATER
BRISHA BORDEN
LOW RISK 3
HIGH RISK 8
Borden was rated high risk for future crime after she and a friend took a kid's bike and scooter that were sitting outside. She did not reoffend.
Two Petty Theft Arrests
VERNON PRATER
Prior Offenses
2 armed robberies, 1 attempted armed robbery
Subsequent Offenses
1 grand theft
BRISHA BORDEN
Prior Offenses
4 juvenile misdemeanors
Subsequent Offenses
None
LOW RISK 3
HIGH RISK 8
Borden was rated high risk for future crime after she and a friend took a kid's bike and scooter that were sitting outside. She did not reoffend.

Source: *Machine Bias, ProPublica.org*

When the COMPAS algorithm was asked to score each of the defendants in the figure above, the woman on the right who is black was rated a high risk compared to the man on the left who was rated a low risk solely based on their colour of the skin. Such racial disparities are a result of false assumptions during the training process itself and needs to be corrected.

Finally there is Facebook. In 2019, Facebook's advertising algorithm was intentionally targeting adverts according to gender, race, and religion. For instance, women were prioritized in job adverts for roles in nursing or secretarial work, whereas job ads for janitors and taxi drivers had been mostly shown to men, in particular men from minority backgrounds.



● Inactive
Nov 4, 2019 - Nov 14, 2019
ID: 991590397853965

About social issues, elections or politics

Dolese Bros. Co.
Sponsored • Paid for by Dolese Bros. Co.

A local career to keep you close to home. We're hiring CDL drivers! #DoleseDelivers #CareerOpportunities

Now Hiring CDL Drivers
Join our team today!
WWW.DOLESE.COM

Data About This Ad

● Inactive
Nov 4, 2019 - Nov 14, 2019
ID: 991590397853965

20K - 25K
Impressions

$100 - $199
Money spent (USD)

Who Was Shown This Ad

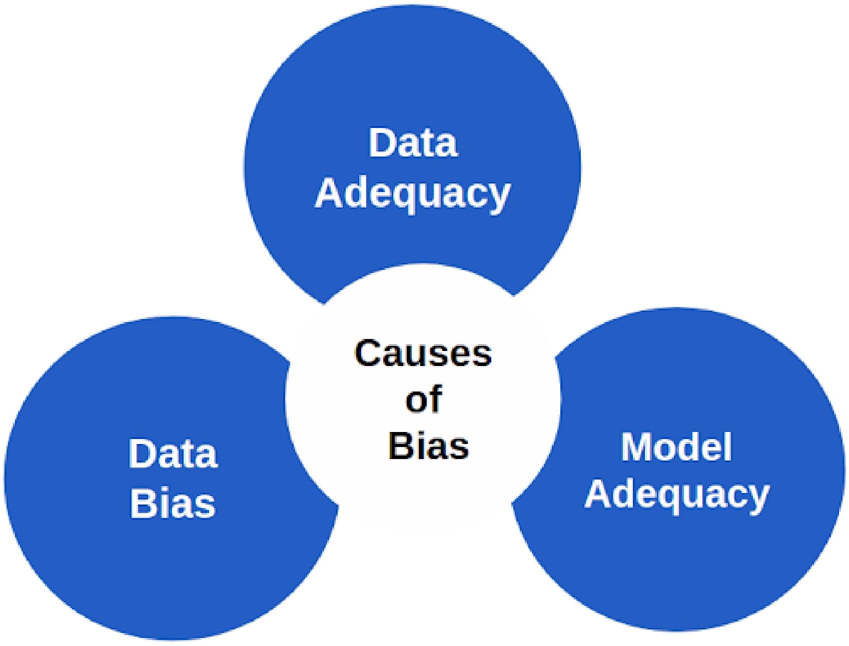
Age and Gender

Source: *A. T. Ava Kofman: ProPublica (2020)*

In an ad posted by a company via Facebook's new ad portal, among the 20,000 people who had seen it, 80% of them were men as the ad featured the need of a longtime driver in a hardhat. It seems like Facebook targeted mostly men considering gender and age when finding audiences as per the requirement of these ads.

These examples only show a small portion of the bulk biases that has been going around with machine learning and artificial intelligence. Biasness decreases the potential of artificial intelligence for business and society by encouraging mistrust and producing distorted results. Bias is all of our responsibility and it will be crucial to reduce bias if AI is to reach its potential and earn people's trust in the systems.

There are many possible causes of bias in machine learning predictions. Three of the most distinctive ones include:



- **Data Adequacy:**
  Data adequacy refers to the infrequent and specific patterns down weighted by the ma chine learning model with the aim of learning the abstract concept and generalisation. In doing so, the minority records can get unfairly neglected. Shortage of balanced data may occur because of unmanaged data collection or removal of instances because of missing values or simply because the group membership is small or more. The biased nature of Amazon's recruiting automation is caused due to data inadequacy.

- **Data Bias:**
  Data bias occurs when although the data is enough to represent each group, training data may reflect existing prejudices like female workers with less wages which are very hard to remove. Such irregularities embedded in the original data causes data bias.

- **Data Adequacy:**
  Data adequacy refers to the infrequent and specific patterns down weighted by the ma chine learning model with the aim of learning the abstract concept and generalisation. In doing so, the minority records can get unfairly neglected. Shortage of balanced data may occur because of unmanaged data collection or removal of instances because of missing values or simply because the group membership is small or more. The biased nature of Amazon's recruiting automation is caused due to data inadequacy.

- **Data Bias:**
  Data bias occurs when although the data is enough to represent each group, training data may reflect existing prejudices like female workers with less wages which are very hard to remove. Such irregularities embedded in the original data causes data bias.

- **Model Adequacy:**
  The architecture of the machine learning model may describe some groups better than others. For example, a classification model architecture may suit one group of data more the other creating biases in the final prediction or results.

It is only fair to discuss the ways to manage bias after we have completed the cause. So, six potential ways to manage bias in an intelligent system for AI practitioners and business and policy leaders are:

- **Context of use:**
  It is important to be aware of the context in which AI can help correct bias as well as where there is a high risk that AI could exacerbate bias. Not only that being aware of the domains that are more prone to unfair bias and avoiding such domains in integration with the company automatically reduces much work load.

- **Testing and Mitigating Bias**
  It is a must to establish a process and practices that promotes testing and mitigating bias. Use of tools that highlights the potential sources of bias in data and traits that influence the outputs heavily. With identification there should be a proper system in place that helps to resolve such bias be it, proper data sampling techniques, data collection techniques or even feature engineering.

- **Human Decisions**
  One should engage in fact based conversations about potential biases in human deci sions. As AI reveals more and more about the decision making process, it is mandatory for policy makers to revisit the assumptions, laws and proxies made in the past regarding AI.

With AI, organisations should consider how human driven processes might be improved in the future.

- **Working Together with Machines**
  One should consider the possibilities of working together with AI, as it might be a com pulsion sooner than one anticipate. One can explore situations where processes can be automated and processes that require a human presence. Combining both the processes can help to reduce bias. Checking recommendations suggested by AI before sending it to the customers can be an example of human and AI working together.

- **Investing in Research**
  Making more data available for research and investing more in bias research will always prove to be valuable for any organization with an adoption of a multidisciplinary approach to continually consider the role of AI in decision making.

- **Diversifying AI**
  A more diverse AI community will be better equipped to anticipate, spot and review issues of unfair bias and better able to engage communities likely affected by bias. So investing more in diversifying the AI field will prove to be beneficial.

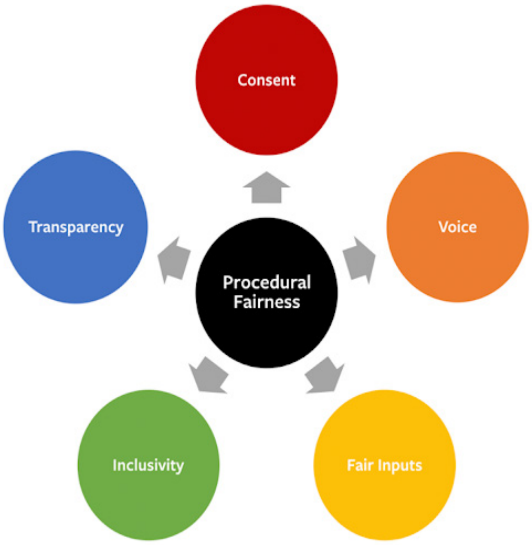
These measures are without a doubt a small part of the solution in mitigating bias in AI. The nature of bias differs exponentially with every domain and so do the ways to tackle, reduce and eliminate them. A major part of the difficulty in ensuring that AI makes unbiased decisions is on the basis of the definition of fairness. Any fair decision can be deemed as unfair from another point of view. So it is important to describe the definition of fairness if we are to understand the unbiased nature of AI.

So, what does it mean to call something fair?

The concept of fairness usually balances a moral evaluation of two things:

- The decision making process by which goods deeds and harms are decided, also known as procedural **fairness**.
- The equality and inequality of distribution of goods or harms resulted from the decision making process above, also known as the **distributive fairness.**

Procedural fairness measures the integrity of the process rather than the result itself. The overall integrity and robustness of the decision making process is paramount for procedural fairness.



Source: *T. A. Lab: LaptrinhX (2020)*

In procedural fairness there are five key elements to consider fair for overall fairness:

- **Transparency**
  The decisions made by the predicting model should be interpretable and explainable on the basis of the data used to arrive at the predicted outcome. Similarly, there should be a transparent process showing the overall decision making process and the rules and data that are being used.

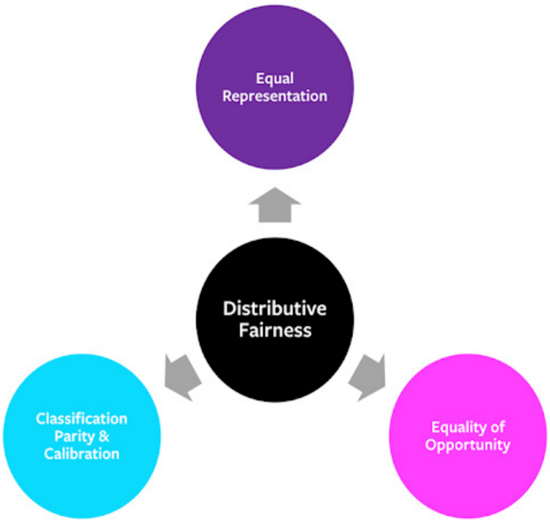
- **Consent**
  With consent one is concerned if people can consent to the process that affects them and do they have any recourse to appeal decisions? How are their data being used? Does it align with the consent they have agreed to before?

- **Voice**
  Voice represents people's opportunity to be heard. People want to have a voice and a two way dialogue with the platform as having a voice empowers people to speak up for the outcomes, provide feedback and question the overall working process.

- **Fair Inputs**
  Do people have reasonable control over the features used to assess them and are these features "fair assessments" of the outcome of interest?

- **Inclusivity:**
  This element of procedural fairness queries about the people who are involved in the training process of the intelligent system. Training data can be biased or underrepresent ed. Inclusivity requires data to include a balance set of all the representatives as the devel opment and the prediction of the model solely depends on this set.

Similarly, Distributive fairness evaluates the distribution of goods and harms from the decision of the system and the overall process. Like procedural fairness, it is paramount for distributive fairness to assess the equality and inequality of the system.



