

The AI Task Force Report - The first steps towards India's AI framework

Elonnai Hickok, Shweta Mohandas and Swaraj Paul Barooah

Edited by Swagam Dasgupta

Introduction

The Task Force on Artificial Intelligence was established by the Ministry of Commerce and Industry to leverage AI for economic benefits, and provide policy recommendations on the deployment of AI for India. The Task Force's Report, released on March 21st 2018, is a result of the combined expertise of members from different sectors¹ and examines how AI will benefit India. It sheds light on the Task Force's perception of AI, the sectors in which AI can be leveraged in India, the challenges endemic to India and certain ethical considerations. It concludes with a set of policy recommendations for the government to leverage AI for the next five years. While acknowledging AI as a social and economic problem solver,² the Report attempts to answer three policy questions:

1. What are the areas where government should play a role?
2. How can AI improve quality of life and solve problems at scale for Indian citizens?
3. What are the sectors that can generate employment and growth by the use of AI technology?

This blog will look at how the Task Force answered these three policy questions. In doing so, it gives an overview of salient aspects and reflects on the strengths and weaknesses of the Report.

Sectors of Relevance and Challenges

¹ The Task Force consists of 18 members in total. Of these, 11 members are from the field of AI technology both research and industry, three from the civil services, one from healthcare research, one with and Intellectual property law background, and two from a finance background. The specializations of the members are not limited to one area as the members have experience or education in various areas relevant to AI. <https://www.aitf.org.in/> There is a notable lack of members from Civil Society. It may also be noted that only 2 of the 18 members are women

² The Report on the Artificial Intelligence Task Force, Pg. 1, http://dipp.nic.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf

In order to navigate the outlined questions, the Report looks at ten sectors that it refers to as ‘domains of relevance to India’. Furthermore, it examines the use of AI along with its major challenges, and possible solutions for each sector. These sectors include: Manufacturing, FinTech, Agriculture, Healthcare, Technology for the Differently-abled, National Security, Environment, Public Utility Services, Retail and Customer Relationship, and Education.³ While these ten domains are part of the 16 domains of focus listed in the AITF’s web page,⁴ it would have been useful to know the basis on which these sectors were identified. A particular strength of the identified sectors is the consideration of technology for the differently abled as well as the recognition to the development of AI systems in spoken and sign languages in the Indian context.⁵

Some of the problems endemic to India that were recognized include infrastructural barriers, managing scale and innovation, and the collection, validation and distribution of data.⁶ The Task Force also noted the lack of consumer awareness, and inability of technology providers to explain benefits to end users as further challenges.⁷ The Task Force — by putting the onus on the individual — seems to hint that the impediment to the uptake of technology is the inability of individuals to understand the benefits of the technology, rather than aspects such as poor design, opacity, or misuse of data and insights. Furthermore, although the Report recognizes the challenges associated to data in India and highlights the importance of quality and quantity of data; it overlooks the importance of data curation in creating reliable AI systems.⁸

Although the Report examines challenges to AI in each sector, it fails to include all challenges that require addressal. For example, the report fails to acknowledge challenges such as the lack of appropriate certification systems for AI driven health systems and technologies.⁹ In the manufacturing sector, the Report fails to highlight contextual challenges associated with the use of AI. This includes the deployment of autonomous vehicles compared to the use of industrial robots.¹⁰

On the use of AI in retail, the Report while examining consumer data and its respective regulatory policies, identified the issues to be related to the definition, discrimination, data breaches, digital products and safety awareness and reporting standards.¹¹ In this, the Report is limited in its understanding of what categories of data can lead to discrimination and

³ *ibid.*

⁴ The Artificial Intelligence Task Force <https://www.aitf.org.in/>

⁵ The Report on the Artificial Intelligence Task Force, Pg. 8

⁶ The Report on the Artificial Intelligence Task Force, Pg. 9,10.

⁷ The Report on the Artificial Intelligence Task Force, Pg. 9

⁸ *ibid.*

⁹ Artificial Intelligence in the Healthcare Industry in India <https://cis-india.org/internet-governance/files/ai-and-healthcare-report>

¹⁰ Artificial Intelligence in the Manufacturing and Services Sector https://cis-india.org/internet-governance/files/AIManufacturingandServices_Report_02.pdf

¹¹ The Report on the Artificial Intelligence Task Force, Pg. 21.

restricts mechanisms for transparency and accountability to data breaches. The Report could have also been more forward looking in its position on security — including security by design and security by default. Furthermore, these issues were noted only in the context of the retail sector and ideally should have been discussed across all sectors.

