A.I.'S RACE FOR

RESPONSIBILITY AND PRIVACY

TABLE OF CONTENTS

INTRODUCTION

Connected automobiles, facial recognition features, voice assistants and even navigation applications are a few examples of Artificial Intelligence that we use every day. Slowly these systems have seeped into our lives and have become an integral part of them. Artificial intelligence (AI) adoption and its effects on businesses and society are at a critical moment globally.

The Puttaswamy judgement included personal autonomy and the right to be left alone under article 21 as a fundamental right. However, the following data proves that free will is a myth in the Digital Era, everything has become personalized, from our social media handles to the attributes of the potential baby. Everything can be controlled.

Private entities have narrowed our scope of understanding by limiting our reach and knowledge to what we already agree with and like so that we spend more time on their page. This has restricted our growth since we are unaware of the conflicting opinions, and we think that every individual is like us and has to have the same thinking as us, which does not happen in reality.

If an individual in the early 20th century wished to buy a book, he would visit a bookstore, skim through all the books, talk to people and then make an informed decision freely, but now if he goes on amazon, the home page will already pop a space which would read “here are some of the book suggestions for you” and even the order in which books would be shown on the screen is controlled by algorithm. Somehow, after that, every ad, that is either shown on YouTube, webpages, Instagram or Facebook would be related to books, essentially forcing me to buy a book, because I am seeing it everywhere. Platforms show us only a fraction of the potentially relevant information that is available and we make a choice out of only 1% of the options available.

In the Digital Era, the interpretation of liberty should be extended to freedom and autonomy because an invisible power control us secretly. Earlier, “liberty” was understood to be violated when someone physically interfered with or stopped you from doing something. Both are different scenarios, hence calling for re-interpretation to safeguard privacy.

WHAT IS ARTIFICIAL INTELLIGENCE?

John McCarthy in his 2004 paper defines Artificial Intelligence as the science and engineering of making intelligent machines, especially intelligent computer programs which can also be defined as leveraging computers and machines to mimic the problem-solving and decision-making capabilities of the human mind.

Artificial Intelligence can be divided into a few types which are:

1

REACTIVE MACHINES:

Limited AI that only responds to various stimuli according to pre-programmed rules does not employ memory, making it unable to learn from new information. A reactive machine is IBM's Deep Blue, which defeated world chess champion, Garry Kasparov, in 1997.

2

LIMITED MEMORY:

Many contemporary AI is thought to have limited memory. By being conditioned with new data over time, generally using an artificial neural network or another training model, it can use memory to get better. Deep learning, a subtype of machine learning, is regarded as artificial intelligence with restricted memory.

3

THEORY OF MIND:

Theory of Mind AI does not currently exist, but research into its potential is underway. It describes AI that can mimic the human mind and has decision-making abilities comparable to humans, such as recognizing and remembering emotions and reacting in social situations.

4

SELF-AWARE:

A step up from the theory of mind AI, or self-aware AI, refers to a mythical machine aware of its existence and possesses human-like emotional and intellectual capabilities. Self-aware AI, like the theory of mind AI, is a thing still under process.

WHERE DOES AI CROSSROAD WITH PRIVACY?

The meaning of privacy has to change with the changing times. It is no longer related to physical dangers like trespassers, but to a more subtle kind of psychological trespass. Privacy in the digital era should entail preserving oneself, his/ her identity.

As we had seen in the previous landmark judgments, the privacy issue was related to physical interference by police or investigating authorities. However, the times have changed, where concerns are raised regarding privacy in cyberspace. It has various aspects attached to it- privacy of data and the concept of free will, or liberty as we may call it.

Since we have already given so much data to grocery stores social media platforms big corporations to government that now we have a little control over it. We are living in a algorithmic world, this combined with scientist doing a lot of research on human body specifically brain, they would eventually understand us better than ourselves, they can basically predict our actions and even make decisions for us, without us even realizing. Ultimately, these small decisions made every day would pan out our lives with a little role of the us, there is a shift in authority.

80 percent of viewing hours streamed on Netflix originate from automated recommendations.

35 percent of sales at Amazon originate from automated recommendations.

And the vast majority of matches on dating apps such as Tinder and OkCupid are initiated by algorithms” The results are alarming, it clearly corroborates the fact that we essentially do not have free will, even though we might think otherwise. Each and every action of ours is tapped and studied, out of millions of possible options, user is shown only a few of them, based on their past preference, or some propaganda or paid ads.

There also exists algorithmic bias, that can have massive impact on an individual’s career and future, for instance in a study it was revealed that women’s CV were grounded by Amazon’s software meant for vetting CV by observing patterns.
Therefore, practicing responsible AI is the way forward to preserve individual’s identity and privacy.

WHAT IS RESPONSIBLE AI?

There have been ground-breaking developments in AI in the past 5 years that have impacted every aspect of our life, making us completely dependent on technology. It is everywhere around us in every single decision we make and every single thought that we have and thus it's time to move to responsible AI. It has completely transformed the landscape, making impossible things possible, such as directing the behaviour of a consumer, manipulation of presidential elections, voice recognition, mass surveillance, etc.

Responsible AI would be a step to ensure that the benefits of AI are enjoyed while varying its negative repercussions and implications. Mere ethics is not enough, for it is subjective; there should be a system that safeguards the implementation of 3 pillars of responsible AI- the system should be lawful, reliable, and ethical. These principles should go hand in hand to reap maximum benefit. One should never undermine the power of AI; there should always be an impact assessment test to reduce its harm. For instance, can a machine replace ce humans? Can you transfer education into a machine? Would it be ethical- since it would not account for insights gained by an employee during his tenure, it might have massive repercussions even if there is the slightest mistake in the algorithm? AI has undoubtedly overshadowed our entire existence; we cannot afford to leave our being in the hands of big companies; we need to make people know better so they can demand better.