Source: *T. A. Lab: LaptrinhX (2020)*

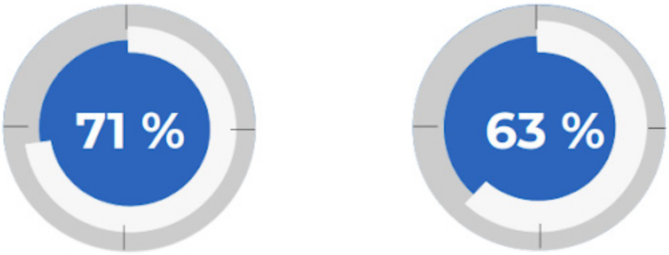
The three key elements of distributive fairness includes:

- **Equality of opportunity:**
  This requires that the opportunities be equally distributed to the people and not condi tionally on their demographic identity(e.g: gender, race, sexuality, disability etc.)

- **Equal Representation**
  Algorithms can under represent or over represent particular groups. So, this element relates how equally distributed outcomes are for specific groups and ensures that each and every class or groups are equally represented regardless of the overall bias.

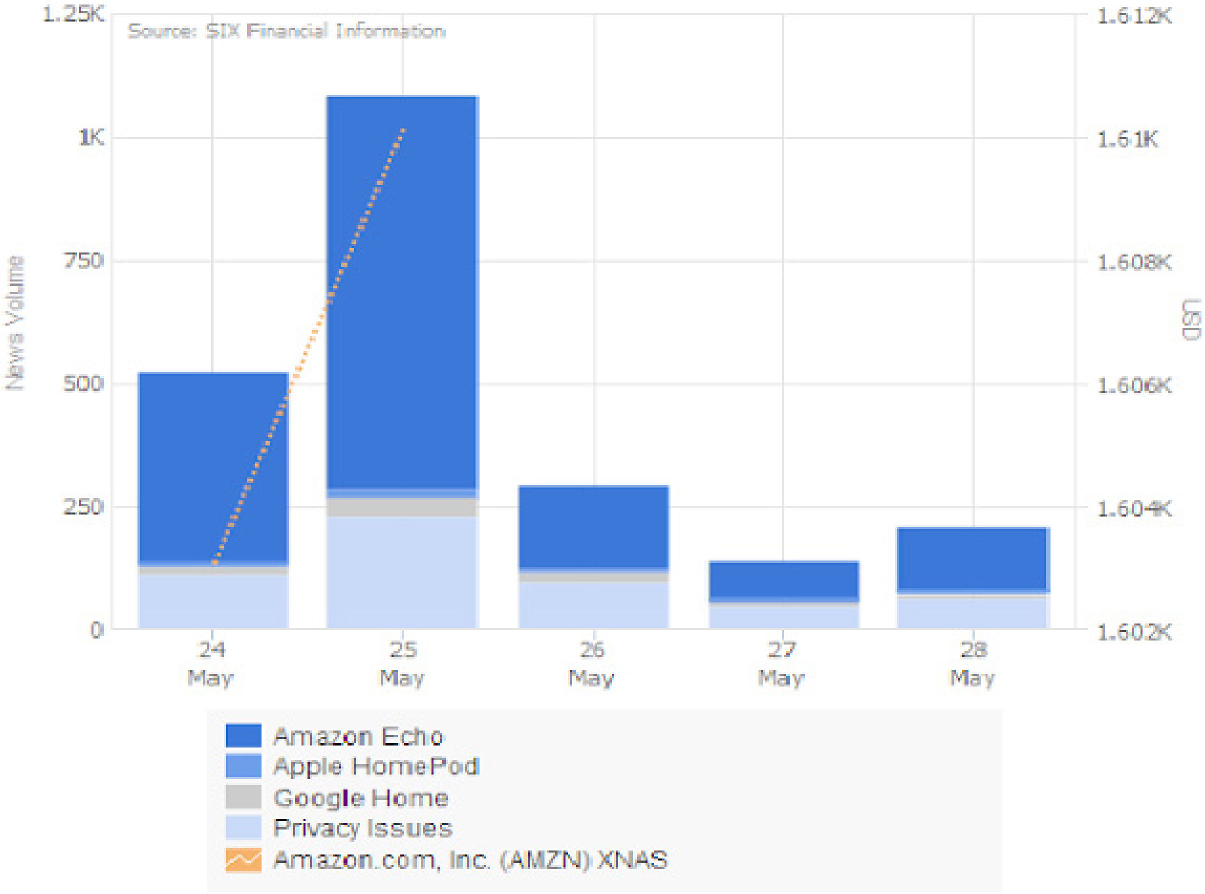
- **Classification Parity and Calibration:**
  Also known as Equality of Accuracy and Error, this element of distributive fairness evalu ates the predictive accuracy of the predicting model across every group and also the error rates of every prediction.

Understanding bias and fairness completes the first region on the dimension of trust. Second, there is Privacy.



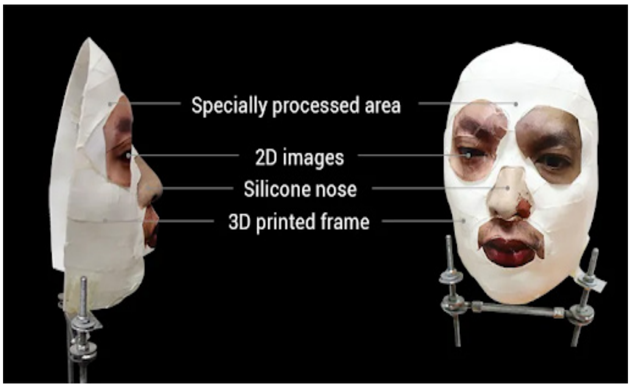
Source: *Genpact, 2018*

Upon conducting a survey among 5000 respondents in Australia, UK and the US, nearly 71% of the respondents did not want AI in business if it infringed on their privacy whereas two thirds ie.e 63% of the respondents worried that AI will make decisions that will impact their lives without their knowledge.



Source: *SIX Financial Information*

Similarly, Amazon's Alexa powered Echo made headlines after reports stated that the smart speaker recorded a family's conversation and sent the audio to someone in the device's contact list. With concerns of such privacy, it is no surprise for the increase in news volume in general and especially in privacy concerns as shown in the figure above. These smart devices know what you are searching for, knows what you are listening to and knows what messages you send. So, it automatically becomes the gateway for your personal information to be leaked to companies like Amazon, Google and more.

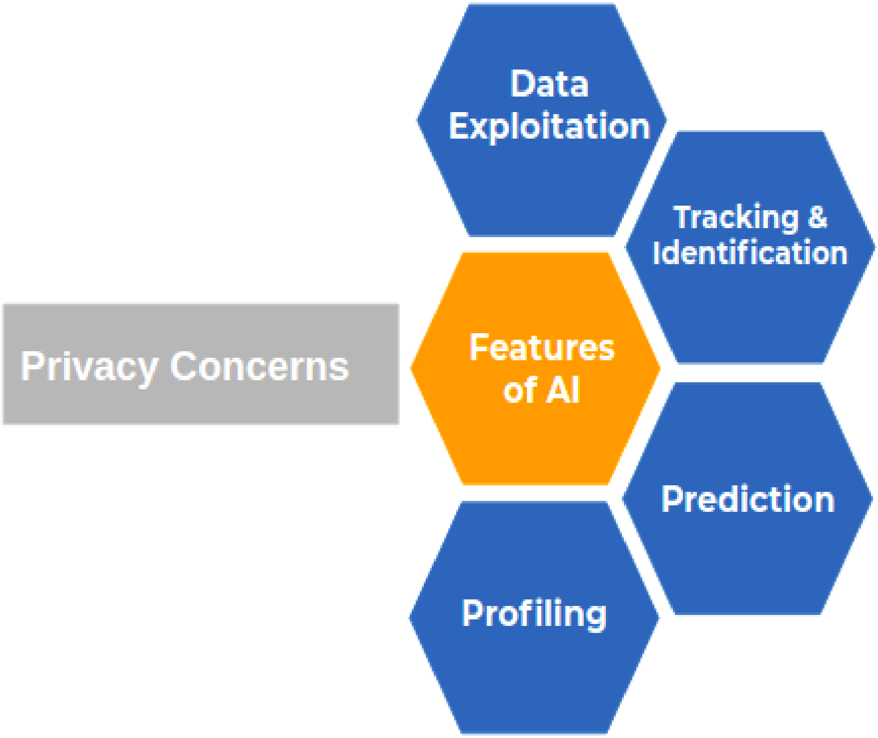


Source: *A. Greenberg: Wired (2017)*

Talking about privacy concerns with a smartphone, Apple's smartphones are sold in figures of hundred millions but the fact that they can be unlocked with a composite mast of 3-D printed plastic raises alarming issues of privacy.

Researchers in a security firm in Vietnam, stated that they were able to crack the Face ID in Apple's smartphones using a cheap mix of materials, 3-D paintings and two dimensional printed eyes. "We just need a half face to create the mask. It was even simpler than we ourselves had thought.", they said. Epitome of locking mechanism, but just some few seconds to crack and get through to all the personal information doesn't particularly preserve privacy. A device so popular, and almost in the hand of every three out of four people can get unlocked with a simple 3D printed is not only an issue of negligence, but also a big threat to privacy.

To understand the nature in which an individual's privacy can be inflicted, one should understand the characteristics of AI that allow it to affect privacy. With the characteristics like speed of processing any information, scale at which it can run computation, automation without any supervision and prediction only using the past data allows AI to raise privacy concerns.



Source: *M. Deane: Medium (2018)*

Some of many, features of AI which inflict privacy concerns are discussed below:

- **Data Exploitation**
  A number of consumer products from automated home assistants to mobile applications, each of these tend to have features that are collected, stored and processed in some way that allows them to have more human interaction. Rapid increment of reliance of digital technology in day to day life, makes it more convenient and efficient to exploit data. These data are the key to private life and exploitation, a stab in right to privacy.

- **Identification and Tracking**

  The advancements in image recognition, object detection and facial recognition techniques don't care about one being anonymous as they have the potential to de-anonymize the data based on identification and tracking across multiple devices that you work, live and travel. Multiple iterations through the social media portals could easily reveal one's identity and tracking is as simple as analysing the GPS location data. The distinction between private and public data is merely a dashed line when it comes to privacy.

- **Prediction**

  Predictive analytics using AI works in a lot of scary ways. AI has the ability to generalise, infer and deduce your sensitive information based on one's non sensitive and everyday available information. One's nature of typing can be used to predict the emotional state of nervousness, sadness or confidence. One's pattern in everyday GPS locations, can be used to predict the whereabouts. Following one's everyday data, AI can be used to predict sexual orientation, political views, ethicic identity, travel history and more.

- **Profiling**

  Not only the task of collecting and storing, AI can use those data to perform sorting, analyzing, ranking, scoring and evaluating people based on collected data points. These profiling results are then used to target advertisements and political campaigns. An example of such profiling is presented in China where social scoring is used to limit the access to employment, housing, social services and even credit cards. Then what is there to talk about privacy when nothing is private.

However, daunting the concerns of privacy become, a company can always ensure the basic privacy protection strategies as mentioned below to fight against the irregularities in privacy protection:

- **Training:**

  It should be mandatory for a company to ensure awareness of data privacy, security, and concerns. More so, it should be integrated into the compulsory general training as part of the new staff's onboarding.