The challenges for utilizing AI for national security could have been examined beyond cost and capacity to include associated ethical and legal challenges such as the need for legal backing. The use of AI in national security demands clear accountability and oversight as it is a ground for legitimate state interference with fundamental rights such as privacy and freedom of expression. As such, there is a need for human rights impact assessments, as well as a need for such uses to be aligned with international human rights norms. Government initiatives that allow country wide surveillance and AI decisions based on such data should ideally be implemented only after a comprehensive privacy law is in place and India's surveillance regime has been revisited.¹²

Recognizing the potential of AI for the benefit of the differently abled is one of the key takeaways from this section of the Report. Furthermore, it also brings in the need for AI inclusivity. AI in natural language generation and translation systems have the potential to help the large number of youth that are disabled or deprived.¹³ Therefore, AI could have a large positive impact through inclusive growth and empowerment.

Although the Report examines each of the ten domains in an attempt to provide an insight into the role the government can play, there seems to be a lack of clarity in terms of the role that each department will and is playing with respect to AI. Even the section which lays down the relevant ministries for each of the ten domains failed to include key ministries and departments. For example, the Report does not identify the Ministry of Education, nor does it list the Ministry of Law for national security. The Report could have also identified government departments which would be responsible for regulation and standardization. This could include the Medical Council of India (healthcare), CII (manufacture and retail), RBI (Fintech) etc. The Report also does not recognize other developments around AI emerging out the government. For example, the Draft National Digital Communications Policy (published on May 1, 2018) seeks to empower the Department of Telecommunication to provide a roadmap for AI and robotics.¹⁴ Along similar lines, the Department of Defence Production has also created a task force earlier this year to study the use of AI to accelerate military technology and economic growth.¹⁵ The government should look at building a cohesive AI government body, or clearly delineating the role of each ministry, in order to ensure harmonization going forward.

¹² Submission to the Committee of Experts on a Data Protection Framework for India, Centre for Internet and Society <https://cis-india.org/internet-governance/files/data-protection-submission>

¹³ The Report on the Artificial Intelligence Task Force, Pg. 22

¹⁴ Draft National Digital Communications Policy-2018, <http://www.dot.gov.in/relatedlinks/draft-national-digital-communications-policy-2018>

¹⁵ Task force set up to study AI application in military, <https://indianexpress.com/article/technology/tech-news-technology/task-force-set-up-to-study-ai-application-in-military-5049568/>

Areas in need of Government Intervention

The Report also lists out the grand challenges where government intervention is required. This includes data collection and management and the need for widespread expertise contributing to research, innovation, and response. However, while highlighting the need for AI experts from diverse backgrounds, it fails to include experts from law and policy into the discussion.¹⁶ While identifying manufacturing, agriculture, healthcare and public utility to be places where government intervention is needed, the Report failed to examine national security beyond an important domain to India and as a sector where government intervention is needed.

Participation in International Forums

Another relevant concern that the Report underscores is India's scarce participation as researchers, AI developers and government engagement in global discussions around AI. The Report states that although efforts were being made by Indian universities to increase their presence in international AI conferences, they were lagging behind other nations. On the subject of participation by the government it recommends regular presence in International AI policy forums. Hence, emphasising the need for India's active participation in global conversations around AI and international rulemaking.

Key Enablers to AI

The Report while analysing the key enablers for AI deployment in India states that positive societal attitudes will be the driving force behind the proliferation of AI.¹⁷ Although relying on positive social attitudes alone will not help in increasing the trust on AI, steps such as making algorithms that are used by public bodies public, enacting a data protection law etc. will be important in enabling trust beyond highlighting success stories.

Data and Data Marketplaces

While the Report identifies data as a challenge where government intervention is needed, it also points to the Aadhaar ecosystem as an enabler. It states that Aadhaar will help in the proliferation of AI in three ways: one as a creator of jobs as related to the collection and digitization of data, two as a collector of reliable data, and three as a repository of Indian data. However, since the very constitutionality of Aadhaar is yet to be determined by the

¹⁶It is not just technical experts that are needed, ethical, technical, and legal experts as well as domain experts need to be part of the decision making process.