AI RELATED LEGISLATIONS ACROSS THE GLOBE

1. European Union (EU)

The EU made its first attempt to impose transnational AI regulation in April 2021. All AI systems in the EU would be categorized under the planned "Artificial Intelligence Act" Based on the risk they pose to citizens' rights, privacy, and way of life. Systems that are regarded to pose a "clear threat to the safety, livelihoods, and rights of individuals" are covered under the term "unacceptable risk." Any system or product that fits under this category will be prohibited. Systems that enable "social scoring" by government agencies and AI programs that manipulate human behavior in order to thwart users' free choice fall under this classification. The other category, "High-risk," contains crucial infrastructure systems that might endanger physical wellbeing, legal compliance structures that might infringe on citizen's constitutional rights, and methods of managing movement of people, asylum-seeking, and border controls, such as checking the validity of travel documents. Before they can be released onto the industry, high-risk AI systems will have to adhere to "tight duties" that include risk analyses, high-quality datasets, "adequate" human control methods, and high levels of security. Chatbots, AI-enhanced video games, and spam filters fall under the "Limited risk" and "Minimal risk" classifications, which have minimal or no requirements. The majority of AI systems will come under this heading.

2. Canada

A new law on artificial intelligence was introduced in Bill C-27, which was introduced on June 16, 2022 by the Minister of Innovation, Science, and Industry. It updated the federal private sector privacy framework. The Artificial Intelligence and Data Act (AIDA), if approved, would be Canada's first law governing the use of AI systems. The stated goal of AIDA is to establish common requirements across Canada for the design, development, and deployment of artificial intelligence systems that are consistent with national and international standards and to prohibit certain conduct in relation to artificial intelligence systems that may seriously harm people or their interests, in each case in a way that upholds Canadian norms and values in accordance with principles of international human rights law.

3. China

China has made efforts to regulate algorithms. The Chinese Cyberspace Administration (CAC) intends to regulate how websites draw in and keep users. The proposed "Internet Information Service Algorithmic Recommendation Management Provisions" will compel the internal workings of services like Taobao, TikTok and Meituan to be examined. The proposed regulations could prohibit models that persuade customers to spend a lot of money. Any AI algorithms that are employed to determine prices, manage search results, offer suggestions, or regulate material would be subject to full regulatory oversight by the nation's cybersecurity authority. Businesses that are found to be in violation of CAC's potential new regulations may be subject to significant fines or harsher penalties, such as losing their business licenses or having all of their apps and services completely removed.

4. United States

The Obama Administration started focusing on the need to regulate the use of artificial intelligence in 2016, and in 2019 the White House's Office of Science and Technology Policy published a draught Guidance for Regulation of Artificial Intelligence Applications. This document contains ten principles for US government agencies to consider when determining whether and how to regulate AI. Following the publication of many papers by other American public groups, the Defense Innovation Board established guidelines for the ethical application of AI.

The Global Catastrophic Risk Mitigation Act was introduced by Senators Rob Portman and Gary Peters in June 2022. This bill, which is supported by both parties, aims to make sure that our country is better prepared for high-consequence events, regardless of their low likelihood, like new disease strains, biotechnology mishaps, or naturally occurring risks like super volcanoes or solar flares that, while unlikely, would be exceptionally deadly if they occurred.

ts law.

5. United Kingdom

The United Kingdom has been at the forefront of initiating the application and development of Artificial Intelligence. In September 2021, the National A.I. Strategy was published by the U.K. Government, which describes actions to assess long-term A.I. risks, including AGI-related catastrophic risks.

AI RELATED LEGISLATIONS IN INDIA

We need to acknowledge the fact that we all have two identities, which may be identical or different, but we are living in 2 other worlds simultaneously; we have come a long way in getting Fundamental Rights in the offline or real world, but there are no effective rights to protect us in the online or reel world, where there is a monopoly of private entities and a considerable power gap.

Even GDPR implemented in 2018 is not capable enough to keep pace with rapid technological changes, let alone a few sections of the only act that deals with the data protection of an individual- the IT Act.

Through the landmark judgment delivered in the case of Justice KS Puttaswamy v. UOI, Article 21 was interpreted liberally, considering the right to privacy as a fundamental right.
In 2018, the Ministry of Electronics and Information Technology established four committees to emphasize and analyze various ethical problems with AI. A Joint Parliamentary Committee is now deliberating on the PDP Bill - Personal Data Protection Bill 2019 - based on a proposed data protection law. The measure will become law after both chambers of Parliament have enacted it. In India, the use of AI is outpacing the creation of regulations.

India still lacks regulations related to data protection specifically to cater to the needs in the wake of rapid technological changes.

COMMENTS FROM FRACTAL

At Fractal, we are actively engaged in navigating the increasing influence of AI in everyday life and promoting the ethical use of AI. We aim to help our clients globally, leverage AI ethically and be responsible to humans, society, and the planet.

We uncover problems through the lenses of intelligence, emotion, speed, and scale, where we leverage interdisciplinary skills of AI, engineering, cognitive sciences, and design to tackle complex problems in the ethical development of AI.

Among the multifaceted challenges posed by AI, Privacy is among the key considerations. AI-based systems need large volumes of data to train and test the ML models. Dataset(s) may contain Personally Identifiable Information (PII) that needs to be handled carefully. Data privacy breaches cost enterprises financially apart from the risk of reputational damage. For example, Cybercriminals (acting alone or belonging to a criminal syndicate) getting access to individuals' health records can put lives at risk.