- **Privacy policy:**

  To ensure that customer's data is well protected and secure, a company needs to have a firm privacy policy that defines the protocols to keep the personal information safe. Gaining the customer's trust will always benefit the company in the long term.

- **Security tools:**
  A company can always make use of the security tools that are available on the internet. Such tools include encrypted storage, solutions, password protections, and VPNs. These tools aid in dramatically reducing the vulnerability to attack from outsiders.

- **Monitor Suspicious Activity:**
  One should always monitor for suspicious activity to identify red flags and prevent a disaster from happening. A company should always monitor for suspicious emails, phishing calls and use multi-layer security that filters out malware, remote logins, and unauthorized access.

- **Hacker's Interest:**
  Don't underestimate the hacker's interest in your company because whether the attack is small or more extensive affects the company in several ways, starting from its reputation to severe economic depletion.

- **Zero Trust Model:**
  It is always recommended to implement a zero-trust model as it restricts the entire network by isolating applications. Not only that, this model segments access based on user's permission, authentication, and user verification. This centralized user approach makes it compulsory to have proper verification to have authorized access. Having such a "trust but verify" mindset is an absolute necessity

Not only these from an individual point of view, being away from unnecessary links and websites, keeping a clean and protected system with latest security softwares, awareness on social engineering scams is a must to ensure data privacy on the user end.

The third region on the dimension to trust is the Security.

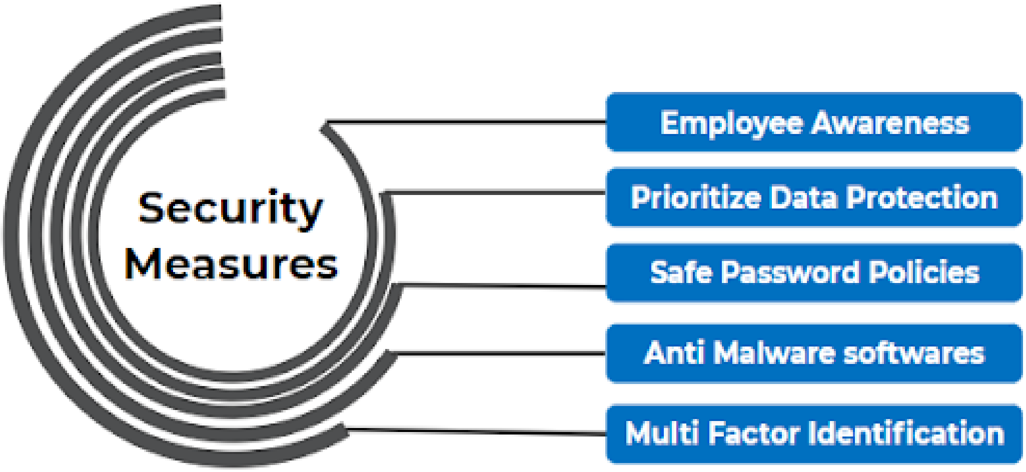
Security can be thought of as a sister to privacy. With security one immediately wanders on the questions like: Is the data stored and protected where unauthorised access cannot find them? Is that information encrypted and secure? Who is responsible in case the information is leaked? The discussions on security are obvious to involve topics like cyber security, hackers, social engineering, scams and more which might take a while to even introduce. So this reading material only focuses on the security of personal information and ways in ways AI can invade personal security and space.

Source: Pixabay

AI can act both as a boon or a bane when it comes to maintaining security. Every business and technology related company has to go through the procedures to ensure proper security when sensitive information like payable salary, job history, health care data and personal information are in play. It is required by the law for all the companies to have a data protection officer and a system that is designed for data protection.

Elements and applications of AI like **facial recognition, data analytics, threat assessment** and more can be used to ensure security whereas these elements can also be used to invade personal space and sensitive information. Malicious use of AI can include spread of falsified information, audio, video and text generation, intelligent automation and even obfuscation.

But with proper security measures and policies in place, the loss of information into the wrong hands can be prevented. So, A key part of building trust with the customers is ensuring their information is securely stored and the ways to do so are listed below:



Security Measures

- Employee Awareness
- Prioritize Data Protection
- Safe Password Policies
- Anti Malware softwares
- Multi Factor Identification

- **Employee Awareness:**
  Employees should be made aware with the education to cyber securities, its effects, potential ways for unauthorised access to get into the system.

- **Prioritize Data Policy:**
  A company must prioritize proper data protection policies before any other services which helps in building trust with the customers.

- **Safe Password Policies:**
  A company should enforce safe password policies which ensure passwords contain an uppercase, capital letters, special characters and update those passwords in every 60-80 days time span. According to the data breach investigation report published by Verizon in 2016, 63% of the data breaches were due to lost, stolen or weak passwords. So enforcing a reliable and secure password is a must.

- **Antimalware softwares:**
  Installation of anti-malware softwares, regular updates of existing softwares with up to date security measures and regular backup of data are the basic measures of security

- **Multi-factor identification:**
  A log into the system by employees should always be multi-factor requiring more than one verification to gain the access. Preferably, an OTP to the employee's phone number or an verification email, but more than one is a necessity.

These small steps ensure heavy damages to the overall company reputation and prevents leakage of valuable customer information.

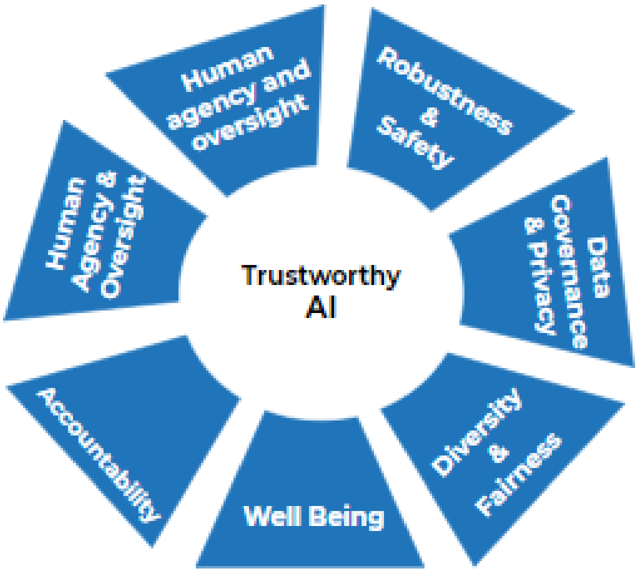
The final topic to discuss on dimensions of the "Trust in AI" is the People Impact.

People impact answers the very important question: What is the intent in capturing the data? Based on the GDPR rules, which will come later in the reading material, it is not right to collect customer's personal data wondering what the data tells. If there is no intent to data, and no vision of what the data will be used for, the company should not capture that data. Monitoring customer data for the wrong reasons always has severe effects. So, it is important before any project for all the team members, stakeholders to sit down and document what data is being collected and why.

Any business vendor/organization should look out for the following things to avoid regarding customer data to maintain trust and support:

- Organisation must not monitor data to measure performance. For example: Yahoo cross checks employees VPN logs to monitor their working hours. Such activities damage a company's reputation and sense of trust.
- Organisation must avoid the use of customer data for anything that is not legally allowed. For example: It is illegal to use customer health data to determine insurance pricing.
- Never cross the boundary between the use of personal and professional data. A company should never give access to personal data to anyone without complete authorization.

To summarise the trust in AI, the following enlist the key requirement for an AI system to be deemed trustworthy:



- **Human Agency and Oversight:**
  AI systems should empower human beings, allowing them to make more informed deci sions fostering their fundamental human rights. Proper oversight mechanisms are needed to be ensured which can be achieved through human-in-the-loop, human-on-the-loop and human-in-command approaches.

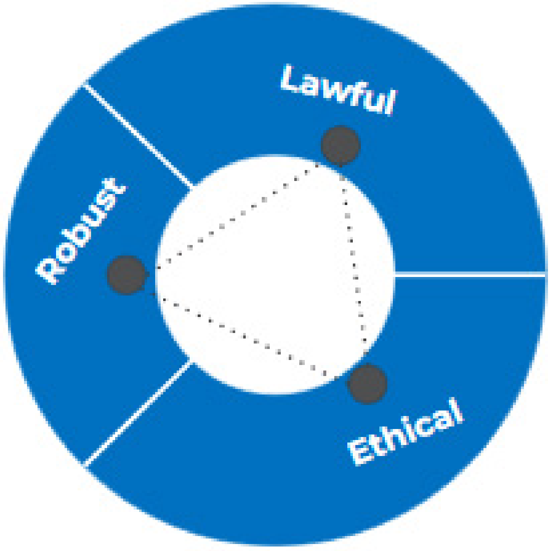
- **Technical Robustness and Safety:**
  AI systems should be resilient and secure. They need to be safe, ensuring a fall back plan in case something goes wrong.

- **Privacy and data governance**
  Beside ensuring privacy and data protection, adequate data governance mechanisms must also be secured to ensure legitimate access to data.

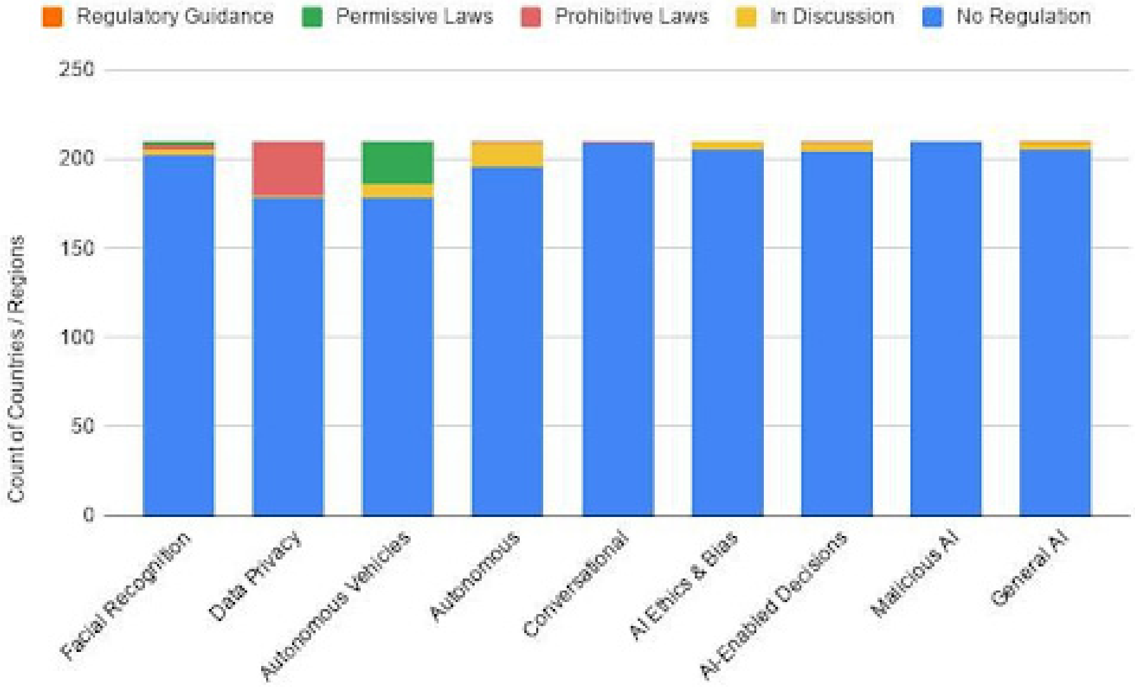
- **Diversity, non discrimination and fairness:**
  An AI system shouldnt present unfair bias as it could have multiple negative implications, from the marginalisation of vulnerable groups to the exacerbation of prejudice and discrimination.