¹⁷ The Report on the Artificial Intelligence Task Force, Pg. 31

Supreme Court,¹⁸ the task force should have used caution in identifying Aadhaar as a definitive solution. Especially while making statements that the Aadhaar along with the SC judgement has created adequate frameworks to protect consumer data. Additionally, the Task Force should have recognized the various concerns that have been voiced about Aadhaar, particularly in the context of the case before the Supreme Court.¹⁹

This section also proposes the creation of a Digital Data Marketplace. A data marketplace needs to be framed carefully so as to not create a situation where privacy becomes a right available to only those who can afford it.²⁰ It is concerning that the discussion on data protection and privacy in the Report is limited to policies and guidelines for businesses and not centered around the individual.

Innovation and Patents

The Report states that the Indian startups working in the field of AI must be encouraged, and industry collaborations and funding must be taken up as a policy measure. One of the ways in which this could be achieved is by encouraging innovations, and one of the ways to do so is by adding a commercial incentive to it, such as through IP rights. Although the Report calls for a stronger IP regime that protects and incentivises innovation, it remains ambiguous as to which aspect of IP rights — patents, trade secrets and copyrights — need significant changes.²¹ If the Report is specifically advocating for stronger patent rights in order to match those of China and US, then it shows that the the task force fails to understand the finer aspects of Indian patent law and the history behind India’s stance on patenting. This includes the fact that Indian patent law excludes algorithms from being patented. Indian patent law, by providing a higher threshold for patenting computer related inventions (CRIs), ensures that only truly innovative patents are granted.²² Given the controversies over CRIs that have dotted the Indian patent landscape²³, the task force would have done well to provide more clarity on the ‘how’ and ‘why’ of patenting in this sector, if that is their intent with this suggestion.

Ethical AI framework

¹⁸Constitutional validity of Aadhaar: the arguments in Supreme Court so far, <http://www.thehindu.com/news/national/constitutional-validity-of-aadhaar-the-arguments-in-supreme-court-so-far/article22752084.ece>

¹⁹ *ibid.*

²⁰ CIS Submission to TRAI Consultation on Free Data

http://traf.gov.in/Comments_FreeData/Companies_n_Organizations/Center_For_Internet_and_Society.pdf

²¹ The Report on the Artificial Intelligence Task Force, Pg. 30

²² Section 3(k) of the patent act describes that a mere mathematical or business method or a computer programme or algorithm cannot be patented.

²³ Patent Office Reboots CRI Guidelines Yet Again: Removes “novel hardware” Requirement

<https://spicyip.com/2017/07/patent-office-reboots-cri-guidelines-yet-again-removes-novel-hardware-requirement.html>

Responsible AI

In terms of establishing an ethical AI framework, the Task Force suggests measures such as making AI explainable, transparent, and auditable for biases. The Report addresses the fact that currently with the increase in human and AI interaction there is a need to have new standards set for the deployment of AI as well as industrial standards for robots. However, the Report does not go into details of how AI could cause further bias based on various identifiers such as gender and caste, as well as the myriad concerns around privacy and security. This is especially a concern given that the Report envisions widespread use of AI in all major sectors. In this way, the Report looks at data as both a challenge and an enabler, but fails to dedicate time towards explaining the various ethical considerations behind the collection and use of data in the context of privacy, security and surveillance as well as account for unintended consequences. In laying out the ethical considerations associated with AI, the report does not make a distinction between the use of AI by the public sector and private sector. As the government is responsible for ensuring the rights of citizens and holds more power than the citizenry, the public sector needs to be more accountable in their use of AI. This is especially so in cases where AI is proposed to be used for sovereign functions such as national security.