We observe several individuals, enterprises, and societal risks, even with existing data privacy practices. AI is challenging and even breaching some of the assumptions of legacy data protection practices. AI is increasingly becoming smarter at detecting small nuances and triangulating sensitive information which exposes people. The challenges require a multipronged approach with support from the government and socio-technical innovation from enterprises to manage the future needs of society.

COMMENTS FROM TSAARO

Tsaaro believes in ensuring that our problem-solving approach is collaborative in nature, i.e., ensuring that we use the best in place resources from the legal and technical domains to ensure that our problem-solving approach is the best in place.

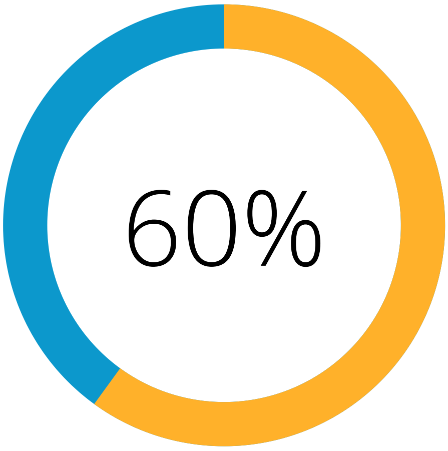
While privacy concerns are usually always a major concern when using new technology, the scope and applicability of AI presents a particularly challenging scenario. Big data's effects can be compared to AI's in some ways. Still, AI technology has the added ability to process enormous amounts of data while also using it to learn, build adaptive models, and make actionable predictions, often without clear, comprehensible procedures.

As per our understanding, we can instil techniques to ensure privacy is an integral part of the deployed A.I. These techniques are divided into 3 groups.

- Techniques for lessening the requirement for training data.
- Data protection techniques that don't compromise the size of the initial dataset.
- Techniques intended to get around the black box problem.

We also believe that government has a significant impact on the atmosphere that allows the development of safe and ethical AI to coexist with technological advancement. A comprehensive, multidisciplinary approach is necessary to strike the correct balance because too much, the wrong kind or the wrong kind of regulation could hinder the adoption of AI or ignore its real problems. Building, employing, and regulating AI will heavily rely on rethinking conventional ideas as well as existing information privacy regulations.

SURVEY METHODOOGY



Why did we conduct this survey?

According to an IBM report titled "Global A.I. Adoption Index 2022," over 60% of Indian companies have already been using A.I., which has been said to have increased due to the pandemic enforced digitisation, and many believe that there is no turning point from here.

With the rapid adoption of A.I. around the world and in India, it was critical to understand where we, both as users and manufacturers, stand to recognise the already existing A.I. in our lives and how much of this is what can be classified as Responsible A.I. Furthermore, we wanted to know how aware the general public is of the crossroads that A.I. has with their privacy and what steps they take to ensure that their privacy remains under their control.

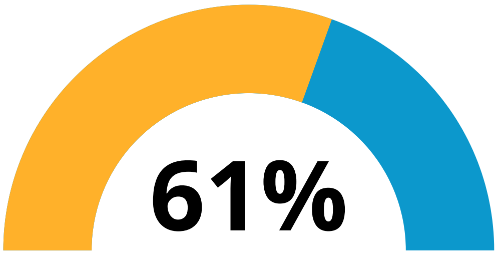
Our Partnership with Fractal on this Survey.

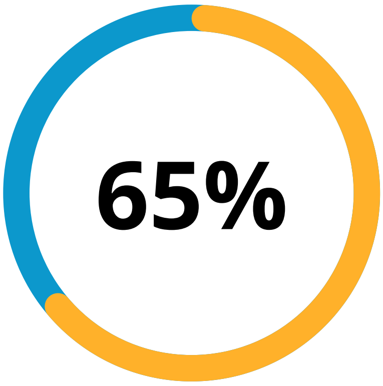
Fractal Analytics is one of India’s significant Unicorns and is the leader in the market of providing A.I. enabled SaaS solutions for decision making. We wanted to partner with this pioneer of A.I. to help understand the various aspects of developing and deploying Responsible A.I. and A.I. in general and where exactly they cross roads with privacy and can end up causing privacy scare. Through this partnership, we were able to understand the process that goes behind instilling the principles of Privacy By Design.

Through this partnership, we were able to delve into two aspects of this survey, one to understand the idea of A.I. and privacy from that of the general public and the other was to understand the mindset of those who work on these A.I. or are directly involved in the development of such A.I.s.

KEY FINDINGS AND MAJOR TAKEAWAYS

Only 61% of the participants are aware of what bias in A.I. is.





65 % of the participants stated that they try avoiding A.I.-enabled features such as phone unlocking using face ID, digital voice assistance, etc.

50% of A.I. developers believe that they are on the verge of developing Responsible A.I.

100% of participants who work on A.I. stated that their company takes measures to teach them about privacy issues relating to A.I.

Survey Process

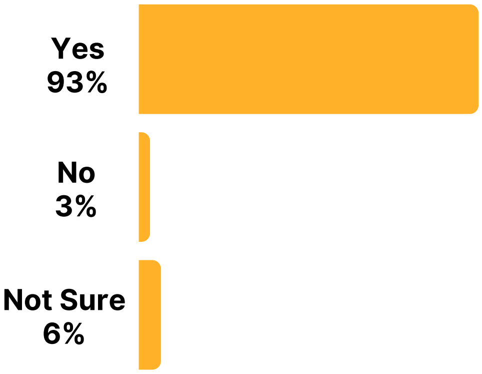
The survey was conducted online through multiple social media, professional channels, and an internal network of both organisations in June 2022. Through this process, our survey: A.I.'s Race for Responsibility and privacy, reached over 1000 people. This sample space was organically attained and consisted of individuals who use these A.I. in their daily lives and those who work on these A.I. systems directly.