- **Well being:**
  AI systems should benefit all human beings including future generations. It must also be sustainable and environment friendly.
- **Accountability:**
  There should be a proper mechanism in place to ensure responsibility and accountability for AI systems and their outcomes.

In brief, A trustworthy AI system should be lawful, robust and ethical in nature.



6. Regulations



Source: Cognilytica, 2020

Looking at the figure, laws regulating autonomous vehicles are starting to make their appearance on the roads where most of the countries don't have any rules and regulations that guide the different use cases of AI. As such, governments and legislative bodies are rapidly facing the need to make sure their traffic laws and other automobile and vehicle-relevant laws and regulations remain relevant.

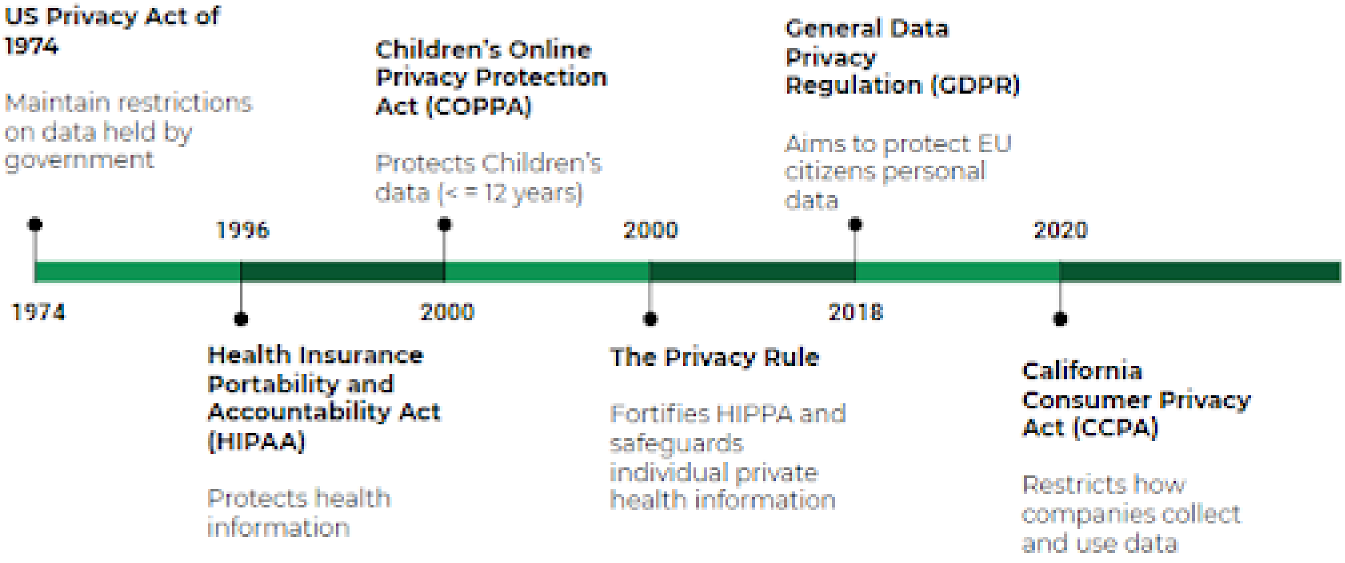
Despite that, Adoption for AI and cognitive technologies shows no signs of slowing down and governments are paying attention to what's brewing. Eventually, we can confidently say that **AI laws are coming.**

But, It may not be surprising to find that most governments are adopting a “wait and see” approach to laws and regulations on AI. Just like with any new technological wave it’s hard to predict just how this new technology will be used, or abused.

The European Union is the most active in proposing new rules and regulations, with existing or proposed rules in seven out of nine categories of areas where regulation might be applicable to AI. On the other hand, the United States maintains a “light” regulatory posture when it comes to laws around AI.

Companies are now required to determine what data privacy acts and laws affect their users. For instance, one must know where the data originated (country and state), what personally identifiable information it might contain and usage methodology.

Organisations can face fines up to the greater of **€20 million ($22 million) or 4% of their annual global turnover** if they are found to be out of compliance with the new privacy regulations. Google has already been fined €50 million for data privacy violations in France.

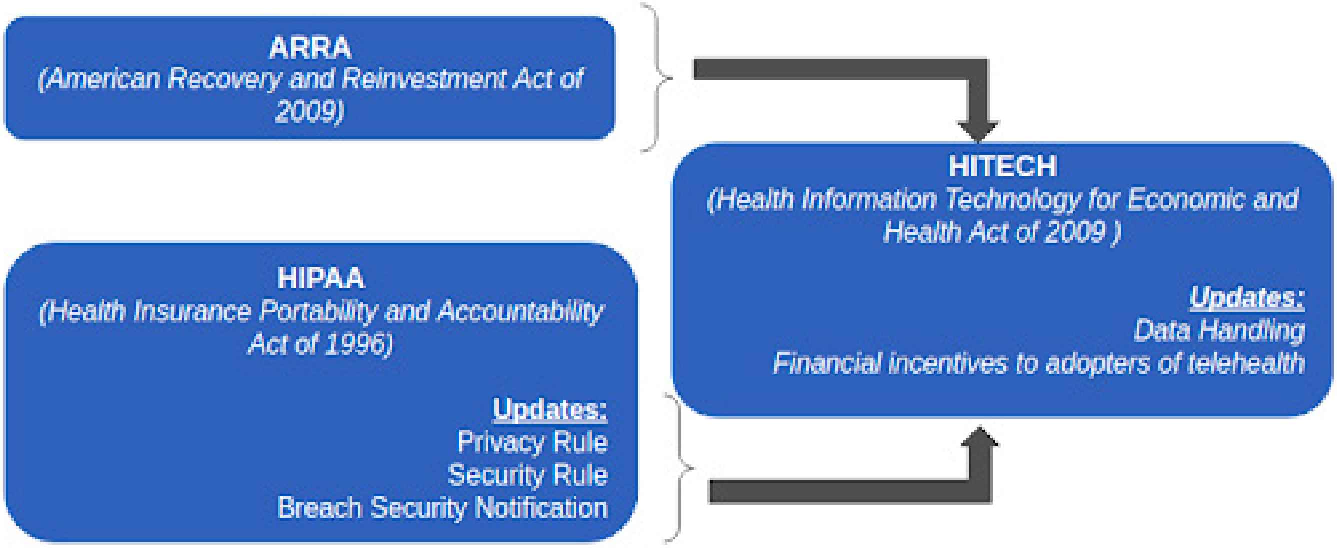

US Privacy Act of 1974
Maintain restrictions on data held by government
Children's Online Privacy Protection Act (COPPA)
Protects Children's data (< = 12 years)
General Data Privacy Regulation (GDPR)
Aims to protect EU citizens personal data
1996
2000
2020
1974
2000
2018
Health Insurance Portability and Accountability Act (HIPAA)
Protects health information
The Privacy Rule
Fortifies HIPPA and safeguards individual private health information
California Consumer Privacy Act (CCPA)
Restricts how companies collect and use data

Source: *Inside Out Security (2020)*

The rules and regulations timeline dates back from 1974 where the US published the Privacy Act of 1974 that focused on maintaining restrictions on data held by the government to the recent California Consumer Privacy Act (CCPA) that restricts how companies collect and use data. Between these timelines there has been a number of significant reports and reforms made. This reading material only covers a few.

- **ARRA, HIPAA and HITECH**

  In the United States of America (US), it is required by the law for health care facilities to be HIPAA (and HITECH) compliant.


ARRA
(American Recovery and Reinvestment Act of 2009)
HITECH
(Health Information Technology for Economic and Health Act of 2009)
Updates:
Data Handling
Financial incentives to adopters of telehealth
HIPAA
(Health Insurance Portability and Accountability Act of 1996)
Updates:
Privacy Rule
Security Rule
Breach Security Notification

Source: *"HIPAA, HITECH, ...and ARRA. How do they relate?" Bridges*

The HITECH Act was passed as a part of American Recovery and Reinvestment Act (ARRA) of 2009. As technology is a moving target, HITECH seeks to protect the technological infrastructures used in telehealth that were not previously available in the HIPAA Act. HIPAA sets the standard for exchange of sensitive patient data or protected health information (PHI) when operating in US and protects the privacy of the patient health information as enforced by the Department of Health and Human Services whereas HITECH incorporates the technological changes in HIPAA to the newer and imminent standards. The primary motive behind HIPAA is to increase the sensitivity of exchange of PHI and improve efficiency, transparency, and security of healthcare systems that deal with sensitive patient data. It addresses the digitization of medical data and paves the pathway for organisations to follow.

HIPAA is built on a number of rules that provides a basis to follow so that the company can well manage sensitive data and remain HIPAA compliant:

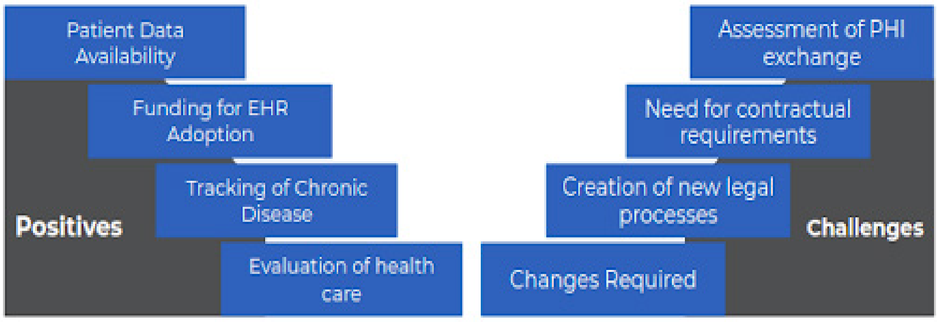
Privacy Rule
Security Rule
Transaction Rule
Identifiers Rule
Enforcement Rule

- **Privacy Rule:**
  This rule indicates standards to protect individual electronic medical records and personal health information and how it can be used by not disclosing it.
- **Security Rule:**
  This rule indicates standards to protect electronic personal health information with right safeguards.
- **Transaction Rule:**
  This rule addresses the safety, accuracy and efficiency of medical reports and PHI during transactions or exchange.
- **Identifiers Rule:**
  This ensures unique identifiers to every PHI and medical reports.
- **Enforcement Rule:**
  This rule addresses the authority's power to enforce penalties for violations and set the breach reporting requirements.

However, HIPAA was not comprehensive enough to address the technological changes over the years. It laid out the groundwork for PHI protection and health care improvements, but to address the technological changes, technological loopholes, and lenient penalties, it was amended to form HITECH Act. HIPAA was designed to address the data leakage in 1974, but it was outdated by the time of 2009. Similarly, third-party applications could easily access PHI and misuse it, creating loopholes that needed to be fixed. Finally, the penalties that were enforced for the misuse of data were not strong enough to prevent rules' violence. These reforms were addressed in the upcoming HITECH Act.

There were four main objectives to the HITECH Act, that focused on overcoming the shortcomings of the previous acts.

- **Subtitle A: Promotion of Health Information Technology**
  This subtitle deals with the creation, application and regulation of national standards for healthcare quality, safety and efficiency.
- **Subtitle B: Testing of Health Information Technology**
  This subtitle points out applicants for grants as a part of healthcare information technolo gy research and testing.
- **Subtitle C - Grants and Loans Funding**
  This subtitle outlines how grants and loans are used and also ensures how these grants are being used and what standards are maintained.
- **Subtitle D-Privacy**
  This subtitle outlines improved security and privacy provisions.

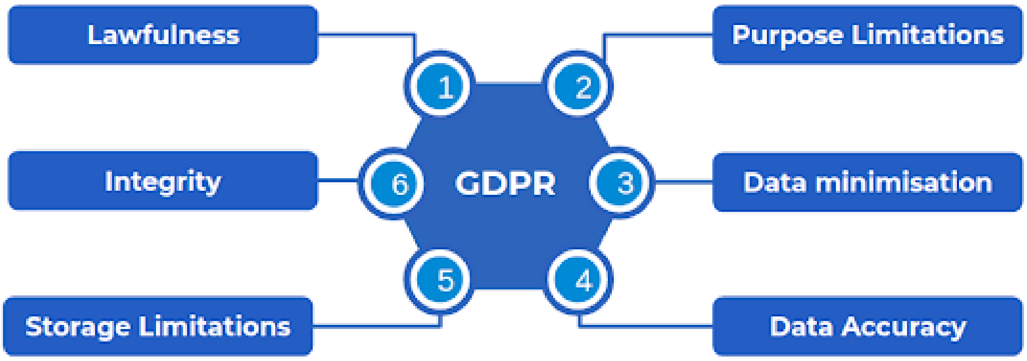

Patient Data Availability
Funding for EHR Adoption
Tracking of Chronic Disease
Evaluation of health care
Positives
Assessment of PHI exchange
Need for contractual requirements
Creation of new legal processes
Changes Required
Challenges

HITECH offers the positive and negative impacts in business application as shown in the figure above. It improves patient data availability and tracking of chronic disease management. It provides stimulus for early EHR, Electronic Health Record, adoption and allows the evaluation of health care based on value, quality and price.

Whereas, with HITECH it creates a need to monitor control to mitigate the risks due to oversight and enforcement. There is also a need to re-engineer, change the system to adapt to the new legal processes along with the contractual language with written requirements. Not only that with newer systems and modification to exchange of PHI, HITECH demands for changes that properly assess the exchange.

- ### General Data Protection Regulation (GDPR)

  When HIPAA and HITECH focused more on the regulations of PHI for companies based in the US, GDPR monitors any company that stores or processes personal information about citizens in the European Union. Not only that any company that holds, stores and works with the data of a citizen of the EU should comply with GDPR even if they don't have any business presence in the EU. As businesses continue their digital transformations, making greater use of digital assets, services, online tools and big data, they must also be accountable for monitoring and protecting that personal customer data on a daily basis

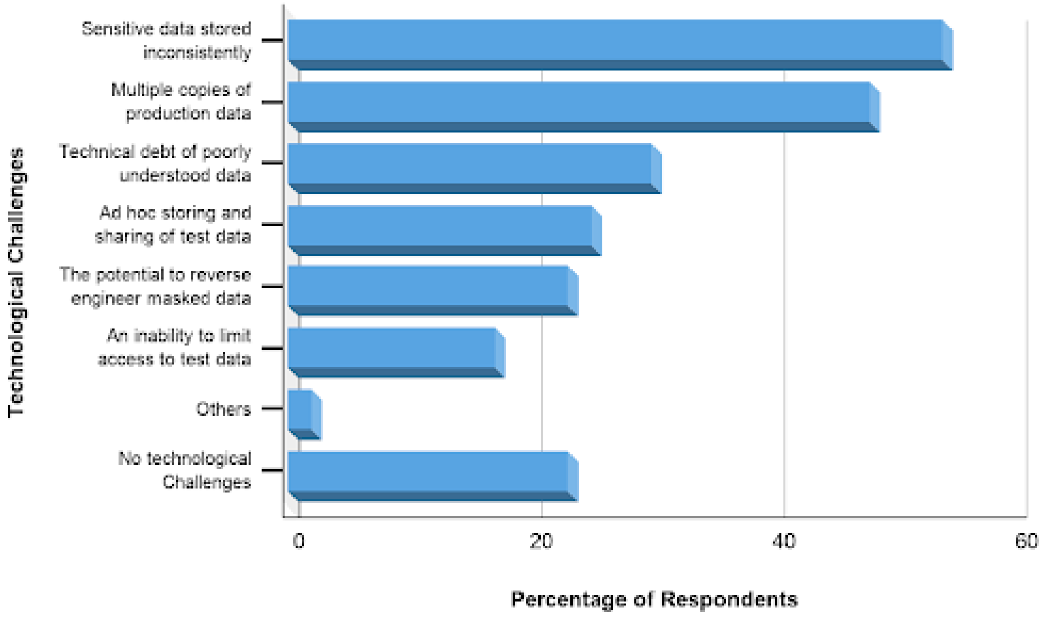


Source: *Mohamed Tirani*

GDPR enlists the six compliance rules for any company working with personal data:

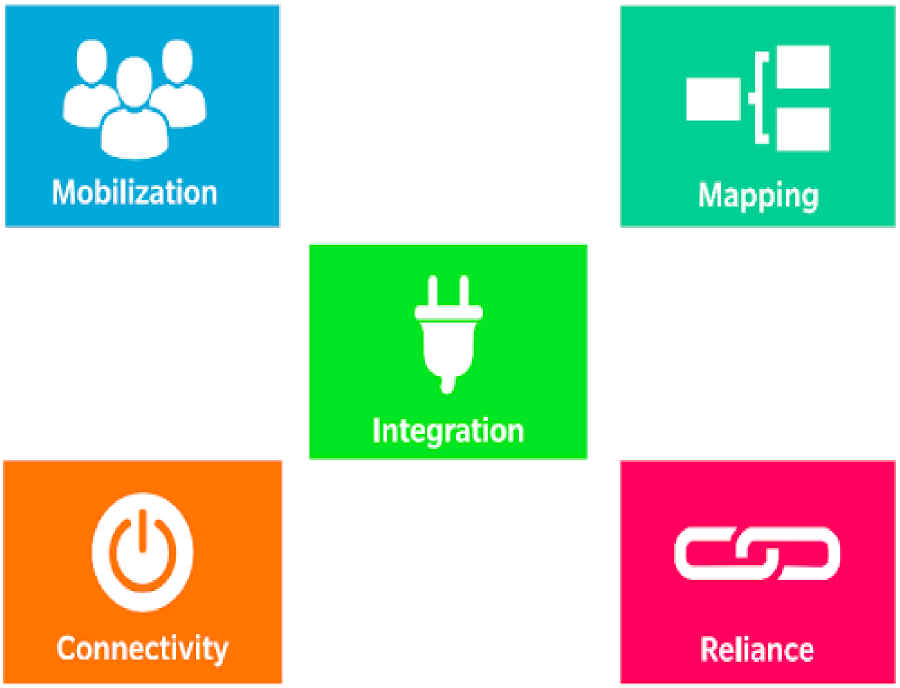
- **Lawfulness:**
  This ensures one must process all data for specific purpose, clearly and trustfully stated and agreed by the user
- **Purpose Limitations:**
  This ensures one must collect data for specified and legitimate purposes by gaining the explicit consent from the user.
- **Data minimisation:**
  This ensures one must limit the amount of data they hold by reviewing what data you hold and why you hold it.
- **Data Accuracy:**
  This ensures one must be updated with all the data stored is correct and accessible.
- **Storage Limitation:**
  This ensues one must store that data that is need and delete the one that are no longer required
- **Integrity:**
  This ensures one must ensure data safeguarding, to protect data against unlawful pro cessing or loss by encrypting and maintaining privacy.

Becoming a GDPR compliant is not going to be easy as there are a number of challenges that violate at least one of the six principles of GDPR. Upon survey conducted among 200 respondents to assess "Which technological challenges might provide a compliance risk to your organisation ". Over half (54%) report that sensitive data is stored inconsistently within their organisation whereas 12% of them there were no technological challenges that present compliances risks.



Source: *EU General Data Protection Regulation (GDPR)*

So, looking at five sustainable steps to ensure GDPR compliance includes the following:



Source: *Future Proofing Privacy: GDPR Compliance in a Networked Banking System*

- **Mobilisation:**
  It includes the appointment of a data protection officer, assessment of privacy impacts, creation of program structures to implement changes.
- **Mapping:**
  It which includes creation of centralised data registry, centralisation of consent handling, monitoring of usage against consent, and breach reporting procedure
- **Integration:**
  which includes integration of centralised data registry, redesign of customer interface to capture consent and finally integration of factual audit trial.
- **Connectivity:**
  It which includes Creation of customer portal to allow customer to amend the consent given, and access their own data and integration with third party data sources
- **Reliance:**
  It includes activities like outsourcing data management to third parties, fostering a market for data services.

References:

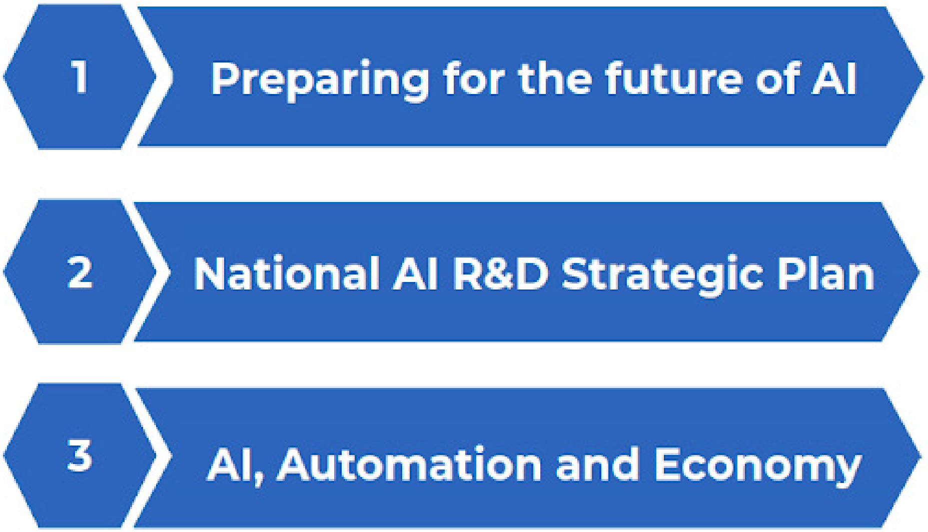
- *https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/?sh=620c6c55a2b4*
- *https://www.varonis.com/blog/data-privacy/*
- *https://www.bridges-inc.com/hipaa-hitech-and-arra-how-do-they-relate/*

7. AI Strategies for Different Nations

The race to become the global superpower in Artificial Intelligence and its application has officially begun. With more and more extraordinary applications brewing up in every research, it is only the matter of how and when, one is implementing it to develop society and the nation in return. A significant number of nations have already devised their strategies in implementing AI for the economic and social developments. No two strategies from different countries are alike, each focusing on different aspects of the development. Some focused on scientific research, talent development and education while others on adoption of AI, ethical and privacy concerns, rules and regulations and more. The priorities remain wide.

This reading material includes national strategies on AI for five different nations namely, United States of America, China, European Union, Canada and United Kingdom.

- **United States of America (USA):**
  Unlike the national strategies of other countries, the US doesn't seem to have a definitive and co-ordinated national strategy for implementing AI and its applications for better use cases rather US lays the foundation for development of AI industry in three separate reports:



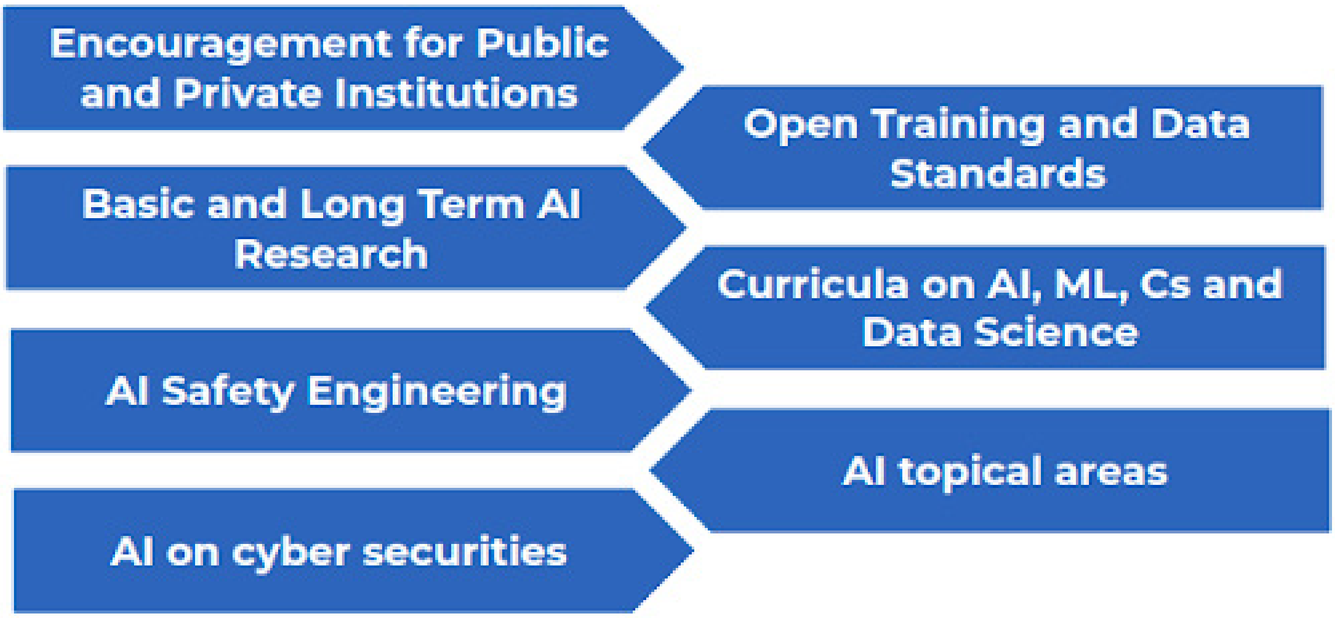
1 Preparing for the future of AI

2 National AI R&D Strategic Plan

3 AI, Automation and Economy

1. **Preparing for the future of AI**
   This report contains the recommendations to AI regulations, public research and development, ethics, fairness, and security in the field of AI. Each recommendation in this report corresponds to a topic of discussion like AI in Federal Government, AI and Regulations, Research and Workforce and so on. Each of these topics of discussions will have specific sets of recommendations for the US government to act on for the development of the country towards a nation with prosperous AI and its applications.

Some of the general recommendations includes:


Encouragement for Public and Private Institutions
Open Training and Data Standards
Basic and Long Term AI Research
Curricula on AI, ML, Cs and Data Science
AI Safety Engineering
AI topical areas
AI on cyber securities

a. Private and public institutions are encouraged to examine whether and how they can responsibly leverage AI and machine learning in ways that will benefit society.

b. Federal agencies should prioritize open training data and open data standards in AI.

c. The Federal government should prioritize basic and long-term AI research.

d. Schools and universities should include ethics, and related topics in security, privacy, and safety, as an integral part of curricula on AI, machine learning, computer science, and data science.

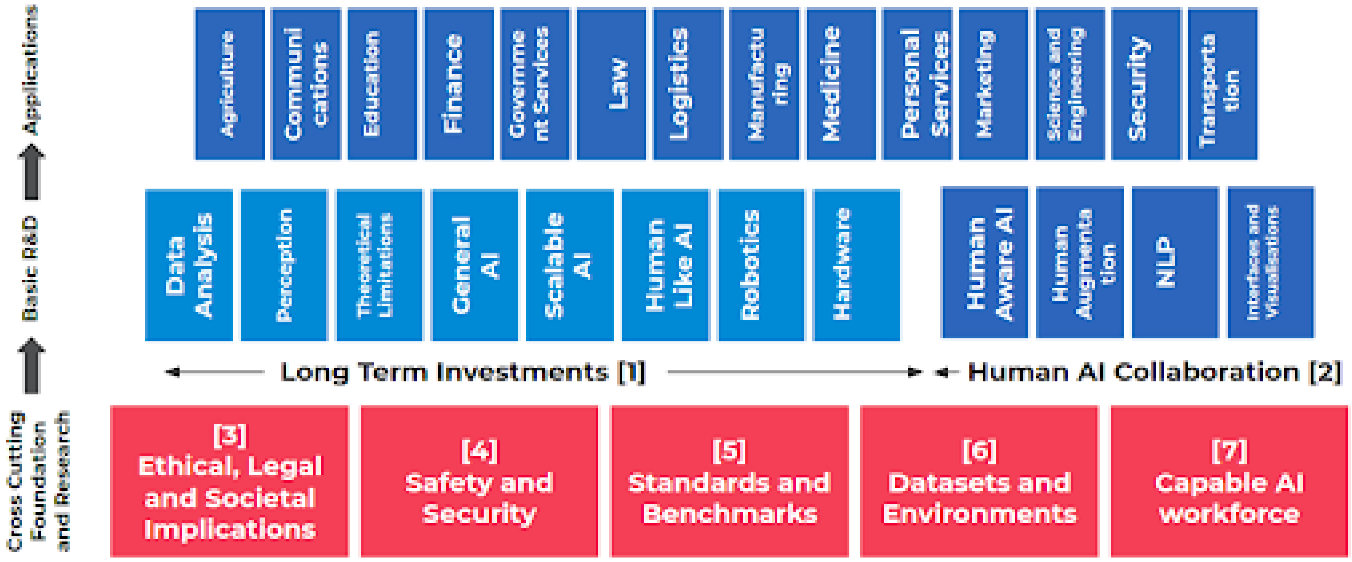
e. AI professionals, safety professionals, and their professional societies should work together to continue progress toward a mature field of AI safety engineering.

f. The U.S. Government should develop a government-wide strategy on international engagement related to AI, and develop a list of AI topical areas that need international engagement and monitoring.

g. Agencies' plans and strategies should account for the influence of AI on cyberse curity, and of cybersecurity on AI.

2. National AI R&D Strategic Plan

This report outlines the strategies for public research and development in artificial intelligence. The report establishes a set of objectives for federally funded AI research, such as academia which aims in bringing new AI applications to benefit the society which minimizes negative impacts. It looks beyond the near term AI capabilities towards long term transformational impacts of AI, resulting in strong industrial growth and commercialization of AI.



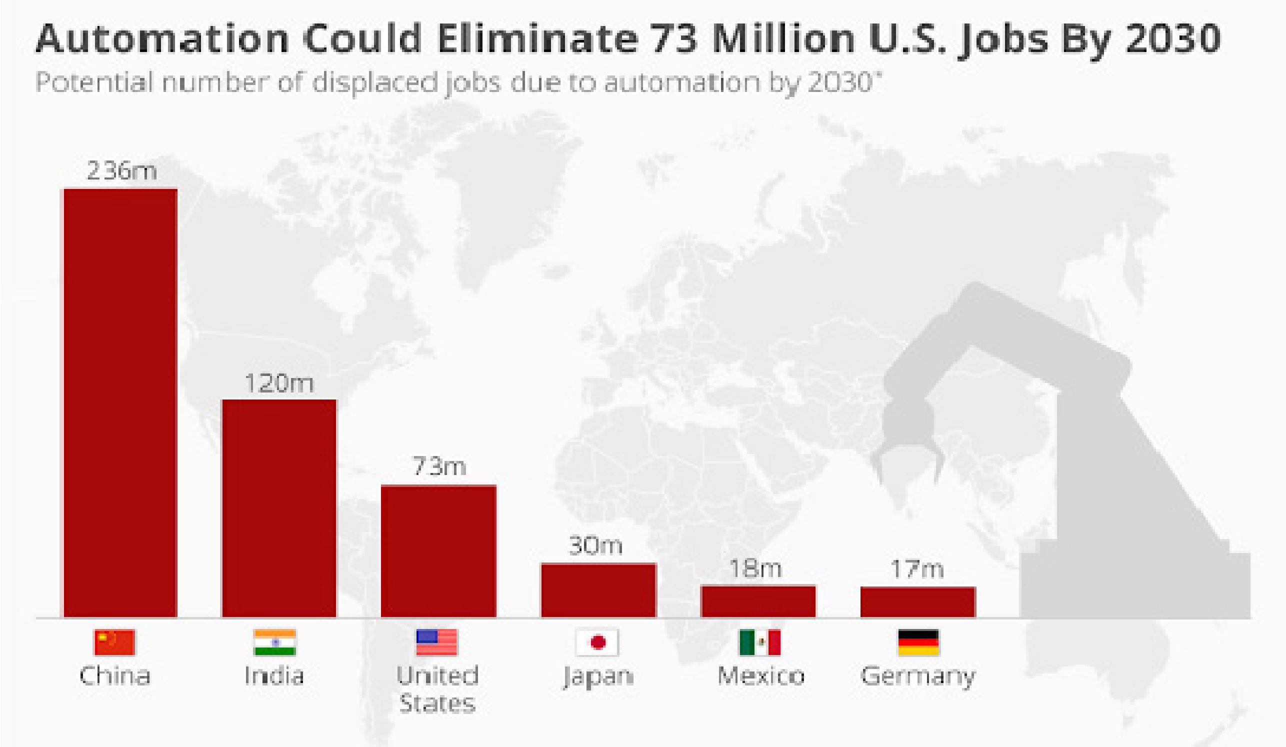
Source: *The National Artificial Intelligence R&D Strategic Plan*

The above figure provides the overall organisation of this AI R&D Strategic Plan. Across the bottom are the crosscutting, underlying foundations that affect the development of all AI systems. The next layer includes many areas of research that are needed to advance AI lik data analysis, general AI, Robotics and so on. This layer also highlights the areas of long term research investments and areas that need human collaborations. The numbering in some of the elements of the above figure each corresponds to the strategic plans proposed which are listed below:

i. Making Long-Term Investments in AI Research
ii. Develop Effective methods for Human AI Collaborations
iii. Understand and Address the Ethical, Legal, Societal Implications of AI
iv. Ensure the safety and security of AI Systems
v. Develop Shared Public Datasets and Environments for AI Training and Testing
vi. Measure and Evaluate AI Technologies through Standards and Benchmarks
vii. Better Understand the National AI R&D Workforce Needs

3. AI, Automation and Economy

The final report examines the impact of automations, policies needed and the benefits of AI.



Source: McKinsey

As the figure shows, in the US, AI could be used to eliminate 73 million Jobs by 2030 as a result of AI automation. Given appropriate attention and the right policy and institutional responses, advanced automation can be compatible with productivity, high levels of employment, and more broadly shared prosperity. So, this report advocates strategies to educate and prepare new workers to enter the workforce, cushion workers who lose jobs, keep them attached to the labor force, and combat inequality. Those strategies includes:

a. Invest in and develop AI for its many benefits.
b. Educate and train Americans for jobs of the future.
c. Aid workers in the transition and empower workers to ensure broadly shared growth.