Privacy and Data

The Report also recognises the significance of the implementation of the Aadhaar Act²⁴, the privacy judgement²⁵ and the proposed data protection laws²⁶, on the development and use of AI for India. Yet, the Report does not seem to recognize the importance of a robust and multi-faceted privacy framework as it assumes that the Aadhaar Act and the Supreme Court Judgement on privacy and potential privacy law have already created a basis for safe and secure utilization and sharing of customer data.²⁷ Although the Report has tried to be an expansive examination of various aspects of AI for India, it unfortunately has not looked in depth at the current issues and debates around AI privacy and ethics and makes policy recommendations without appearing to fully reflect on the implementation and potential impact of the same. Similar to the discussion paper by the Niti Aayog,²⁸ this Report does not consider the emerging principles of data protection such as right to explanation and right to opt-out of automated processing, which directly relate to AI.²⁹ Furthermore, there is a lack of

²⁴ The Report on the Artificial Intelligence Task Force, Pg. 37

²⁵ The Report on the Artificial Intelligence Task Force, Pg. 7

²⁶ *ibid.*

²⁷ The Report on the Artificial Intelligence Task Force, Pg. 8

²⁸ National Strategy for Artificial Intelligence:

http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

²⁹ Meaningful information and the right to explanation, Andrew D Selbst Julia Powles, International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, Pages 233–242

discussion on issues such as data minimisation and purpose limitation which some big data and AI proponents argue against.³⁰

Liability

On the question of liability, the Report only states that specific liability mechanisms need to be worked out for certain categories of machines. The Report does not address the questions of liability that should be applicable to all AI systems, and on whom the duty of care lies, not only in case of robots but also in the case of automated decision making etc. Thus, there is a need for further thinking on mechanisms for determining liability and how these could apply to different types of AI (deep learning models and other machine learning models) and AI systems.

AI and Employment

On the topic of jobs and employment, the Report states that AI will create more jobs than it takes as a result of an increase in the number of companies and avenues created by AI technologies. Additionally, the Report provides examples of jobs where AI could replace the human (autonomous drivers, industrial robots etc.) but does not go as far as envisioning what jobs could be created directly from this replacement. Though the Report recognizes emerging forms of work such as crowdsourcing platforms like Mturk³¹, it fails to examine the impact of such models of work on workers and traditional labour market structures and processes.³² Going forward, it will be important that the government and the private sector undertake the necessary steps to ensure that fair, protected, and fulfilling jobs are created simultaneously with the adoption of AI. This will include revisiting national and organizational skilling programmes, labor laws, social benefit schemes, relevant economic policies, and exploring best practices with respect to the adoption and integration of AI in work.

Education and Re-skilling

The task force emphasised the need for a change in the education curriculum as well as the need to reskill the labour force to ensure an AI ready future. This level of reskilling will be a massive effort, and a thorough review and audit of existing skilling programmes in India is needed before new skilling programmes are established and financed. The Report also clarifies that the statistics used were based on a study on the IT component of the industry, and that a similar study was required to analyse AI's effect on the automation component.³³

³⁰ The Principle of Purpose Limitation and Big Data, https://www.researchgate.net/publication/319467399_The_Principle_of_Purpose_Limitation_and_Big_Data

³¹ M-Turk <https://www.mturk.com/>

³² For example a lesser threshold of minimum wages, no job security etc, <https://blogs.scientificamerican.com/guilty-planet/httpblogsscscientificamericancomguilty-planet20110707the-pros-cons-of-amazon-mechanical-turk-for-scientific-surveys/>

³³ The Report on the Artificial Intelligence Task Force, Pg. 41

Going forward, there is the need for a comprehensive study of the labour intensive sectors and formal and informal sectors to develop evidence based policy responses.

Policy Recommendations

The Task Force, in its policy recommendations, notes that the successful adoption of AI in India will depend on three factors: people, process and technology. However, it does not explain these three factors any further.

National Artificial Intelligence Mission

The most significant suggestion made in the Report is for the establishment of the National Artificial Intelligence Mission (N-AIM) — a centralised nodal agency for coordinating and facilitating research, collaboration and providing economic impetus to AI startups.³⁴ The mission with a budget allocation of Rs 1,200 crore over five years aims, among other things, to look at various ways to encourage AI research and deployment.³⁵ Some of the suggestions include targeting and prototyping AI systems and setting up of a generic AI test bed. These suggestions seem to draw inspiration from other countries such as the US DARPA Challenge³⁶ and Japan's sandbox for self driving trucks.³⁷ The establishment of N-AIM is a welcome step to encourage both AI research and development on a national scale. The availability of public funds will encourage more AI research and development.³⁸ Additionally, government engagement in AI projects has thus far been fragmented³⁹ and a centralised body will presumably bring about better coordination and harmonization. Some of the initiatives such as Capture the flag competition⁴⁰ that seeks to centre around the provision for real datasets to catalyze innovation will need to be implemented with appropriate safeguards in place.