Survey Insights

Our sample space consisted of over 1198 individuals.

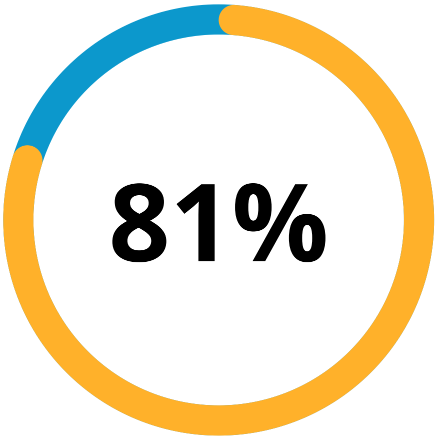
Segment One: General Public

Are you aware of Artificial Intelligence?



93% percent of Public aware about Artificial Intelligence

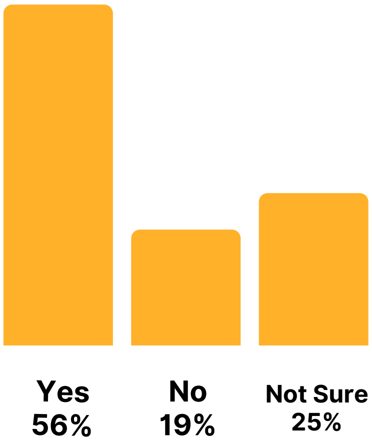
Are you using any A.I. device daily?



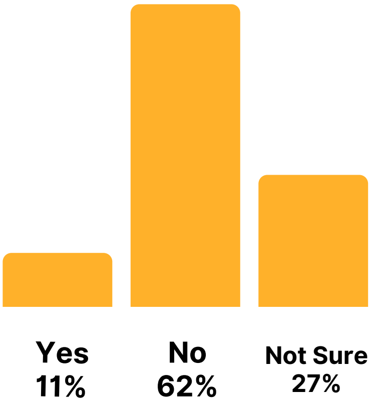
81% percent of Public aware using A.I. device daily

Are you aware of the privacy concerns attached to A.I.?

56% percent of the Public is aware of privacy concerns attached to A.I.?

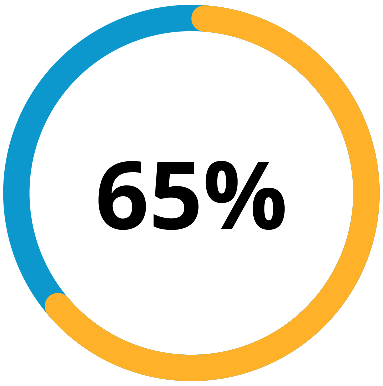


Do you think the A.I. you use is at par with public safety expectations?



62% percent of the Public is not sure that A.I. is at par with public safety expectations

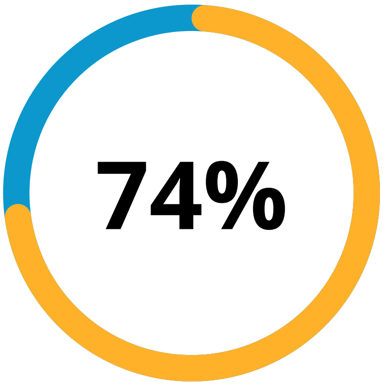
Do you take any steps in your daily life to protect your privacy?



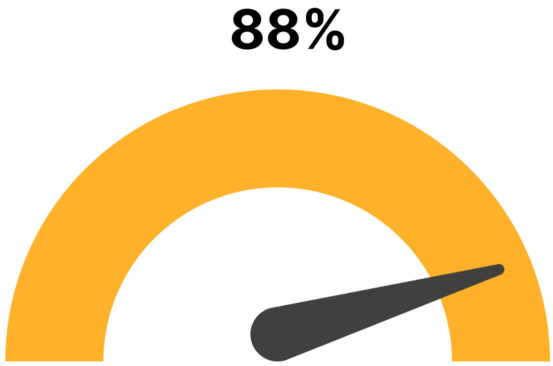
65% of people take steps to avoid A.I.-enabled features such as phone unlocking using face ID, digital voice assistance, etc.

Would you prefer the convenience of A.I. processes over privacy?

74% of people prefer Privacy over convenience



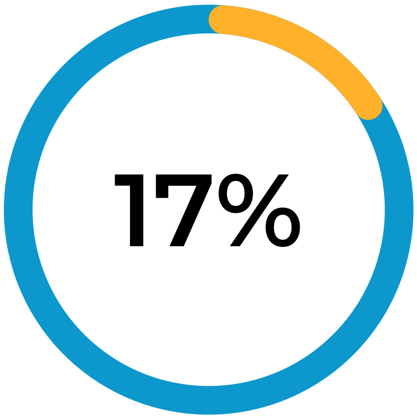
Do you believe A.I. and its use is indispensable in today's day and age?



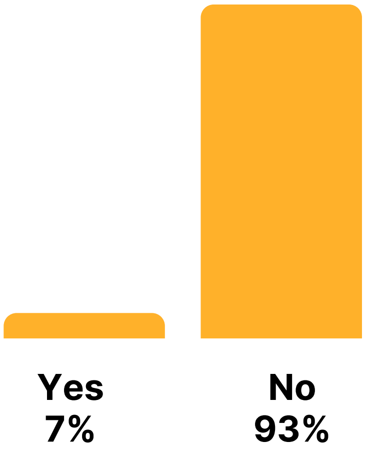
55% of the participants believe that A.I. and its use is indispensable in today's day and age?

Do you think there are any laws in our country that govern the usage of A.I.?

Only 17% of the participants answer yes that there are any laws in our country that govern the usage of A.I.



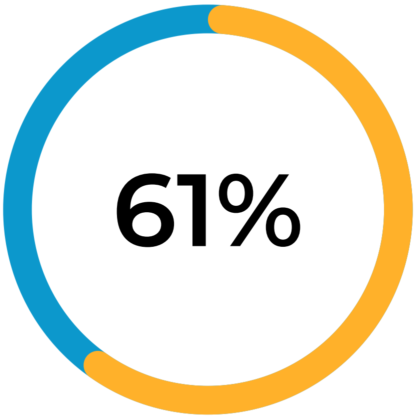
Do you think India has enough safeguards to handle privacy violations caused by the usage of A.I.?



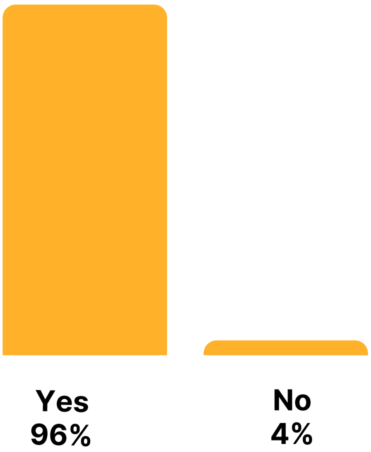
Only 7% of the participants believe that India has enough safeguards to handle privacy violations caused by the usage of A.I.

Are you aware of bias in A.I.?

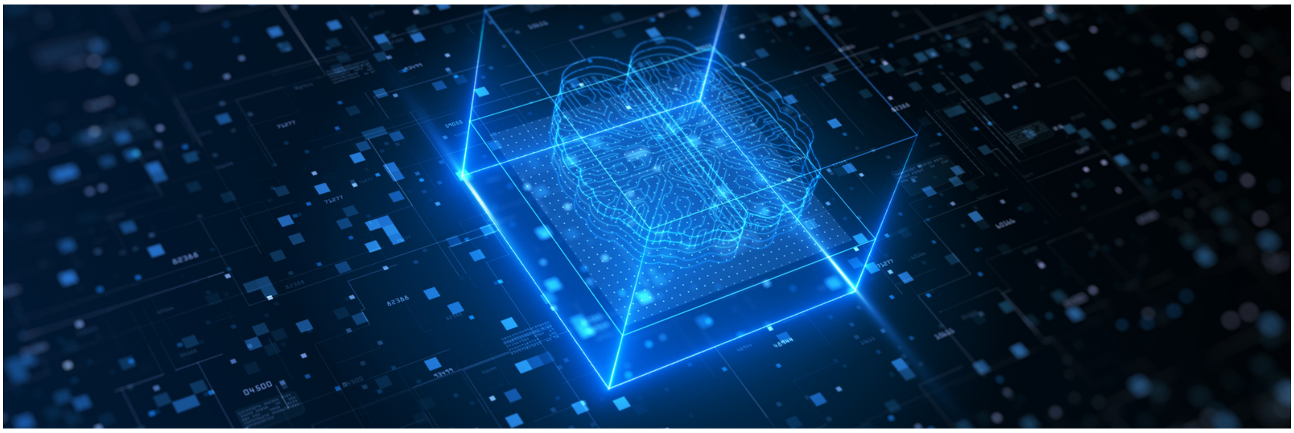
61% percent of the Participants is aware of bias in A.I.



Do you think there is a lack of A.I. governance in our country?

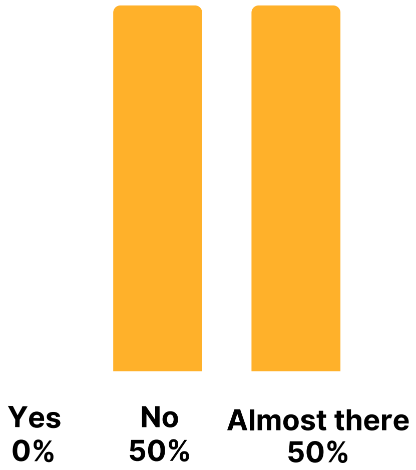


96% percent of participants think that there is a lack of A.I. governance in our country



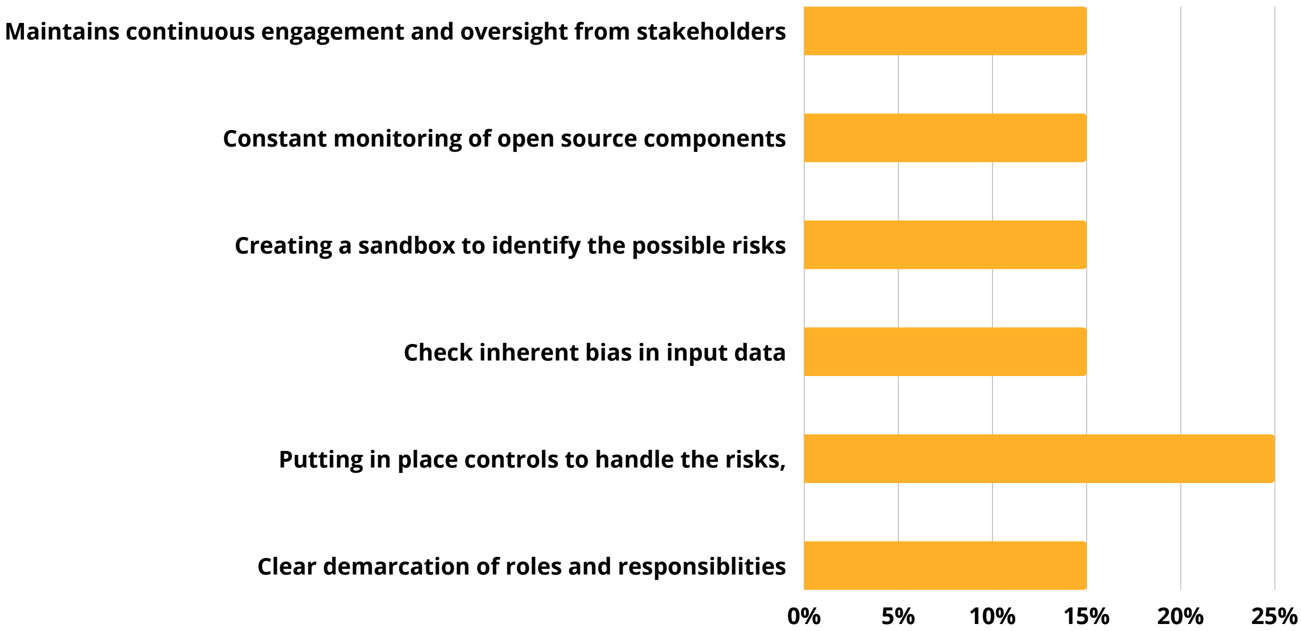
Segment Two: A.I. Developers

Have you implemented fully responsible A.I.?

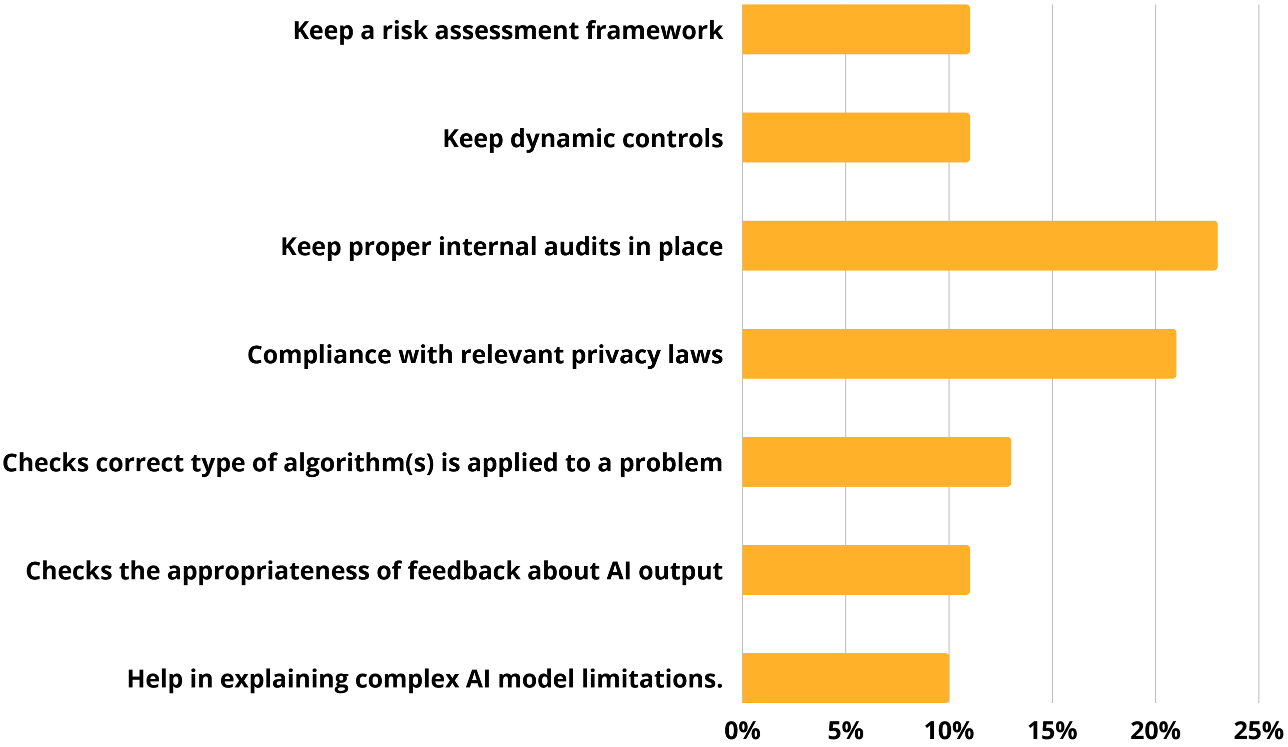


50% percent of participants is on the verge of implementing fully responsible A.I.

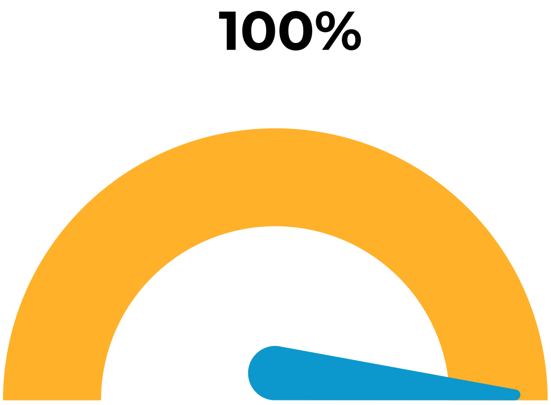
Do you have a Risk Assessment Framework in place?



What steps do you take to prevent attacks or mishandling of your AI?



What steps do you take to prevent attacks or mishandling of your AI?

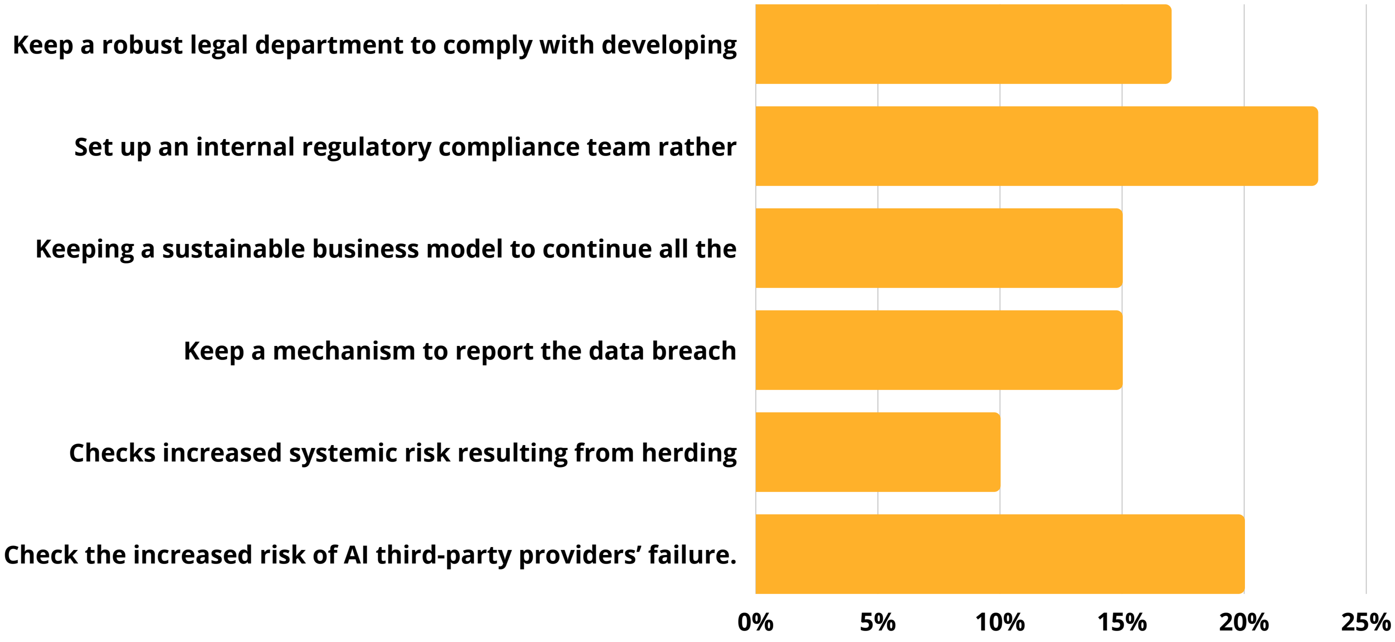


100% Mandatory cyber security training for all employees,

Do we have the organizational ability to plan, check for and remove biases from AI models before releasing them to production?

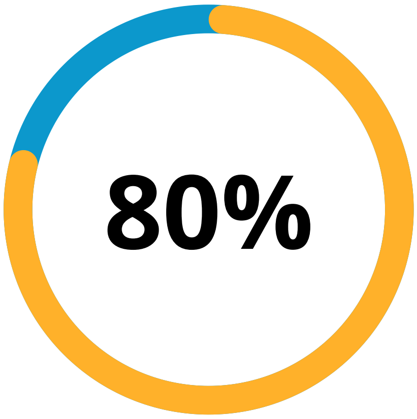
participants state they have established review processes and rely on multiple stakeholders to identify potential biases along with in-house bias detection assests

What steps do you take to prevent attacks or mishandling of your AI?

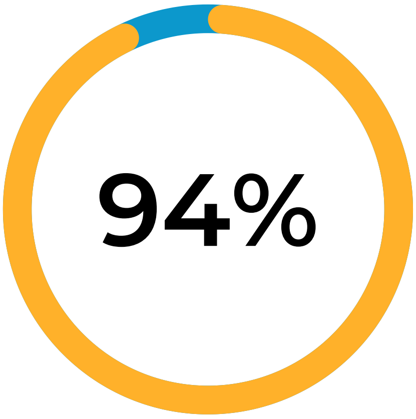


Do you look forward to using synthetic data for your AI in future?

80% of participants anticipate adopting synthetic data for your AI in the future.



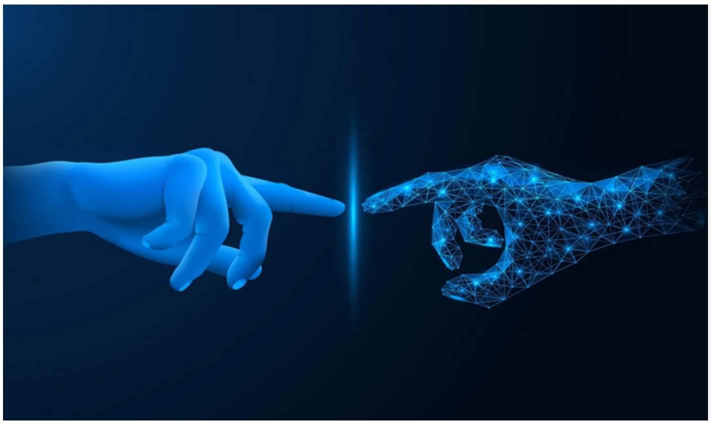
Do you think your company is prepared if a law governs AI technology in our country?



94% of the participants believe that the company is prepared if a law governs AI technology in our country

SUMMARY OF THE FINDINGS

This survey has helped us understand the concept of Privacy in A.I. from the perspectives of both the users and the individuals who work on developing and deploying the A.I. Through this survey; we've come to realise that the public, in general, is very much aware of the privacy issue the present day A.I. that we use in our daily life is consisting of and a more significant part of this sample space 80%, believe that the use of these A.I.s has become indispensable and we end up using them in one way or another.

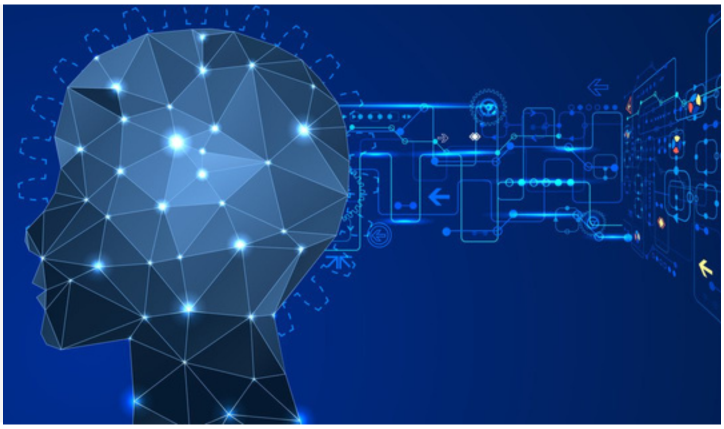


AWARENESS AND USE OF A.I.

- 81% users interact with A.I. regularly, and 56% have a fair knowledge of A.I.'s potential impact on privacy.
- 65% users avoid A.I. enabled features, which shows the importance of privacy.

GOVERNANCE OF A.I.

- 74% users prefer privacy over convenience by using A.I., which reflects a deep mistrust over A.I.
- 93% users feel that A.I. governance in the country is insufficient, and it must be an eye-opener for the concerned stakeholders.



ON RESPONSIBLE AI

- The survey shows a slow-moving mindset among AI developers.
- When communicating with data subjects through A.I. produced data, the environment is primarily opaque.
- A cybersecurity training programme is required for all developers' workers.

SUGGESTIONS FOR IMPROVEMENT

Since we are witnessing the Big Bang of technological advancements, we can see an active deployment of Artificial Intelligence as a part of our everyday schedule. But with their presence and active participation in trying to ease our way of life, we give in something more than just space at home or in our life. We also give them our personal information.

It can be said that there is no control over how personal data is utilised, including when it is used against you. The good news is that developers can reduce privacy issues even before a product is produced. In this approach, we may still enjoy the technological advantages of AI without violating people's privacy. We recommend keeping your data governance policies and integrating them into your AI and allocating resources to developing AI products and monitoring, security, and privacy. Additional measures to safeguard privacy in AI include:

- **Towards transparency by design:** Only the data types required to build the AI should be gathered, and even those should be kept secure and preserved for as long as necessary to achieve the goal.

- **Usage of refined data sets:** Developers should construct AI utilising accurate, fair, and representative data sets. When feasible, programmers should create AI algorithms that check other algorithms' performance and quality.

- **Handing over user control:** Users are supposed to be aware of how their data is being utilised, whether AI is being used to draw judgments about them, and whether their data is being used to build AI. Additionally, they should have the option to agree to their data usage.

- **Minimise algorithmic bias:** When training AI, ensure that the data sets are extensive and diverse. For populations who make up a small part of the technology workforce, such as women, minorities, and the elderly, algorithmic prejudice presents issues most frequently.

- **Mask sensitive information:** Not only PII data but any other data (purchase history, transactions, medical records, navigation data etc.) should be made differentially private at all stages

- **Data Audit:** A comprehensive data audit (and governance) should be in place. The audit should entail permission about data access, usability, needs, purpose, lineage, quality, and documentation to start with.

Akarsh Singh
(CEO & Co-Founder, Tsaaro)
Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

Rohit Jain
(Director Privacy Technology, Tsaaro)
Rohit is the head of the technology department at Tsaaro and is experienced in ensuring the incorporation of Privacy into networked data systems and technologies by default.

Krishna Srivastava
(Co-Founder & Head of Cyber Security, Tsaaro)
Krishna is an xKPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Tsaaro Netherlands Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW, Netherlands
P: +31-686053719

Tsaaro India Office
Manyata Embassy Business Park, Ground Floor, E1 Block,
Beech Building, Outer RingRoad,
Bangalore- 560045
India

Level 1, Building 10A,
Cyber Hub, DLF Cyber City,
Gurugram, Haryana 122002
India
P: +91-77609-23421

Email us
info@tsaaro.com

ABOUT FRACTAL

Fractal is one of the most prominent players in the Artificial Intelligence space. Fractal's mission is to power every human decision in the enterprise and bring AI, engineering, and design to help the world's most admired Fortune 500® companies.

Fractal product companies include Qure.ai, Crux Intelligence, Theremin.ai, Eugenie.ai & Samya.ai.

Fractal has more than 3,600 employees across global locations, including the United States, UK, Ukraine, India, and Australia. Fractal has consistently been rated as India's best company to work for by The Great Place to Work® Institute, a 'Leader' by Forrester Research in its Wave™ on Specialized Insights Services, Computer Vision & Customer Analytics, and an "Honorable Vendor" in 2021 Magic Quadrant™ for data & analytics by Gartner.

ABOUT TSAARO

Tsaaro is a leading data privacy and cyber security service provider helping businesses across technology companies and new-age start-ups secure their applications through future-ready solutions that help keep up with the changing technology landscape.

Our strength lies in assessing security risks, monitoring for threats, and safeguarding applications against compliance issues and the latest threats. We provide data privacy services to align the organization's security roadmap to leading privacy frameworks such as GDPR, CCPA, PDPB, HIPPA. Our information security services complement our privacy and security capabilities with an exhaustive list of assessment and implementation frameworks such as ISO 27001:2013, NIST, and PCI-DSS.

We take a pragmatic, risk-based approach to provide our clients with real-world, workable advice, guidance, and support that helps them to deal with a wide range of security and privacy-related challenges.