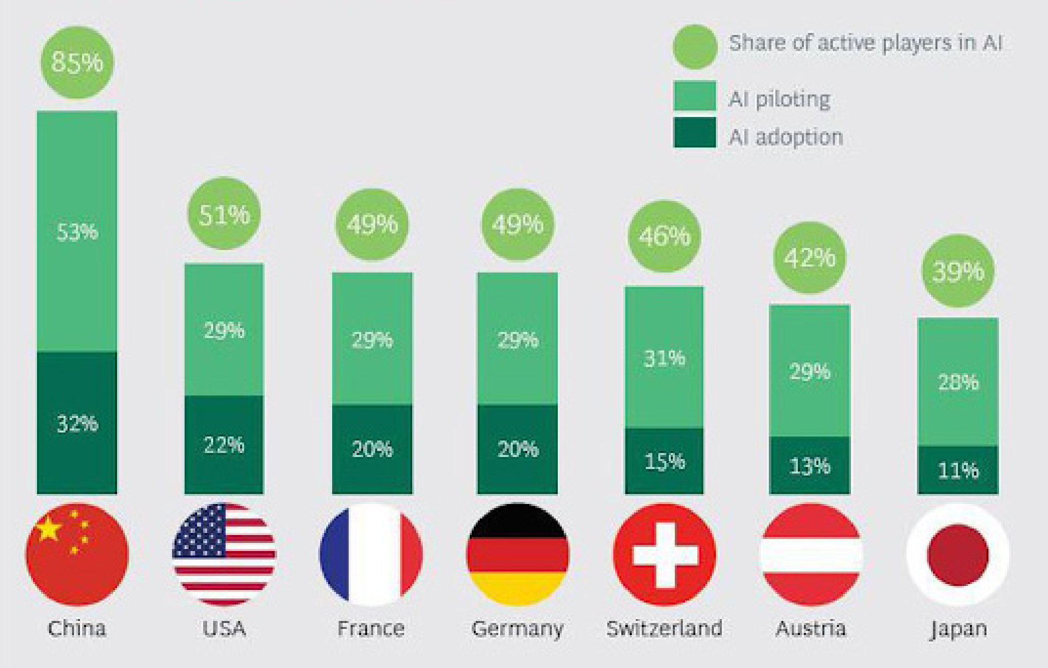
4. Free Market Oriented Approach

Apart from the above three reports, the US also has the free market oriented approach outlined at the summit on Artificial Intelligence for American Industry which announces four goals of the government for the development of the AI industry. They are:

a. Maintain American leadership in AI
b. Support the American worker
c. Promote public R&D
d. Plan on removing barriers to innovation.

- **China:**

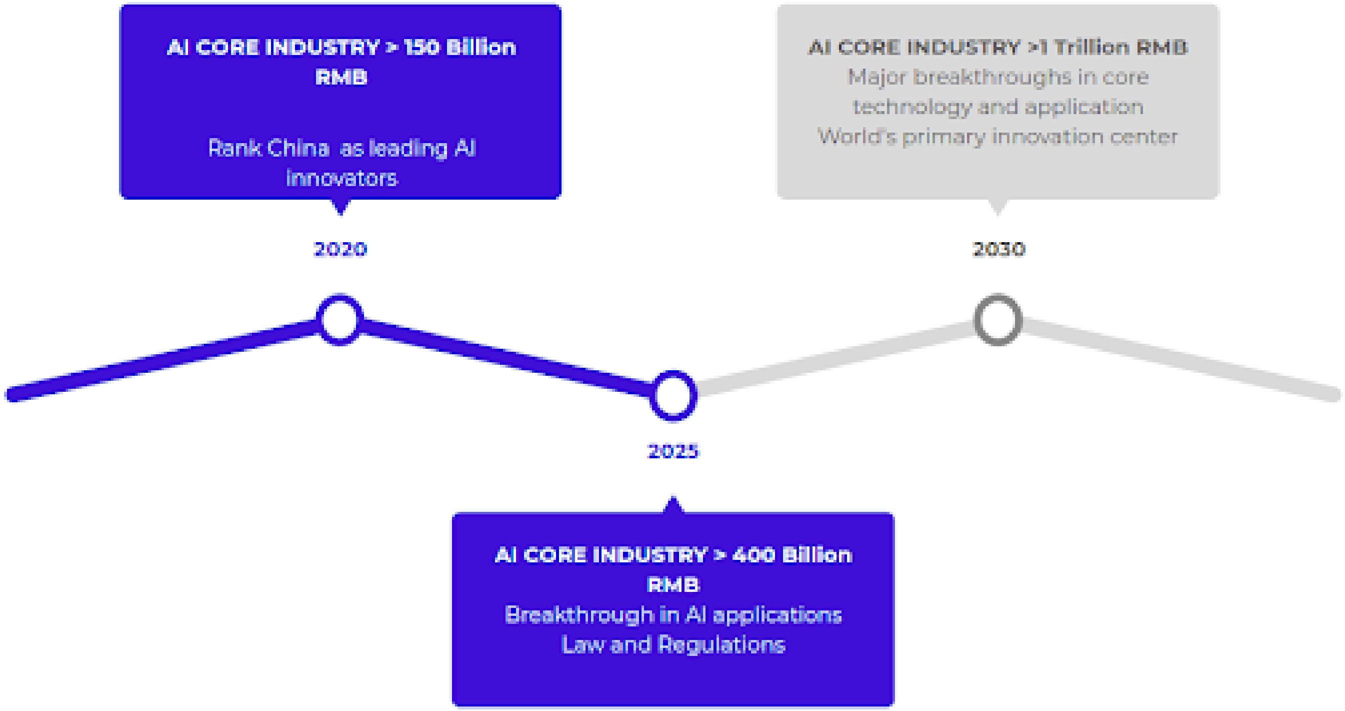
China is widening their lead in AI globally by concentrating on a core set of best practices that energize entire industries to pilot and adopt AI for unique use cases.
With the implementation of shorter innovation cycles in Chinese industries, they are starting to dominate the industry. China ranks first in leading and leveraging AI in other categories of industry as well and according to the study conducted by the Boston Consulting Group (BCG), 85% of the Chinese companies are active players in the field of AI surpassing all the other nations by a lot not only in AI pilotting but also in AI adoption.



The rapid development of AI in China and its clear dominance can be attributed to their *Next Generation Artificial Intelligence Development Plan.*

The next generation artificial intelligence development plan is China's ambitious plan to lead the AI industry in theories, technologies and application. The plan is comprehensive with initiatives and missions for research and development, industrialization, education, talent development, skills acquisition, ethical settings, security and more.
The comprehensive plan can be understood in three steps:

a. Make China's AI industry in line with its competitors by 2020 with a potential investment of over 150 billion RMB equivalent to about 23 billion US dollar.
b. Reach the peak in AI applications in some of the fields by 2025 with a potential equivalent investment of just over 61 billion US dollars.
c. Declare China as the primary center for Innovation by 2030 with a huge investment equivalent to just over 154 billion US dollars.


AI CORE INDUSTRY > 150 Billion RMB
Rank China as leading AI innovators
2020
AI CORE INDUSTRY >1 Trillion RMB
Major breakthroughs in core technology and application
World's primary innovation center
2030
2025
AI CORE INDUSTRY > 400 Billion RMB
Breakthrough in AI applications
Law and Regulations

Source: *FactorDaily (2018)*

The government is planning to make the AI core Industry a total worth of 1 trillion RMB by 2030 and related industries of worth 10 Trillion RMB. Not only that, the Chinese government plans to recruit the world's best AI Talent, strengthen the training of the domestice AI labour force and lead the world in laws and regulations that promote AI.

- **European Union**

Europe is home to a world-leading AI research community, as well as innovative entrepreneurs and deep-tech startups. It has a strong industry, producing more than a quarter of the world's industrial and professional service robots (e.g. for precision farming, security, health, logistics) and is leading in manufacturing, healthcare, transport and space technologies – all of which increasingly rely on AI. One of the main challenges for the EU to be competitive is to ensure the take-up of AI technology across its economy. European industry cannot miss the train. Only a fraction of European companies have already adopted digital technologies. This trend is particularly acute in small and medium-sized businesses.

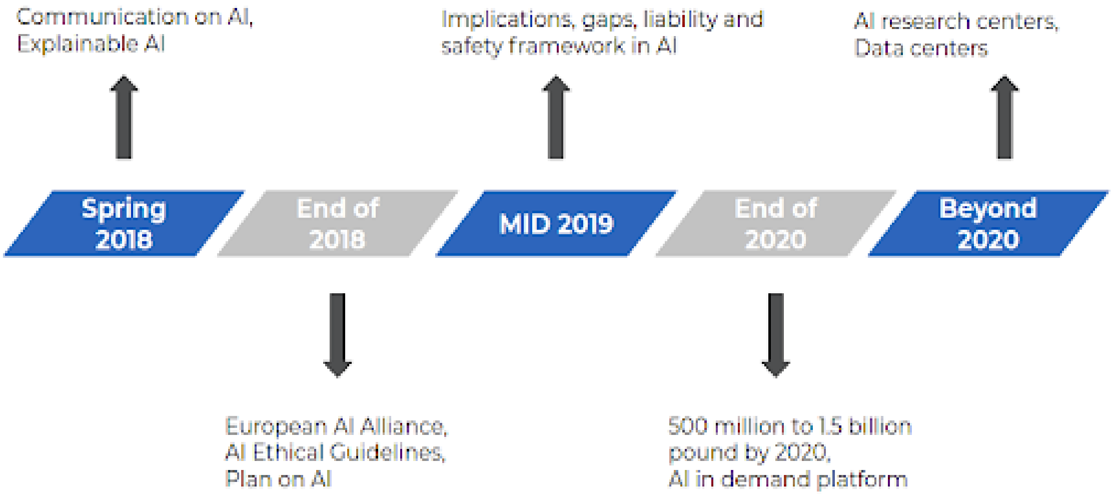
AI has featured in the EU research and development framework programmes since 2004 with a specific focus on robotics.

Overall, around EUR 1.1 billion has been invested in AI-related research and innovation during the period 2014-2017 under the Horizon 2020 research and innovation programme, including in big data, health, rehabilitation, transport and space-oriented research.

One of the key initiatives from the EU includes a commitment to increase the EU's investment in AI from 500 in 2017 to 1.5 billion euro by the end of 2020. Not only that, the EU is preparing to create European AI Alliance, a new set of Ethical guidelines to address issues such as fairness, safety and transparency.

European Union adopted the Communication on AI documented approach to AI which aims to:

1. Increase the EU's technological and industrial capacity and AI uptake by the public and private sectors
2. Prepare Europeans for the socioeconomic changes brought about by AI
3. Ensure that an appropriate ethical and legal framework is in place



Source: A timeline for the EU Commission AI strategy | via Tim Dutton

European commission is now working with individual state members to develop a coordinated plan that maximizes the impact of investments at EU and the national levels, encourages synergies and co-operation across EU, exchange best practices and collectively define the way forward to ensure that the EU as a whole can compete globally.

- **United Kingdom:**

The UK or the British government put forward its ideas, infrastructure people and business environment relating to AI in a document AI sector deal in 2018 which is a part of the government's larger industrial strategy. The document aims to position the UK as one of the global leaders in AI.

This Sector Deal is the first commitment from government and industry to realise this technology's potential, outlining a package of up to £0.95 billion of support for the sector, which includes government, industry and academic contributions up to £603 million in newly allocated funding, and up to £342 million from within existing budgets, alongside £250 million for Connected and Autonomous Vehicles. This Sector Deal aims to attract and retain both domestic and global AI talent; deliver major upgrades to the digital and data infrastructure; ensure that the UK is the best place to start and grow an AI business; and contribute to communities' prosperity by spreading the benefits of AI across the country.

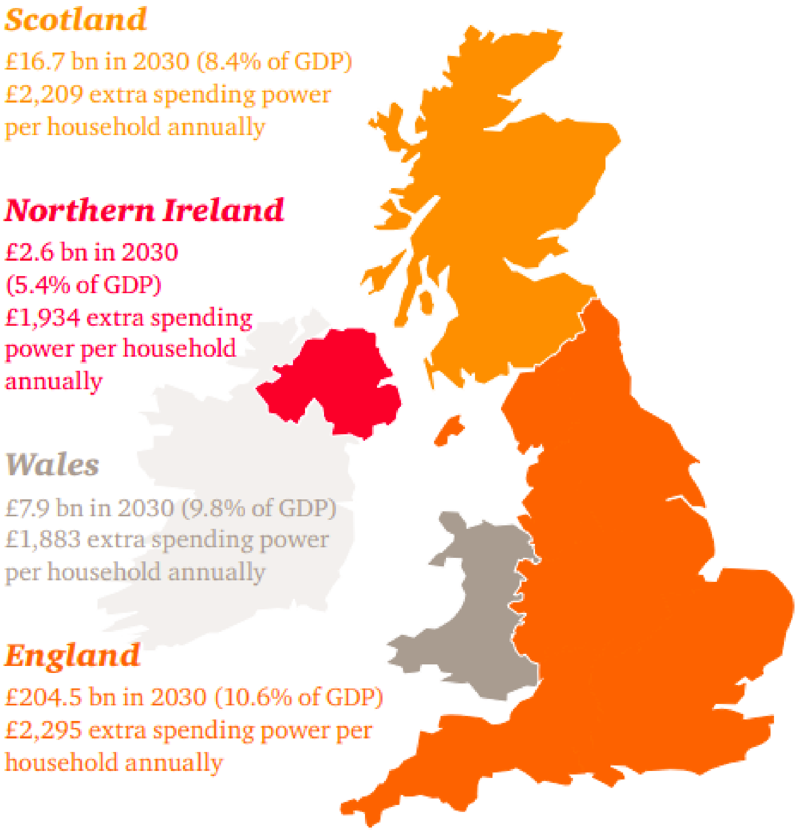
The Sector Deal reinforces the 5 foundations of the Industrial Strategy:

- **Ideas**
- **People**
- **Infrastructure**
- **Business environment**
- **Places**

It is quite comprehensive, with policies to boost public and private R&D, invest in STEM education, improve digital infrastructure, develop AI talent, and lead the global conversa tion on data ethics. The plans are focused in the expansion of the Alan Turing Institute, creation of turing fellowships, provision of 300 million pound investment in private sec tors from domestic and foreign companies and also establishment of a center for data ethics and innovation center.

Not only that, the UK government has focused the impacts of AI in multiple sectors of the economy and will not limit it to the firms that develop and produce AI.

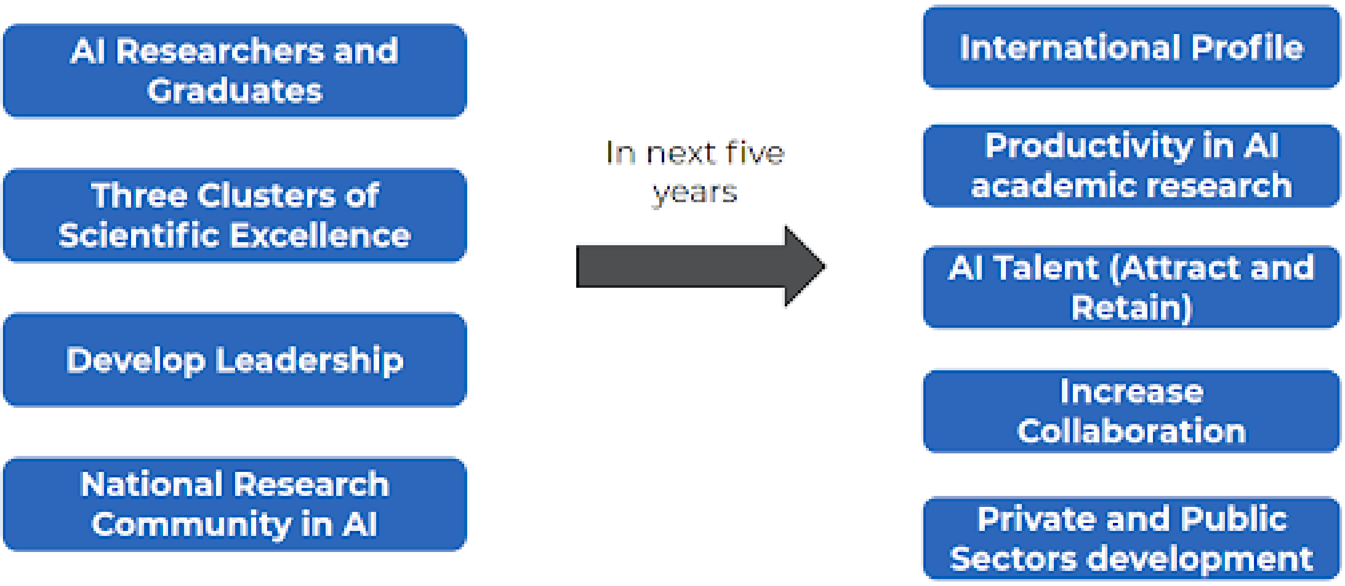
The following figure shows the impact of AI in the GDP of every household by 2030.


Scotland
£16.7 bn in 2030 (8.4% of GDP)
£2,209 extra spending power per household annually
Northern Ireland
£2.6 bn in 2030 (5.4% of GDP)
£1,934 extra spending power per household annually
Wales
£7.9 bn in 2030 (9.8% of GDP)
£1,883 extra spending power per household annually
England
£204.5 bn in 2030 (10.6% of GDP)
£2,295 extra spending power per household annually

Source: *The economic impact of artificial intelligence on the UK economy*

- ## Canada

Canada was the first country to publish its national strategy on Artificial Intelligence that aimed at investing a total of 125 million canadian dollar which is equivalent to just over 98 million US dollar in AI research and talent over the course of five years.


AI Researchers and Graduates
Three Clusters of Scientific Excellence
Develop Leadership
National Research Community in AI
In next five years
International Profile
Productivity in AI academic research
AI Talent (Attract and Retain)
Increase Collaboration
Private and Public Sectors development

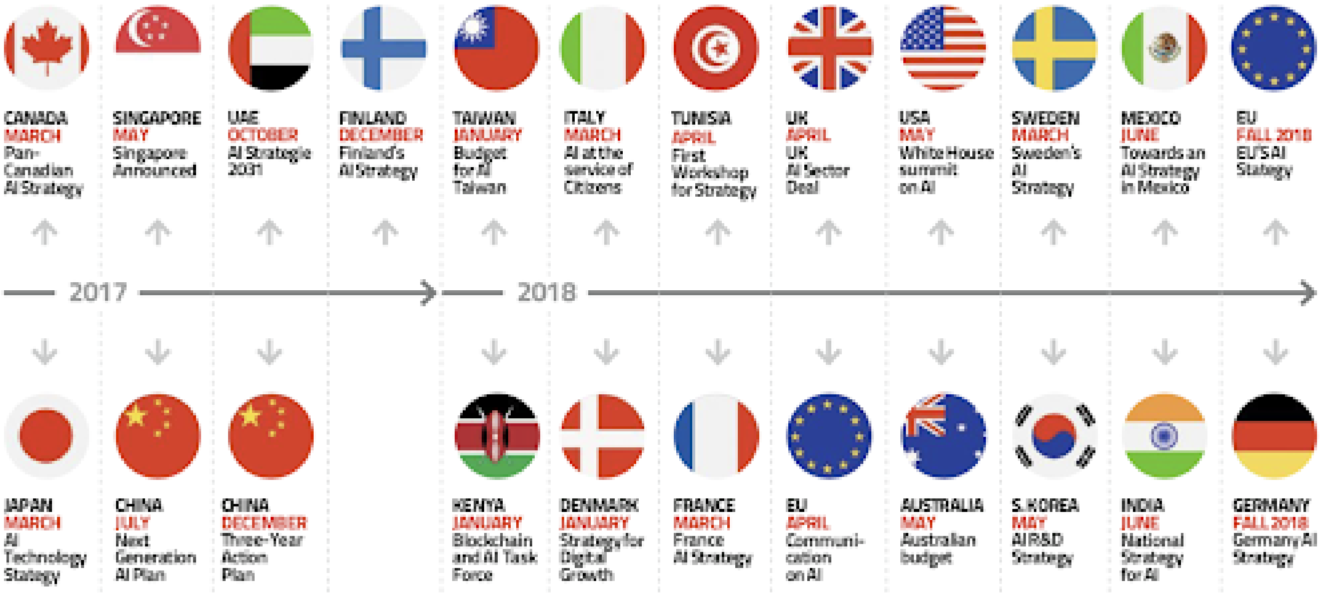
The Pan-Canadian Artificial Intelligence Strategy which is the national AI strategy for Canada outlined the following:

a. Increase the number of AI researchers and graduates and retain them
b. Establish three clusters of scientific excellence in Edmonton, Montreal and Toronto.
c. Develop leadership on the economic, ethical, policy and legal implications of AI
d. Support national research community on AI

Similarly, With that over the next five years Canadian institute for advanced research (CIFAR) will focus on:

a. Enhancing canada's international profile in AI research and innovation
b. Increase the productivity in AI academic research and enhanced capacity to generate world class research and innovation
c. Attract and retain outstanding AI Talent in Canadian universities and industry
d. Increase collaboration across geographical areas of excellence in AI research and strengthen relationships with receptors of innovation
e. Translate AI research discoveries in the private and public sectors leading to socio-economic benefits for Canada

Within such a small span of time many countries have already started releasing plans and strategies to promote and introduce AI in the development of the country. Each and every strategy focuses on different aspects of the society including scientific research, skills, education, sustainable development and so on. The figure below shows the timeline with the document specifying the strategy of different nations over the span of two years. As mentioned earlier, Canada was the first to release its strategies and it didn't stop there.



Source: *Politics +AI, Tim Dutton*

References:

- https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd
- https://www.holoniq.com/wp-content/uploads/2020/02/HolonIQ-2020-AI-Strategy-Landscape.pdf
- https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf
- https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf
- https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF
- https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/
- https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/ attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/ attachment_data/file/702810/180425_BEIS_AI_Sector_Deal__4_.pdf
- https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal
- https://cifar.ca/ai/
- https://www.holoniq.com/wp-content/uploads/2020/02/HolonIQ-2020-AI-Strategy-Landscape.pdf
- https://innovator.news/europes-place-in-the-ai-race-c3e8c9dd0f10