Other recommendations

There are other suggestions that are problematic — particularly that of funding “an interdisciplinary large data integration center in pilot mode to develop an autonomous AI Machine that can work on multiple data streams in real time and provide relevant information and

³⁴ Report of Artificial Intelligence Task Force Pg, 46, 47

³⁵ *ibid.*

³⁶ The DARPA Challenge <https://www.darpa.mil/program/darpa-robotics-challenge>

³⁷ Japan may set regulatory sandboxes to test drones and self driving vehicles <http://techwireasia.com/2017/10/japan-may-set-regulatory-sandboxes-test-drones-self-driving-vehicles/>

³⁸ Mariana Mazzucato in her 2013 book *The Entrepreneurial State*, argued that it was the government that drives technological innovation. In her book she stated that high-risk discovery and development were made possible by government spending, which the private enterprises capitalised once the difficult work was done.

³⁹ <https://tech.economictimes.indiatimes.com/news/technology/govt-of-karnataka-launches-centre-of-excellence-for-data-science-and-artificial-intelligence/61689977>, <https://analyticsindiamag.com/amaravati-world-centre-for-ai-data/>

⁴⁰ The Report on the Artificial Intelligence Task Force, Pg. 47

predictions to public across all domains.”⁴¹ Before such a project is developed and implemented there are a number of factors where legal clarity is required; a few being: data collection and use, accuracy and quality of the AI system. There is also a need to ensure that bias and discrimination have been accounted for and fairness, responsibility and liability have been defined with consideration that this will be a government driven AI system. Additionally, such systems should be transparent by design and should include redress mechanisms for potential harms that may arise. This can be through the presence of a human in the loop, or the existence of a kill switch. These should be addressed through ethical principles, standards, and regulatory frameworks.

The recommendations propose establishing operation standards for data storage and privacy, communication standards for autonomous systems, and standards to allow for interoperability between AI based systems. A significant lacuna in this list is the development of safety, accuracy, and quality standards for AI algorithms and systems.

Similarly, although the proposed public private partnership model for research and startups is a good idea, this initiative should be undertaken only after questions such as the implications of liability, ownership of IP and data, and the exclusion of critical sectors are thought through.

Furthermore, the suggestion to ‘fund a national level survey on identification of cluster of clean annotated data necessary for building effective AI systems’⁴² needs to recognize the existing initiatives around open data or use this as a starting place. The Report does not clarify if this survey would involve identifying data.

Conclusion

The inconspicuous release of the Report as well as the lack of a call for public comments⁴³ results in the fact that the Report does not incorporate or reflect on the sentiments of the public or draw upon the expertise that exists in India on the topic or policies around emerging technologies, which will have a pervasive and wide effect on society. The need for multi stakeholder engagement and input cannot be understated. Nonetheless, the Report of the Task Force is a welcome step towards understanding the movement towards an definitive AI policy. The task force has attempted answering the three policy questions keeping people, process and technology in mind. However, it could have provided greater details about these indices. The Report, which is meant for a wider audience, would have done well to provide greater detail, while also providing clarity on technical terms. On a definitional plane, a list of technologies that the task force perceived as AI for this Report, could have also helped keep it grounded on possible and plausible 5 year recommendations.

⁴¹ Report of Artificial Intelligence Task Force Pg. 49

⁴² The Report on the Artificial Intelligence Task Force, Pg. 47

⁴³ The AI task force website has a provision for public comments although it is only for the vision and mission and the domains mentioned in the website.

Compared to the recent Niti Aayog Discussion Paper⁴⁴, this Report misses out on a detailed explanation on AI and ethics, however, it does spend some considerable amount of time on education and the use of AI for the differently abled. Additionally, the Report's statement on the democratization of development and equal access as well as assigning ownership and framing transparent rules for usage of the infrastructure is a positive step towards making AI inclusive. Overall, the Report is a progressive step towards laying down India's path forward in the field of Artificial Intelligence. The emphasis on India's involvement in International rulemaking gives India an opportunity to be a leader of best practice in international forums by adopting forward looking and human rights respecting practices. Whether India will also become a strong contender in the AI race, with policies favouring the development of a socio-economically beneficial, and ethical-AI backed industries and services is yet to be seen.

⁴⁴National Strategy for Artificial Intelligence:
http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf